Loi fédérale sur la protection des données

Dernière modification : 27.07.2026

PDF créé le : 06.10.2026

COMMENTAIRE EN LIGNE
LE COMMENTAIRE JURIDIQUE
EN OPEN ACCESS

TABLE DES MATIÈRES

Vorb. zu Art. 1 LPD 7
Art. 1 LPD 15
Art. 2 LPD 21
Art. 3 LPD 31
Art. 4 LPD 37
Art. 5 let. c LPD 49
Art. 5 let. d LPD 65
Art. 5 lit. f und g LPD 75
Art. 6 al. 3-5 LPD 93
Art. 6 al. 6 et 7 LPD 115
Art. 7 LPD 139
Art. 10 LPD 165
Art. 11 LPD 187
Art. 12 LPD 203
Art. 14 LPD 223
Art. 15 LPD 233
Art. 19 LPD 239
Art. 18 LPD 267
Art. 20 LPD 275
Art. 21 LPD 293
Art. 22 LPD 333
Art. 23 LPD 357
Art. 25 LPD 373
Art. 26 LPD 389
Art. 27 LPD 399
Art. 28 LPD 407
Art. 29 LPD 431
Art. 31 al. 2 let. e LPD 441
Art. 33 LPD 451

Art. 34 LPD 457
Art. 35 LPD 477
Art. 38 LPD 487
Art. 39 LPD 505
Art. 40 LPD 519
Art. 41 LPD 533
Art. 42 LPD 547
Art. 43 LPD 553
Art. 44 LPD 569
Art. 44a LPD 579
Art. 45 LPD 585
Art. 46 LPD 593
Art. 47 LPD 599
Art. 47a LPD 607
Art. 48 LPD 613
Art. 49 LPD 621
Art. 50 LPD 633
Art. 51 LPD 651
Art. 52 LPD 667
Art. 54 LPD 685
Art. 55 LPD 717
Art. 58 LDP 755
Art. 57 LPD 773
Art. 60 LPD 789
Art. 61 LPD 801
Art. 62 LPD 815
Art. 63 LPD 825
Art. 64 LPD 833
Art. 65 LPD 843
Art. 66 LPD 849

Art. 67 LPD 855
Art. 69 LPD 873
Art. 72 LPD 881
Art. 72a LPD 887

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Vorb. zu Art. 1 LPD

Un commentaire de Sandra Husi-Stämpfli

PROPOSITION DE CITATION

Sandra Husi-Stämpfli, Kommentierung zu Vorb. zu Art. 1 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Husi-Stämpfli, N. XXX zu Vorb. zu Art. 1 DSG.

TABLE DES MATIÈRES

En bref 9
I. Le serment d'Hippocrate comme premier secret professionnel 9
II. 20e siècle : Le droit de la protection des données fait son entrée dans les systèmes juridiques 9
III. 21e siècle : Protection des données et numérisation 11
A. Impulsion : révision de la protection des données dans l'UE 11
B. La voie suisse vers une loi moderne sur la protection des données 11
Bibliographie 13

EN BREF

Le droit de la protection des données trouve son origine dans les secrets professionnels (antiques), tels qu'ils ont été développés pour la première fois par Hippocrate : Il s'agissait de garder secrètes les informations concernant les patientes et les patients. C'est à partir de ce concept que se sont développées, à partir de 1970, les premières codifications globales du droit de la protection des données, d'abord dans certains pays, puis peu à peu au-delà des frontières, par le biais d'organisations internationales et enfin de la Communauté européenne, en raison des progrès techniques croissants, de la complexité et de la mondialisation de l'échange d'informations qui en découlent. La première loi sur la protection des données en Suisse est entrée en vigueur en 1992, la révision totale (nouvelle) loi sur la protection des données le 1er septembre 2023.

I. LE SERMENT D'HIPPOCRATE COMME PREMIER SECRET PROFESSIONNEL

La première réglementation codifiée relative à la protection des données personnelles remonte à la période comprise entre 460 et 370 avant Jésus-Christ : Avec le serment d'Hippocrate, les médecins s'engagent encore aujourd'hui à garder secrètes les informations concernant leurs patients. Divers secrets professionnels ont suivi, comme le secret des sages-femmes, le secret de la confession ou le secret des avocats. 1

II. 20E SIÈCLE : LE DROIT DE LA PROTECTION DES DONNÉES FAIT SON ENTRÉE DANS LES SYSTÈMES JURIDIQUES

Les prescriptions relatives à la protection des informations personnelles, initialement liées à la profession, telles que le secret médical, le secret des sages-femmes ou encore le secret professionnel des avocats, reposent sur la conviction que les violations peuvent être constatées immédiatement et que les personnes responsables peuvent également être tenues responsables sans autre effort. 2

3 Ce concept de responsabilités claires a été dépassé dès le siècle dernier par le progrès technique, la complexité qui en découle et la mondialisation croissante de l'échange d'informations. C'est ainsi que dans les années 70 du siècle dernier sont apparues les premières questions concernant le traitement "automatisé" des données, c'est-à-dire l'utilisation d'ordinateurs et les responsabilités et défis qui y sont liés en matière de sécurité des données - soudain, ce n'était par exemple plus "seulement" le médecin qui rédigeait une note manuscrite dans le dossier physique du patient - les données étaient enregistrées sur un ordinateur personnel, dont la maintenance était éventuellement assurée par une entreprise informatique externe, etc. Les nouveaux défis qui en découlent ont donné le coup d'envoi, vers 1970, à la création des premières codifications globales en matière de protection des données, d'abord dans certains pays, puis, peu à peu, au niveau transfrontalier, par des organisations internationales et, enfin, par la Communauté européenne.

4 Exemples :

- 1973 : Suède.
- 1977 : République fédérale d'Allemagne.
- 1978 : Autriche et France.
- 1980 : Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données à caractère personnel.
- 1981 : Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.
- 1995 : Directive européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- 2000 : Charte des droits fondamentaux de l'UE (EU-GRC) avec l'art. 8 "Protection des données à caractère personnel".

En Suisse, le mouvement de codification, tant au niveau cantonal que fédéral, a débuté dans les années 1970 et a finalement abouti à la loi fédérale sur la protection des données en 1992.

III. 21E SIÈCLE : PROTECTION DES DONNÉES ET NUMÉRISATION

Issue d'une époque où les "traitements automatisés de données" étaient l'exception, la LPD pouvait de moins en moins répondre aux exigences du monde numérisé. La révision de la LPD a été fortement influencée par la révision de la protection des données dans l'UE : 5

A. Impulsion : révision de la protection des données dans l'UE

En 2012, l'Union européenne a lancé les discussions sur le droit moderne de la protection des données. Après d'intenses négociations, le Parlement européen et le Conseil de l'Union européenne ont finalement adopté en 2016 le règlement général sur la protection des données (RGPD) de l'UE et la directive 2016/680. 6

- Le RGPD régit principalement la protection des données traitées dans le cadre du marché intérieur européen, mais s'applique également au secteur public. Il est entré en vigueur le 25 mai 2018.
- La directive 2016/680 vise à protéger les données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution des peines, y compris la protection contre les menaces à la sécurité publique et la prévention de telles menaces. La directive 2016/680 est alignée sur le texte du RGPD afin d'obtenir un vocabulaire de base uniforme dans tout l'espace de l'UE en ce qui concerne les principes généraux. Elle est entrée en vigueur le 5 mai 2016.

B. La voie suisse vers une loi moderne sur la protection des données

Le 9 décembre 2011, le Conseil fédéral a approuvé un rapport sur l'évaluation de la LPD et a chargé le Département fédéral de justice et police (DFJP) d'examiner des mesures législatives visant à renforcer la protection des données en tenant compte des résultats de l'évaluation et des développements en cours dans l'UE et au Conseil de l'Europe. Le Conseil fédéral s'était alors demandé dans quelle mesure il fallait accroître la transparence sur les traitements de données et sensibiliser davantage les 7

personnes concernées aux nouveaux risques. Lors de l'examen de la nécessité de légiférer, il faudrait notamment tenir compte du fait que les mineurs sont particulièrement vulnérables en ce qui concerne le traitement de leurs données. Parallèlement, le Conseil fédéral a souligné que lors de l'examen des mesures législatives, il fallait également tenir compte du fait que les mesures de protection des données pouvaient entrer en conflit avec d'autres intérêts. Outre la protection de la personnalité, il convient donc de prendre en compte les intérêts de l'économie, le droit à la liberté d'opinion et d'information ainsi que d'autres intérêts privés et publics. Ces travaux ont été menés avec la participation d'un groupe d'accompagnement qui a défini la nécessité de légiférer jusqu'en 2014.

8 Après avoir pris connaissance du rapport du groupe d'accompagnement le 1er avril 2015, le Conseil fédéral a chargé le DFJP d'élaborer un avant-projet de révision de la LPD d'ici fin août 2016 au plus tard. Cet avant-projet de révision totale de la LPD et de modification d'autres actes législatifs relatifs à la protection des données en vue de la consultation a été mis en consultation le 21 décembre 2016.

9 Le 15 septembre 2017, le Conseil fédéral a finalement adopté le message relatif à la "nouvelle" loi sur la protection des données. L'objectif du Conseil fédéral était "d'adapter la protection des données à l'ère d'Internet et de (renforcer) la position des citoyens". Parallèlement, le niveau de protection des données en Suisse devait être aligné sur celui de l'UE afin de préserver la décision d'adéquation, importante pour la libre transmission des données entre les entreprises suisses et celles de l'UE.

10 Les délibérations parlementaires ont été difficiles, les avis étaient parfois fondamentalement divergents quant à l'étendue du nouveau droit de la protection des données. Mais en même temps, le temps pressait : certaines dispositions du nouveau droit de la protection des données étaient "pertinentes pour Schengen" et devaient être mises en œuvre dans les deux ans suivant l'entrée en vigueur du droit Schengen correspondant. Le Parlement a donc décidé de scinder le projet en deux : La loi dite "loi sur la protection des données Schengen" a été adoptée le 28 septembre 2018 et est entrée en vigueur le 1er mars 2019. Elle a été abrogée ou réintégrée dans la nouvelle loi sur la protection des données dès l'entrée en vigueur de cette dernière. La "loi sur la protection des données Schengen" régissait le traitement de données personnelles par les organes fédéraux à des fins de

prévention, de détection ou de poursuite d'infractions pénales ou d'exécution de peines, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

Dans une deuxième étape, les aspects de la révision de la protection des données qui n'étaient pas pertinents pour les Schengen et qui étaient fortement influencés par le DSGVO ont été discutés. Il s'agissait notamment des nouveautés concernant le traitement de données personnelles par des personnes privées (c'est-à-dire en premier lieu des entreprises). Les thèmes suivants ont été au centre des discussions : 11

- Le renforcement des droits des personnes concernées : Extension du droit d'accès (OK-Steiger ad art. 25 LPD) et introduction d'un droit à la portabilité des données (voir à ce sujet le commentaire du CO ad art. 28 LPD).
- Extension des obligations des responsables du traitement des données et des sous-traitants : introduction du principe de privacy by design and default (OK-Klaus ad art. 7 LPD) et de l'obligation de procéder à une analyse d'impact sur la protection des données pour certaines formes de traitement des données (OK-Harasgama ad art. 22 LPD) et de notifier les violations de la protection des personnes concernées à l'autorité de surveillance (OK-de la Cruz ad art. 24 LPD).
- Introduction d'un catalogue de sanctions (OK-Gassmann ad art. 60 ss LPD) et renforcement des compétences du PFPDT (OK-Reinle ad art. 49 LPD ; OK-Fanger/Oehri ad art. 50 LPD).

Finalement, après trois ans, la loi révisée sur la protection des données a pu être adoptée le 25 septembre 2020. Le référendum n'ayant pas été utilisé, la loi est entrée en vigueur le 1er septembre 2023, en même temps que l'ordonnance d'exécution (OAD), elle aussi totalement révisée. 12

Dans ce commentaire, l'auteur donne son appréciation personnelle.

BIBLIOGRAPHIE

Husi-Stämpfli Sandra, Kommentierung zur Entstehungsgeschichte des DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Auflage, Bern 2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 1 LPD

Un commentaire de Sandra Husi-Stämpfli

PROPOSITION DE CITATION

Sandra Husi-Stämpfli, Kommentierung zu Art. 1 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Husi-Stämpfli, N. XXX zu Art. 1 DSG.

Chapitre 1
But, champ d'application et autorité fédérale de surveillance

Art. 1 But

La présente loi vise à protéger la personnalité et les droits fondamentaux des personnes physiques dont les données personnelles font l'objet d'un traitement.

TABLE DES MATIÈRES

En bref 17
I. Avant tout : les différentes formes de protection de la personnalité 17
A. Protection constitutionnelle de l'autodétermination en matière d'information au sens de l'art. 13 al. 2 Cst. 17
B. Protection de la personnalité en droit civil 18
II. Protection de la personnalité en vertu du droit de la protection des données 19
A. Genèse de l'art. 1 LPD 19
B. Finalité de la LPD 19
C. Nature juridique de l'art. 1 LPD 20
Bibliographie 20

EN BREF

Le droit de la protection des données assure, conjointement avec la protection de la personnalité de droit civil, la mise en œuvre de la protection de la personnalité relevant des droits fondamentaux : la LPD sert à protéger la personnalité et les droits fondamentaux des personnes physiques, et non plus à protéger les personnes morales, comme c'était encore le cas dans l'ancienne LPD. L'objectif de la LPD est donc plus restreint que celui du DSGVO, par exemple, qui a également pour but de permettre la libre circulation des données. Avec la formulation choisie, le législateur suisse indique clairement que le droit de la protection des données est la protection de la personnalité avant tout, et non la protection des acteurs économiques, de la sécurité publique ou d'autres intérêts.

I. AVANT TOUT : LES DIFFÉRENTES FORMES DE PROTECTION DE LA PERSONNALITÉ

Le droit de la protection des données assure, conjointement avec la protection de la personnalité en droit civil (art. 27 et art. 28 ss CC, voir N. 3), la mise en œuvre de la protection de la personnalité inscrite dans les droits fondamentaux (art. 10 Cst., voir N. 2) et, en tant qu'expression de celle-ci, de la sphère privée ou de l'autodétermination en matière d'information (art. 13 al. 2 Cst., voir N. 2). L'interaction entre ces éléments de la protection de la personnalité se présente comme suit : 1

A. Protection constitutionnelle de l'autodétermination en matière d'information au sens de l'art. 13 al. 2 Cst.

L'art. 13 Cst. protège la sphère privée en tant qu'espace de développement et d'épanouissement de la personnalité individuelle. Toute personne, indépendamment de son sexe, de son origine, de son âge, etc., a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. L'art. 13 al. 2 Cst. accorde, en tant qu'aspect particulier du droit à la vie privée, un droit à la protection contre l'utilisation abusive des données personnelles. Selon la jurisprudence, le libellé de l'al. 2 est trop restrictif : la "protection des données relevant des droits fondamentaux" doit en principe couvrir tout traitement de données personnelles par l'État. 2

B. Protection de la personnalité en droit civil

3 Les droits de la personnalité définis aux art. 27 et 28 ss. CC, qui font partie intégrante du droit fondamental de la liberté personnelle de l'art. 10 Cst., reviennent à l'être humain pour lui-même et sont indissociables de sa personne. Le domaine protégé par l'art. 28 CC est majoritairement divisé en trois catégories dans la doctrine : la personnalité physique, la personnalité affective et la personnalité sociale.

- La personnalité physique concerne l'intégrité corporelle et la liberté de mouvement.
- La personnalité affective ou psychique protège le domaine psycho-émotionnel de la vie d'une personne.
- La protection sociale de la personnalité contribue à l'organisation harmonieuse des relations sociales et sociétales et protège tous les biens auxquels une personne doit avoir droit pour lui permettre de vivre harmonieusement dans la société : Il s'agit notamment du droit au nom, du droit à l'honneur, du droit à l'image, de la protection des données, de la liberté économique et du droit au respect et à la considération de la vie privée.

4 Les dispositions fondamentales pour la protection de droit privé des articles 27 et suivants du Code civil sont applicables. CC s'appliquent lorsqu'une atteinte à la personnalité a été commise par une autre personne privée et que le cas ne peut pas être réglé par une norme spéciale du droit privé. Un schéma d'examen en deux étapes est ensuite déduit de l'art. 28 CC :

- Dans un premier temps, on examine s'il y a une atteinte à la personnalité.
- Ensuite, dans un deuxième temps, il faut examiner s'il existe un motif justificatif de l'art. 28 al. 2 CC pour que l'atteinte puisse être considérée comme non illicite. Si toutefois, après l'examen de l'art. 28 al. 2 CC, il n'existe pas de motif justificatif, on parle d'atteinte illicite à la personnalité.

II. PROTECTION DE LA PERSONNALITÉ EN VERTU DU DROIT DE LA PROTECTION DES DONNÉES

A. Genèse de l'art. 1 LPD

L'art. 1 LPD a été repris tel quel de l'ancienne LPD, bien que, du moins lors de la procédure de consultation, plusieurs parties aient exprimé le souhait que, par analogie avec l'art. 1 RGPD, les flux transfrontières de données et la protection de la compétitivité soient également inclus dans les finalités de la LPD. Cette disposition n'a toutefois pas été contestée lors des débats parlementaires. 5

B. Finalité de la LPD

La LPD, tout comme les lois cantonales (sur l'information et la protection des données), stipulent dans leurs finalités que la protection des données ne doit pas être comprise comme une fin en soi, mais comme un instrument visant à préserver les droits fondamentaux ou à protéger la personnalité des personnes physiques dont les données sont traitées - les données des personnes morales ne sont plus couvertes par la LPD (voir à ce sujet OK-Husi-Stämpfli, art. 2, n. 12). 6

Dans cette conception, le droit suisse de la protection des données se distingue clairement du RGPD qui, outre la protection de la personnalité, désigne également la libre circulation des données comme l'objectif du règlement. En d'autres termes, le droit suisse de la protection des données est justement la protection de la personnalité avant tout, et non la protection des acteurs économiques, de la sécurité publique ou d'autres intérêts. 7

La protection de la personnalité vise en premier lieu le traitement des données par des personnes privées, la protection des droits fondamentaux vise la protection contre les ingérences des autorités publiques. Compte tenu du fait que, d'un point de vue constitutionnel, la protection de la personnalité est une conséquence du devoir de protection de l'Etat ou du devoir de réaliser les droits fondamentaux non seulement par l'Etat, mais aussi entre les particuliers (art. 35 al. 3 Cst.), il aurait été plus logique, d'un point de vue légal, de mentionner d'abord la protection des droits fondamentaux, puis la protection de la personnalité. 8

9 Les "droits fondamentaux" mentionnés à l'art. 1 LPD ne comprennent d'ailleurs pas seulement l'art. 13 al. 2 Cst. ou l'art. 8 CEDH. Il faut plutôt comprendre l'art. 1 LPD comme englobant tous les droits fondamentaux susceptibles d'être touchés par le traitement des données, comme par exemple la liberté d'opinion, l'interdiction de discrimination, etc. L'action de l'Etat ne doit pas seulement être conforme à la LPD, mais aussi aux droits fondamentaux (art. 36 Cst.).

C. Nature juridique de l'art. 1 LPD

10 L'art. 1 LPD est une disposition programmatique : elle ne fonde pas de droits ni d'obligations, mais doit être comprise comme une ligne directrice pour l'interprétation des dispositions suivantes.

Dans ce commentaire, l'auteur donne son appréciation personnelle.

BIBLIOGRAPHIE

Fey Marco, Kommentierung zu Art. 1 DSG, in: Baeriswyl Bruno/Pärli Kurt/ Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Biaggini Giovanni, Kommentar zur Bundesverfassung der Schweizerischen Eidgenossenschaft, 2. Aufl., Zürich 2017.

Maurer-Lambrou Urs/ Kunz Simon, Kommentierung zu Art. 1 DSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz / Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014.

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 2 LPD

Un commentaire de Sandra Husi-Stämpfli

PROPOSITION DE CITATION

Sandra Husi-Stämpfli, Kommentierung zu Art. 2 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Husi-Stämpfli, N. XXX zu Art. 2 DSG.

Art. 2 Champ d'application à raison de la personne et de la matière

[1] La présente loi régit le traitement de données personnelles concernant des personnes physiques effectué par:

a. des personnes privées;

b. des organes fédéraux.

[2] Elle ne s'applique pas:

a. aux traitements de données personnelles effectués par une personne physique pour un usage exclusivement personnel;

b. aux traitements de données personnelles effectués par les Chambres fédérales et les commissions parlementaires dans le cadre de leurs délibérations;

c. aux traitements de données personnelles effectués par les bénéficiaires institutionnels au sens de l'art. 2, al. 1, de la loi du 22 juin 2007 sur l'État hôte qui jouissent en Suisse de l'immunité de juridiction.

[3] Les traitements de données personnelles effectués dans le cadre de procédures devant des tribunaux ou dans le cadre de procédures régies par des dispositions fédérales de procédure, ainsi que les droits des personnes concernées, obéissent au droit de procédure applicable. La présente loi s'applique aux procédures administratives de première instance.

[4] Les registres publics relatifs aux rapports de droit privé, notamment l'accès à ces registres et les droits des personnes concernées, sont régis par les dispositions spéciales du droit fédéral applicable. À défaut la présente loi s'applique.

TABLE DES MATIÈRES

En bref 24
I. Généralités 24
A. But de la norme 24
B. Compétence de réglementation 24
II. Champ d'application personnel (art. 2 al. 1 LPD) 26
III. Champ d'application matériel : données relatives aux personnes physiques 26
IV. Exceptions 26
A. Utilisation à des fins privées (art. 2 al. 2 let. a LPD) 27
B. Traitement par les Chambres fédérales et les commissions parlementaires (art. 2 al. 2 let. b LPD) 27
C. Traitements de données par des représentations diplomatiques et des organisations internationales (art. 2 al. 2 let. c LPD) 27
D. Procédures judiciaires ou fédérales en cours (art. 2 al. 3 LPD) 28
E. Registres publics des relations juridiques privées 29
Bibliographie 30

EN BREF

La LPD s'applique au traitement des données des personnes physiques par les organes fédéraux et les personnes privées. La LPD ne s'applique toutefois pas de manière absolue : certains cas, notamment les traitements de données effectués exclusivement à des fins personnelles ou dans le cadre d'une procédure judiciaire ou fédérale en cours, sont exclus de la LPD ou sont régis par des dispositions (de procédure) spécifiques séparées.

I. GÉNÉRALITÉS

A. But de la norme

1 L'article 2 LPD définit le champ d'application de la loi fédérale sur la protection des données ainsi que les exceptions correspondantes. Le champ d'application de la LPD a été partiellement élargi lors de la révision, notamment pour répondre aux exigences de la CCE 108+ : Ainsi, les exceptions relatives aux procès civils en cours, aux procédures pénales, aux procédures d'entraide judiciaire internationale ainsi qu'aux procédures de droit public et administratif (art. 2 al. 2 let. c LPD) et celle concernant les registres publics des relations juridiques privées (art. 2 al. 2 let. d LPD) ont été adaptées.

B. Compétence de réglementation

2 La compétence de réglementer le droit de la protection des données découle de la répartition générale des compétences au niveau fédéral : selon les art. 3 et 42 Cst., la Confédération dispose d'une habilitation individuelle limitée, tandis que les cantons exercent toutes les tâches qui ne sont pas déléguées à la Confédération.

3 La Confédération est ainsi habilitée à réglementer également le traitement des données dans les domaines où elle est en principe habilitée à légiférer - notamment dans le cadre de l'organisation et de la procédure des autorités fédérales (art. 164 ch. 1 let. g Cst.). Le préambule de la LPD se réfère aux art. 95 ("Activité économique lucrative privée"), 122 ("Droit civil") et 173 al. 2 Cst. ("Autres tâches et compétences"). Même si ces articles ne mentionnent pas expressément la compétence de la Confédération dans le domaine de la

protection des données, il est incontestable qu'ils incluent les compétences pour édicter des dispositions légales en matière de protection des données.

La question de savoir si le traitement de données personnelles satisfait aux conditions de la protection des données est déterminée, d'une part, par les dispositions des lois (sur l'information et la protection des données) (droit "général" de la protection des données) et, d'autre part, par les dispositions des lois spéciales qui règlent le traitement des données dans les cas d'application concrets (droit "spécial" de la protection des données). 4

Dans un premier temps, les organes publics et les personnes privées doivent s'orienter vers le droit "général" de la protection des données lorsqu'ils souhaitent traiter des données personnelles : 5

- Les organes fédéraux et les personnes privées doivent s'orienter vers les directives de traitement de la loi fédérale sur la protection des données.
- Si des organes publics cantonaux traitent des données personnelles, ils doivent se conformer aux lois cantonales (sur l'information et la protection des données).

Le droit "général" de la protection des données règle - au niveau cantonal et fédéral - entre autres les thèmes suivants : Objectif de la loi, champ d'application, définitions, principes de traitement, règles de responsabilité, droits des personnes concernées, etc. Conformément à sa nature de législation fondamentale, le droit "général" de la protection des données contient généralement aussi des dispositions d'exception qui définissent les cas dans lesquels les dispositions de droit spécial priment. 6

Dans un deuxième temps, les organes publics doivent vérifier s'ils sont autorisés à traiter les données personnelles en question dans le cadre de l'accomplissement de leurs tâches légales, c'est-à-dire si les lois sectorielles respectives (le droit "spécial" de la protection des données, spécifique à un domaine) règlent spécifiquement le traitement des données. 7

Le droit spécifique ou le droit "particulier" de la protection des données doit satisfaire aux exigences du droit général de la protection des données et fixer, outre la finalité du traitement (c'est-à-dire la tâche concrète pour l'accomplissement de laquelle des données personnelles doivent être traitées), entre autres les responsabilités et les éventuelles conditions de la communication. 8

9 De leur côté, les personnes privées doivent s'assurer dans cette deuxième étape qu'elles disposent d'un motif justificatif pour le traitement de données en question, dans la mesure où le traitement porte atteinte aux droits de la personnalité.

II. CHAMP D'APPLICATION PERSONNEL (ART. 2 AL. 1 LPD)

10 Le droit fédéral de la protection des données s'applique au traitement de données de personnes physiques par des organes fédéraux (à ce sujet, n. 11 commentaire de l'art. 5 let. i et OK-Zysset art. 34 LPD) et par des personnes privées (à ce sujet, OK-dal Molin ad art. 30 LPD). La loi cantonale respective (sur l'information et la protection des données) s'applique au traitement de données personnelles par les organes publics cantonaux (à ce sujet, n. 5).

III. CHAMP D'APPLICATION MATÉRIEL : DONNÉES RELATIVES AUX PERSONNES PHYSIQUES

11 Est considéré comme personne physique au sens juridique tout être humain, et tout être humain a la capacité juridique (art. 11 al. 1 CC). Tout être humain possède donc la capacité d'avoir des droits et des obligations (art. 11, al. 2, CC) - parmi ces droits figure le droit de la personnalité, tant du point de vue du droit civil que du point de vue du droit de la protection des données (art. 28 ss CC ou art. 1 en particulier en relation avec l'art. 30 LPD et l'art. 34 LPD).

12 La dernière révision de la protection des données a restreint le champ d'application matériel : Les données des personnes morales ne sont plus couvertes par la LPD, ce qui est de toute façon insignifiant dans la pratique, car les personnes morales peuvent toujours porter atteinte à leur personnalité sur la base des art. 28 et suivants LPD. CC (comme par exemple les atteintes à la réputation). Elles bénéficient en outre de la protection de la loi fédérale contre la concurrence déloyale, de la loi sur le droit d'auteur ou des dispositions spécifiques relatives aux secrets professionnels, d'affaires ou de fabrication.

IV. EXCEPTIONS

13 La LPD ne s'applique pas de manière absolue. L'art. 2 al. 2-4 LPD mentionne diverses exceptions pour lesquelles la LPD ne s'applique pas.

A. Utilisation à des fins privées (art. 2 al. 2 let. a LPD)

La LPD ne s'applique pas lorsque les données personnelles en question sont traitées par une personne physique exclusivement pour son usage personnel (art. 2 al. 2 let. a LPD). On peut citer comme exemple la collection de lettres ou de courriels qu'un couple s'est échangés pendant des années et qui contiennent également des remarques et des anecdotes sur d'autres personnes. Les albums photos privés contenant des photos de fêtes de famille, de vacances, etc. ne sont pas non plus soumis à la LPD, pour autant que les photos ne soient pas diffusées (par exemple numérisées et publiées). 14

B. Traitement par les Chambres fédérales et les commissions parlementaires (art. 2 al. 2 let. b LPD)

Les données personnelles sont traitées par les Chambres fédérales et les commissions parlementaires dans le cadre de leurs délibérations (art. 2 al. 2 let. b LPD). Cette disposition a été reprise telle quelle de l'ancienne LPD. Selon le message, l'exception à la LPD se justifie par le fait que le Parlement ne pourrait pas assumer ses tâches constitutionnelles s'il devait dans tous les cas respecter les principes de protection des données - le message mentionne ici explicitement les prescriptions relatives à la communication de données personnelles. L'argumentation selon laquelle le droit spécial qui régit le déroulement des affaires des Chambres (le "droit spécial de la protection des données") contient des détails sur le traitement des informations (et donc des données personnelles), raison pour laquelle un assujettissement à la LPD n'est tout simplement pas nécessaire, semble toutefois beaucoup plus plausible. 15

C. Traitements de données par des représentations diplomatiques et des organisations internationales (art. 2 al. 2 let. c LPD)

Les traitements effectués par une représentation diplomatique ou consulaire d'un autre Etat ou par une organisation internationale ne sont pas non plus couverts par la LPD. En d'autres termes, cette exception concerne les bénéficiaires institutionnels visés à l'art. 2 al. 1 de la loi sur l'Etat hôte du 22 juin 2007, qui bénéficient en Suisse de l'immunité de juridiction : ils jouissent, en vertu du droit international public et de la LEIS, de l'indépendance et de la liberté d'action nécessaires à l'accomplissement de leurs fonctions 16

internationales ; on ne peut donc pas attendre d'eux qu'ils se soumettent aux règles du droit suisse en ce qui concerne les données traitées par leurs représentations diplomatiques ou consulaires.

D. Procédures judiciaires ou fédérales en cours (art. 2 al. 3 LPD)

17 La LPD ne s'applique pas non plus aux procédures judiciaires ou fédérales en cours, car celles-ci sont régies par le droit de procédure correspondant, qui contient des prescriptions détaillées sur le traitement des données personnelles (des parties, des plaignants, etc.).

18 La notion de "procédures judiciaires" englobe toutes les procédures devant les tribunaux pénaux, civils et administratifs cantonaux et fédéraux, mais aussi devant les tribunaux arbitraux ayant leur siège en Suisse. Contrairement à l'aLPD, l'art. 2 al. 3 LPD renonce à la notion de procédure pendante, car seule la procédure civile parle de litispendance et cette notion a parfois posé des problèmes de délimitation.

19 Désormais, le seul critère déterminant est de savoir si une procédure se déroule devant un tribunal ou si elle est régie par un code de procédure fédéral. Une procédure a lieu devant un tribunal lorsque celui-ci est saisi pour la première fois d'une affaire par l'introduction de la procédure selon le règlement de procédure déterminant. Une procédure est régie par des règles de procédure fédérales dès lors qu'une situation donnée est traitée par une autorité conformément aux dispositions de l'une de ces lois.

Parmi les codes de procédure fédéraux qui contiennent des prescriptions sur le traitement des données personnelles ou sur les droits des personnes concernées dans le cadre de ces procédures, on trouve notamment 20

- la loi fédérale sur la procédure administrative du 20 décembre 1968 (PA, dans la mesure où il ne s'agit pas de la procédure administrative de première instance),
- le code de procédure civile du 19 décembre 2008 (CPC),
- la loi fédérale du 11 avril 1889 sur la poursuite pour dettes et la faillite (LP),
- le code de procédure pénale du 5 octobre 2007 (CPP),
- la loi fédérale sur le droit pénal administratif du 22 mars 1974 (DPA) ou encore
- la loi fédérale sur l'entraide internationale en matière pénale du 20 mars 1981 (EIMP).

Les traitements de données effectués par les services administratifs des tribunaux et des autorités n'entrent pas dans le champ d'application du droit de procédure correspondant, de sorte que l'art. 2 al. 3 LPD ne s'applique pas. 21

En règle générale, le code de procédure déterminant reste applicable même après la clôture de la procédure : Des dispositions particulières s'appliquent par exemple à la gestion du dossier, à la consultation du dossier, à la rectification ou à la conservation du dossier. Il n'est toutefois pas exclu que le droit de procédure applicable déclare la LPD applicable après la clôture de la procédure (cf. art. 99 CPP). 22

E. Registres publics des relations juridiques privées

Enfin, les traitements de données effectués dans le cadre des registres publics des relations juridiques privées, qui sont tenus en vertu du droit fédéral et par des organes fédéraux, sont exclus du champ d'application de la LPD. Dans ce 23

cas, c'est le droit spécial qui s'applique. Parmi ces registres, on compte notamment

- le registre d'état civil électronique Zefix,
- le registre des aéronefs de l'Office fédéral de l'aviation civile et
- les registres de l'Institut fédéral de la propriété intellectuelle (notamment le registre des marques, le registre des brevets et le registre des designs).

24 Les registres publics des relations juridiques privées, pour lesquels les cantons sont compétents, sont soumis au droit cantonal de la protection des données. Parmi les registres cantonaux, on compte par ex.

- le registre foncier,
- le registre des bateaux,
- les registres du commerce et
- les registres des poursuites et des faillites.

Dans ce commentaire, l'auteur donne son appréciation personnelle.

BIBLIOGRAPHIE

Rudin Beat, Kommentierung zu Art. 2 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Rudin Beat/Husi-Stämpfli Sandra, Kommentierung zu Art. 37 DSG, in: Maurer-Lambrou Urs/Blectha Gabor-Paul (Hrsg.), Datenschutzgesetz / Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014.

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 3 LPD

Un commentaire de Sandra Husi-Stämpfli

PROPOSITION DE CITATION

Sandra Husi-Stämpfli, Kommentierung zu Art. 3 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Husi-Stämpfli, N. XXX zu Art. 3 DSG.

Art. 3 Champ d'application territorial

[1] La présente loi s'applique aux états de fait qui déploient des effets en Suisse, même s'ils se sont produits à l'étranger.

[2] Les prétentions de droit privé sont régies par la loi fédérale du 18 décembre 1987 sur le droit international privé. Sont également réservées les dispositions régissant le champ d'application territorial du code pénal.

TABLE DES MATIÈRES

En bref 33
I. Généralités 33
A. Contexte et objectif de la norme 33
B. Historique 33
II. Applicabilité de la LPD selon le principe des effets (art. 3 al. 1 LPD) 34
III. Règles de conflit de lois dans les opérations de traitement de données de droit privé (art. 3 al. 2 LPD) 34
IV. règles de conflit de lois pénales (art. 3 al. 2 LPD) 35
Bibliographie 35

EN BREF

L'article 3 LPD consacre le principe dit des "effets", selon lequel les dispositions de la LPD s'appliquent lorsque les opérations de traitement des données concernées sont "perceptibles" en Suisse. Ainsi, le champ d'application de la LPD ne concerne pas uniquement les opérations de traitement de données purement "suisses", mais également les constellations dans lesquelles un traitement de données est initié à l'étranger, mais dont les conséquences se font sentir en Suisse.

I. GÉNÉRALITÉS

A. Contexte et objectif de la norme

Le droit public ne connaît pas de règles de conflit de lois codifiées, contrairement au droit privé et au droit pénal. Dans la pratique, c'est donc le principe de territorialité qui s'applique en principe aux situations transfrontalières de droit public : Le droit public suisse s'applique toujours lorsqu'une situation se déroule en Suisse. 1

Parmi les critères utilisés pour déterminer le droit applicable, on trouve notamment le domicile ou le lieu de séjour, le lieu d'activité ou le lieu des effets. Selon la jurisprudence du Tribunal fédéral, le principe dit des effets constitue une "expression spéciale" du principe de territorialité : Les faits qui se sont produits à l'étranger peuvent être pris en compte par les autorités suisses s'ils ont "un impact suffisant sur le territoire suisse". Toutefois, la pratique ne définit pas de manière uniforme ce qui constitue un lien suffisant avec la Suisse au sens du principe de l'impact : en général, il est nécessaire que l'impact soit sensible, important, significatif ou considérable. 2

L'article 3 LPD règle l'application locale de la LPD conformément aux principes généraux d'application du droit public et notamment au principe des effets. 3

B. Historique

L'ancienne LPD ne contenait aucune disposition relative au champ d'application local, pas plus que le projet de nouvelle LPD. Dans le cadre des 4

débats parlementaires, il a toutefois été demandé d'introduire une disposition sur le champ d'application territorial - qui correspondrait idéalement à l'art. 3 al. 1 et 2 RGPD. Selon cette disposition, la LPD aurait également dû s'appliquer lorsqu'un responsable du traitement ou un sous-traitant ayant un établissement en dehors de la Suisse traite des données de personnes en Suisse afin de leur proposer des biens ou des services (à titre onéreux ou gratuit) ou d'observer leur comportement en Suisse.

5 Compte tenu des règles de conflit de lois déjà existantes, notamment en droit privé, le législateur est arrivé à la conclusion, lors des délibérations, qu'une inscription du principe des effets défini par la jurisprudence ainsi qu'un renvoi explicite aux dispositions de la loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (EIMP, RS 351.1) ou du droit pénal permettraient de tenir suffisamment compte des préoccupations des personnes concernées par un traitement (international) de données. En conséquence, la réglementation discutée par analogie avec l'art. 3 al. 1 et 2 du DSGVO a été abandonnée.

II. APPLICABILITÉ DE LA LPD SELON LE PRINCIPE DES EFFETS (ART. 3 AL. 1 LPD)

6 En vertu du principe de l'effet, les dispositions de la LPD s'appliquent lorsque les opérations de traitement des données concernées ont un impact en Suisse. Ainsi, le champ d'application de la LPD ne concerne pas uniquement les opérations de traitement de données purement "suisses", mais également les constellations dans lesquelles un traitement de données est initié à l'étranger, mais dont les conséquences sont "perceptibles" en Suisse.

III. RÈGLES DE CONFLIT DE LOIS DANS LES OPÉRATIONS DE TRAITEMENT DE DONNÉES DE DROIT PRIVÉ (ART. 3 AL. 2 LPD)

7 Dans le contexte du droit privé, la LDIP règle quel droit est applicable aux tribunaux suisses dans les relations internationales ; dans le contexte du droit de la protection des données, il convient de tenir compte de l'art. 139 al. 1 LDIP. Selon cette disposition, la personne lésée dispose d'un large droit de

choix quant au droit applicable à son cas. Concrètement, la personne lésée a la possibilité de décider si le droit de l'Etat s'applique,

- dans lequel elle a sa résidence habituelle (al. 1 let. a),
- dans lequel l'auteur de l'atteinte a son établissement ou sa résidence habituelle (al. 1 let. b) ou
- dans lequel le résultat de l'acte de contrefaçon se produit (al. 1 let. c).

La personne lésée a ainsi la possibilité de choisir la loi qui lui est la plus favorable. Afin de préserver cet avantage, la LPD stipule explicitement que la LDIP doit s'appliquer aux prétentions de droit privé. 8

IV. RÈGLES DE CONFLIT DE LOIS PÉNALES (ART. 3 AL. 2 LPD)

Les dispositions pénales de la LPD (art. 60 ss.) font partie du droit pénal accessoire, de sorte que leur application territoriale est déterminée par les principes du CP (cf. art. 333 al. 1 en relation avec l'art. 104 et art. 3 ss. CP) : Selon le principe de protection individuelle ancré dans le CP, est en principe punissable celui qui porte atteinte à l'étranger aux biens juridiques de ressortissants suisses. Au vu de cette règle de conflit déjà existante, la LPD renvoie au code pénal et ne contient pas de directives propres sur le champ d'application territorial dans le contexte du droit pénal. 9

Dans ce commentaire, l'auteur donne son appréciation personnelle.

BIBLIOGRAPHIE

Rudin Beat, Kommentierung zu Art. 3 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl. 2020, Zürich/St. Gallen.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 4 LPD

Un commentaire de Michael Reinle

PROPOSITION DE CITATION

Michael Reinle, Commentaire de l'art. 4 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Reinle, art. 4 LPD N. XXX.

Art. 4 Préposé fédéral à la protection des données et à la transparence

[1] Le Préposé fédéral à la protection des données et à la transparence (PFPDT) est chargé de surveiller la bonne application des dispositions fédérales de protection des données.

[2] Il ne peut exercer aucune surveillance sur:

a. l'Assemblée fédérale;

b. le Conseil fédéral;

c. les tribunaux fédéraux;

d. le Ministère public de la Confédération, en ce qui concerne le traitement de données personnelles dans le cadre de procédures pénales;

e. les autorités fédérales, en ce qui concerne le traitement de données personnelles dans le cadre de leurs activités juridictionnelles ou dans le cadre de procédures d'entraide judiciaire internationale en matière pénale.

TABLE DES MATIÈRES

En bref 40
I. Généralités 40
A. But de la norme et contexte 40
B. Genèse 41
II. Surveillance par le PFPDT 42
A. Surveillance de l'application des dispositions fédérales en matière de protection des données (al. 1) 42
B. Exceptions à la surveillance (al. 2) 43
1. Assemblée fédérale (let. a) 43
2. Conseil fédéral (let. b) 44
3. Tribunaux fédéraux (let. c) 44
4. Ministère public de la Confédération (let. d) 45
5. Autorités fédérales dans l'exercice de leur fonction juridictionnelle ou dans le cadre de procédures d'entraide judiciaire internationale en matière pénale (let. e) 45
Bibliographie 46
Matériaux 47

EN BREF

Le PFPDT surveille l'application des dispositions fédérales en matière de protection des données. Sont soumis à sa surveillance les organes fédéraux ainsi que les personnes physiques et morales privées. Il existe des exceptions à la surveillance des organes fédéraux, fondées sur le principe de la séparation des pouvoirs et visant à garantir l'indépendance de la justice. Cette exception ne signifie pas que les organes fédéraux exemptés ne sont pas tenus de respecter les dispositions de la LPD lors du traitement de données. Les exceptions au champ d'application matériel de la LPD sont réglées à l'art. 2 LPD.

I. GÉNÉRALITÉS

A. But de la norme et contexte

1 La surveillance générale exercée par le PFPDT sur l'application des dispositions fédérales en matière de protection des données ne constitue pas une nouveauté par rapport à l'ancienne LPD (art. 27, al. 1, aDSG). La principale nouveauté réside dans le fait que l'art. 4 LPD mentionne désormais le PFPDT et non plus le préposé, comme c'était le cas à l'art. 27 aDSG. Cela tient au fait que la LPD révisée distingue entre le PFPDT en tant qu'autorité et le préposé en tant que personne chargée par le chef de l'autorité. La notion de préposé n'est toutefois définie qu'à l'art. 43, al. 1, LPD.

2 L'art. 4 LPD tire principalement sa signification des exceptions à la surveillance du PFPDT prévues à l'al. 2. Dans l'ancien droit, seul le Conseil fédéral était soustrait à la surveillance du PFPDT (art. 27, al. 1, aDSG). Dorénavant, l'exception à la surveillance du PFPDT s'applique non seulement au Conseil fédéral, mais aussi à d'autres organes fédéraux. La liste des exceptions à l'art. 4, al. 2, LPD est exhaustive. La LPD ne prévoit aucune exception à la surveillance de l'IPDT sur les personnes privées qui traitent des données.

3 Le Conseil fédéral a été exclu de la surveillance de l'IPDT, car celui-ci ne saurait être l'organe de contrôle de sa propre autorité de surveillance et d'élection.

Les exceptions nouvellement introduites à l'al. 2 pour l'Assemblée fédérale, les tribunaux fédéraux, le Ministère public de la Confédération et d'autres autorités fédérales en cas de traitements spécifiques de données répondent à des considérations similaires. Elles visent à mettre en œuvre le principe de la séparation des pouvoirs et à garantir l'indépendance de la justice. 4

B. Genèse

Dans le projet de révision de la loi sur la protection des données du 29 octobre 2014, la surveillance des organes fédéraux par le PFPDT était certes abordée, mais la question des exceptions à cette surveillance n'avait pas été traitée. 5

L'art. 2, al. 3 et 4, AP-LPD prévoyait des exceptions à la surveillance du PFPDT pour les tribunaux fédéraux (al. 3) et pour le Conseil fédéral et l'Assemblée fédérale (al. 4). L'exception concernant les tribunaux fédéraux était motivée par le fait que le PFPDT devait désormais être habilité, selon l'AP-LPD, à rendre des décisions à l'encontre d'organes de la Confédération. Cela aurait pu porter atteinte à l'indépendance des tribunaux et à la séparation des pouvoirs. En outre, le Tribunal administratif fédéral et le Tribunal fédéral sont les instances de recours contre les décisions du PFPDT. Cela aurait pu conduire à ce que ces deux tribunaux aient dû examiner des décisions du PFPDT les concernant eux-mêmes. 6

En outre, selon l'art. 2, al. 2, let. c, AP-LPD, le traitement de données personnelles par des autorités judiciaires fédérales indépendantes dans le cadre de leur activité juridictionnelle devait être exclu du champ d'application de la LPD et donc aussi du contrôle du PFPDT. Cette exception a également été motivée par le fait que l'assujettissement de ces autorités judiciaires à la surveillance du PFPDT pourrait porter atteinte au principe de la séparation des pouvoirs et à l'indépendance de la justice. 7

L'art. 2, al. 2, let. c, ainsi que les al. 3 et 4 AP-LPD ont été discutés et critiqués lors de la consultation. Il a notamment été critiqué que certaines notions étaient imprécises (« autorités judiciaires indépendantes »), que les exceptions contredisaient la Convention SEV 108, que le PFPDT devait continuer à exercer la surveillance des tribunaux tout en ne pouvant émettre que des recommandations à leur égard, ou encore que les exceptions prévues à l'art. 2, al. 3 et 4, AP-LPD devaient être réglées systématiquement dans la section 8

consacrée au PFPDT et non dans le contexte du champ d'application matériel de la LPD.

9 Les critiques formulées lors de la consultation sur l'AP-LPD ont été prises en compte dans la mesure où le message LPD 2017 a introduit un nouvel art. 3 P-LPD qui traite exclusivement de la surveillance exercée par le PFPDT. Cette décision a permis de séparer la question de la surveillance de celle du champ d'application matériel de la LPD, ce qui est également correct sur le plan dogmatique. Le contenu de l'art. 3 P-LPD correspond sans modification à celui du nouvel art. 4 LPD.

10 L'art. 3 P-LPD et l'art. 4 LPD n'ont pas été discutés lors des délibérations parlementaires. La proposition du Conseil fédéral (art. 3 P-LPD) a été acceptée sans intervention.

II. SURVEILLANCE PAR LE PFPDT

A. Surveillance de l'application des dispositions fédérales en matière de protection des données (al. 1)

11 L'art. 4, al. 1, LPD stipule que le PFPDT est chargé de surveiller l'application des dispositions de droit fédéral en matière de protection des données. Sont soumises à la surveillance du PFPDT les personnes physiques et morales de droit privé ainsi que les organes fédéraux.

12 L'expression « dispositions de droit fédéral en matière de protection des données » souligne que le PFPDT ne surveille pas uniquement l'application des dispositions de la LPD. Comme à l'art. 27, al. 1, aDSG, le PFPDT surveille également, en vertu de l'art. 4, al. 1, LPD, les dispositions spécifiques de la Confédération en matière de protection des données. Il s'agit des dispositions relatives à la protection des données contenues dans d'autres actes législatifs fédéraux ainsi que des traités internationaux spécifiques à la protection des données.

13 La question de la surveillance des organes fédéraux par le PFPDT doit être distinguée de l'application matérielle de la LPD aux traitements concrets de données effectués par les organes fédéraux. Les organes fédéraux peuvent être soumis à la surveillance du PFPDT même si certains de leurs traitements de données sont exclus du champ d'application de la LPD en vertu de l'art. 2

LPD. Inversement, certains organes fédéraux peuvent être exemptés de la surveillance du PFPDT (art. 4, al. 2, LPD), même si leurs traitements de données ne sont pas exclus du champ d'application matériel de la LPD en vertu de l'art. 2 LPD. C'est le cas, par exemple, du Conseil fédéral. Celui-ci est exclu du champ de la surveillance du PFPDT en vertu de l'art. 4, al. 2, let. b, LPD, mais il doit respecter la LPD pour certains traitements de données. Il en va de même pour l'Assemblée fédérale. Celle-ci est désormais exclue du champ de la surveillance. En vertu de l'art. 2, al. 2, let. b, LPD, certains traitements de données effectués par l'Assemblée fédérale sont également exclus du champ d'application matériel de la LPD, mais pas tous.

B. Exceptions à la surveillance (al. 2)

1. Assemblée fédérale (let. a)

L'Assemblée fédérale est exclue de la surveillance du PFPDT, car sinon le principe de la séparation des pouvoirs pourrait être compromis. 14

En ce qui concerne l'exception à la surveillance du PFPDT dont bénéficie l'Assemblée fédérale, la question se pose de savoir jusqu'où s'étend cette exception. Les travaux préparatoires ne se prononcent pas sur cette question. 15

Au regard de l'art. 2, al. 2, let. b, LPD, il est frappant de constater que le législateur, lorsqu'il mentionne le Parlement, fait une distinction entre l'Assemblée fédérale, les conseils fédéraux et les commissions parlementaires. Cela semble indiquer que l'Assemblée fédérale désigne le collège au sens de l'art. 148 Cst. Selon l'art. 148, al. 2, Cst., l'Assemblée fédérale comprend le Conseil national et le Conseil des États. Par conséquent, l'Assemblée fédérale ne devrait pas désigner uniquement l'Assemblée fédérale réunie en tant qu'organe spécifique, mais aussi le Conseil national, le Conseil des États et l'Assemblée fédérale réunie. 16

Il n'est pas clair si les commissions parlementaires et les services parlementaires sont également exemptés de la surveillance du PFPDT. Les délibérations des commissions parlementaires sont exemptées de la LPD (art. 2, al. 2, let. b, LPD). Cette exception ne s'applique toutefois qu'aux délibérations elles-mêmes et non, par exemple, aux rapports sur ces délibérations ou aux publications. Au vu des motifs qui ont justifié l'exception faite à l'Assemblée fédérale, il serait toutefois judicieux d'exclire également les 17

commissions parlementaires de la surveillance du PFPDT. En ce qui concerne les services du Parlement, il est déterminant de savoir si le traitement des données est en relation directe avec l'activité parlementaire. Les traitements qui ne sont pas en relation directe avec l'activité parlementaire sont soumis à la surveillance du PFPDT.

2. Conseil fédéral (let. b)

18 Selon le message, le Conseil fédéral a été exempté de la surveillance du PFPDT, car cela pourrait porter atteinte au principe de la séparation des pouvoirs.

19 Le Conseil fédéral désigne ici le collège. Les départements et la Chancellerie fédérale sont en revanche soumis à la surveillance du PFPDT.

20 L'exception du Conseil fédéral à la surveillance du PFPDT était justifiée à l'art. 27, al. 1, aDSG par le fait que l'organe électoral du préposé ne devait pas être soumis à sa surveillance. Désormais, le préposé est toutefois élu par l'Assemblée fédérale (art. 43 s. LPD). L'art. 39 P-LPD prévoyait en outre que le préposé était nommé par le Conseil fédéral, sous réserve d'approbation par l'Assemblée fédérale. L'art. 3, al. 2, P-LPD soustrayait donc tant le Conseil fédéral que l'Assemblée fédérale à la surveillance. Au Conseil national, une majorité s'est toutefois prononcée en faveur d'une élection par l'Assemblée fédérale réunie et non plus par le Conseil fédéral. Le Conseil des États s'est rallié à cette décision. Étant donné que le Conseil fédéral n'est désormais plus l'organe de nomination du préposé, il n'y a plus de raison que le Conseil fédéral continue d'être exempté de la surveillance du PFPDT. Le fait que le Conseil fédéral reste soustrait à la surveillance du PFPDT en vertu de l'art. 4, al. 2, let. b, LPD tient sans doute au fait que le Parlement avait adopté l'art. 3 P-LPD avant de se pencher sur la question de l'élection du préposé.

3. Tribunaux fédéraux (let. c)

21 Les tribunaux fédéraux sont exemptés de la surveillance du PFPDT, car sinon la séparation des pouvoirs et l'indépendance de la justice pourraient être compromises. En effet, le PFPDT est désormais habilité à rendre des décisions à l'encontre d'organes fédéraux (art. 51 LPD). De plus, le Tribunal administratif fédéral et le Tribunal fédéral sont les instances de recours contre les décisions du PFPDT. Sans cette exception, elles devraient statuer en tant qu'instance de recours sur les décisions du PFPDT qui les concernent.

Afin de satisfaire aux exigences de la directive (UE) 2016/680 et de l'E-OEP 108, les tribunaux fédéraux doivent mettre en place leur propre autorité de surveillance indépendante en matière de protection des données. Cette autorité de surveillance doit être conçue de manière analogue au PFPDT, pour autant que les circonstances concrètes ne nécessitent pas de dérogations. 22

4. Ministère public de la Confédération (let. d)

Le Ministère public de la Confédération n'est exclu de la surveillance du PFPDT que lorsqu'il traite des données personnelles dans le cadre de procédures pénales. Pour les autres traitements de données (p. ex. dans le domaine du personnel), le Ministère public de la Confédération est soumis à la surveillance du PFPDT. Cette exception se justifie également par la séparation des pouvoirs et l'indépendance de la justice. 23

Les autorités fédérales de police restent soumises à la surveillance du PFPDT, même lorsqu'elles agissent sur mandat du Ministère public de la Confédération. Le PFPDT applique les dispositions en matière de protection des données du droit procédural applicable (art. 2, al. 3, LPD). 24

5. Autorités fédérales dans l'exercice de leur fonction juridictionnelle ou dans le cadre de procédures d'entraide judiciaire internationale en matière pénale (let. e)

Cette exception est également justifiée par le principe de la séparation des pouvoirs et de l'indépendance de la justice. 25

En outre, lors des travaux législatifs, l'exception a été justifiée par le fait que les droits des parties et des personnes impliquées dans la procédure sont régis par le droit procédural, qui leur offre une protection équivalente à celle prévue par la LPD. 26

Ne sont pas concernés par l'exception et sont donc soumis à la surveillance du PFPDT les traitements de données qui n'ont pas de lien concret avec l'activité juridictionnelle ou les procédures d'entraide internationale en matière pénale. Sont donc soumis à la surveillance du PFPDT les traitements de données effectués par les services administratifs de ces autorités, tels que le traitement de données relatives au personnel. 27

28 La notion d'activité juridictionnelle remplace celle de « procédure pendante » à l'art. 2, al. 2, let. c, aDSG.

29 L'exception concerne principalement le Ministère public de la Confédération et l'Office fédéral de la justice. Selon la déclaration du Conseil fédéral relative à l'article 1 de la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959, l'Office fédéral de la justice doit être considéré comme une autorité judiciaire suisse au sens de la convention. L'exception a toutefois une portée limitée. Le PFPDT peut contrôler la licéité d'un traitement de données lorsqu'une personne concernée fait valoir ses droits au sens de l'art. 11c E-EIMP.

30 Les traitements de données effectués par les autorités fédérales dans le cadre d'une procédure pénale administrative ne tombent pas sous le coup de cette exception.

BIBLIOGRAPHIE

Baeriswyl Bruno, Kommentierung zu Art. 4 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2022.

Drechsler Christian, Kommentierung zu Art. 2 DSG, in: Blechta Gabor-Paul/Vasella David (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, 4. Aufl., Basel 2024.

Huber René, Kommentierung zu Art. 4 DSG, in: Blechta Gabor-Paul/Vasella David (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, 4. Aufl., Basel 2024.

Jöhri Yvonne, Kommentierung zu Art. 27 aDSG, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Rosenthal David, Kommentierung zu Art. 2 aDSG, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Rudin Beat, Kommentierung zu Art. 2 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2022.

Waldmann Bernhard/Bickel Jürg, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht – Grundlagen und öffentliches Recht, Bern 2011.

Waldmann Bernhard/Oeschger Magnus, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht – Grundlagen und öffentliches Recht, Bern 2011.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBI 2017 S. 6941 ff., abrufbar unter https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2017/2057/de/pdf-x/fedlex-data-admin-ch-eli-fga-2017-2057-de-pdf-x.pdf, besucht am 30.3.2023.

Botschaft zum Bundesgesetz über den Datenschutz vom 23.3.1988, BBI 1988 II S. 413 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/de, besucht am 30.3.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 5 let. c LPD

Un commentaire de Franziska Sprecher

PROPOSITION DE CITATION

Franziska Sprecher, Commentaire de l'art. 5 let. c LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Sprecher, art. 5 let. c LPD N. XXX.

Chapitre 2 Dispositions générales

Section 1 Définitions et principes généraux

Art. 5 Définitions

On entend par:

c. *données personnelles sensibles (données sensibles):*

les données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales,
les données sur la santé, la sphère intime ou l'origine raciale ou ethnique,
les données génétiques,
les données biométriques identifiant une personne physique de manière univoque,

les données sur des poursuites ou sanctions pénales et administratives,
les données sur des mesures d'aide sociale;

TABLE DES MATIÈRES

En bref 52
I. Généralités 52
A. But de la norme et contexte 52
B. Historique 53
II. Données personnelles sensibles en général 53
III. Données relatives aux opinions ou activités religieuses, philosophiques, politiques ou syndicales (ch. 1) 54
IV. Données relatives à la santé, à la sphère intime ou à l'appartenance à une race ou à une ethnie (ch. 2) 55
V. Données génétiques (ch. 3) 58
VI. Données biométriques permettant d'identifier de manière unique une personne physique (ch. 4) 59
VII. Données relatives aux poursuites ou sanctions administratives ou pénales (ch. 5) 60
VIII. Données relatives aux mesures d'aide sociale (ch. 6) 60
Bibliographie 61
Matériaux 63

EN BREF

Les données personnelles sensibles constituent une sous-catégorie spécifique de données personnelles dont le traitement est soumis à une protection particulière en raison du risque accru de discrimination ou de stigmatisation. Leur traitement n'est autorisé que dans des conditions juridiques strictes, par exemple en présence d'un consentement explicite, après réalisation d'une analyse d'impact préalable relative à la protection des données ou sur la base d'une loi formelle en cas de traitement par une autorité.

I. GÉNÉRALITÉS

1 Les données personnelles sensibles constituent une **sous-catégorie privilégiée des données personnelles** (art. 5, let. a, LPD). Elles sont considérées comme particulièrement sensibles au regard de la protection des droits fondamentaux et de la personnalité des personnes concernées (risque de discrimination ou de stigmatisation en raison de ces caractéristiques) (cf. N. 6 ss). L'art. 5, let. c, LPD énumère *de manière exhaustive* les catégories de données personnelles sensibles. Sous réserve de dispositions légales spéciales, les données personnelles sensibles sont couvertes partout où la loi fait référence aux données personnelles.

2 Le législateur subordonne l'**admissibilité du traitement** de ce type privilégié de données personnelles à des conditions particulières. Il impose ainsi des exigences plus strictes pour le consentement au traitement de données personnelles sensibles. Celui-ci doit notamment être donné *de manière expresse* (par exemple, art. 6, al. 7, let. a, LPD). Il existe en outre l'obligation de procéder à une *analyse d'impact relative à la protection des données* (p. ex. art. 22, al. 2, let. a, LPD). Les organes de la Confédération ont besoin d'une *base légale au sens formel* pour traiter des données personnelles sensibles (art. 34, al. 2, let. a, LPD).

A. But de la norme et contexte

3 En créant les *catégories abstraites et formelles* des données personnelles sensibles, le législateur part du principe qu'il existe certains types ou catégories de données qui sont particulièrement sensibles en raison de leur lien étroit avec la sphère privée ou la vie privée d'une personne. La

sensibilité de ces données s'accompagne d'un risque particulier pour les droits de la personnalité des personnes concernées (par exemple, risque de stigmatisation en raison de leurs caractéristiques), ce qui rend ces données particulièrement dignes de protection. Cette opinion est partagée par la LPD, la Convention 108+ (art. 6), la directive 2016/680 (art. 10) et le DSGVO (art. 9).

B. Historique

La catégorie des données personnelles particulièrement sensibles figurait déjà dans aDSG (art. 3, let. c, aDSG) et, selon la volonté du Conseil fédéral, elle devait être maintenue après la révision totale de la LPD. Dans le cadre de la révision, le Conseil fédéral a estimé que la protection des « données personnelles sensibles » était essentielle « pour le maintien de la décision d'adéquation de l'UE » et a souligné que « le catalogue du Conseil fédéral [...] répondait donc aux exigences minimales de la Convention 108 plus sur la protection des données et de la directive européenne relative à la protection des données dans le domaine pénal ». 4

Les tentatives visant à réduire le catalogue existant sous l'aDSG ont échoué lors des délibérations parlementaires (cf. N. 12, N. 32). Au contraire, dans le cadre de la révision totale de la LPD, la notion de données personnelles sensibles a été étendue aux **données génétiques** et **biométriques** qui identifient clairement un individu, ainsi qu'aux **données relatives à l'origine ethnique**, alignant ainsi la LPD sur l'art. 6, al. 1, de la Convention 108+ et à l'art. 10 de la directive UE 2016/680. 5

II. DONNÉES PERSONNELLES SENSIBLES EN GÉNÉRAL

Les données personnelles sensibles sont **formellement et abstraitement catégorisées** dans la LPD. Le législateur part du principe que les données personnelles désignées comme particulièrement sensibles à l'art. 5, let. c, LPD touchent particulièrement les droits de la personnalité de la personne concernée en raison de leur *caractère sensible*, car elles proviennent de la sphère privée ou de la vie privée de la personne et/ou peuvent influencer considérablement sa réputation. Ce n'est pas l'existence d'un danger particulier pour la personnalité ou les droits fondamentaux qui motive la classification comme données personnelles sensibles, mais plutôt le fait que les informations concernées touchent à un aspect de la vie qui relève d'un domaine protégé par la loi. 6

7 Cette approche, qui repose sur une catégorisation *définitive*, formelle et abstraite, est *controversée*. Le danger pour les droits de la personnalité ne provient pas de certains types de données formellement juridiques, mais de leur utilisation à des fins spécifiques ou dans un contexte particulier, de l'étendue du traitement, etc. (**contexte d'utilisation**). Il convient de se baser sur la *sensibilité réelle* des données en ce qui concerne la protection de la personnalité d'une personne concernée spécifique.

8 À cela s'ajoute le fait que les termes utilisés pour décrire de manière exhaustive les catégories de données personnelles particulièrement sensibles sont **flous** et que la sélection semble statique, désuète et incomplète. Bien que cette critique existait déjà sous aDSG, la catégorisation formelle et abstraite a été maintenue lors de la révision totale. *Rudin* souligne à juste titre : « Ce n'est pas la donnée elle-même, mais son utilisation dans un certain contexte (le **contexte d'utilisation**) qui constitue un danger. »

9 Depuis la révision totale de la LPD, les données des personnes morales ne relèvent plus du champ d'application de la loi. En conséquence, la notion de données personnelles (art. 5, let. a, LPD) et, par conséquent, celle de données sensibles (art. 5, let. c, LPD) s'appliquent uniquement aux **personnes physiques**.

III. DONNÉES RELATIVES AUX OPINIONS OU ACTIVITÉS RELIGIEUSES, PHILOSOPHIQUES, POLITIQUES OU SYNDICALES (CH. 1)

10 Conformément à l'art. 5, let. c, ch. 1, LPD, les **données relatives aux opinions ou activités religieuses, philosophiques, politiques ou syndicales** font partie des données personnelles sensibles. La disposition se réfère en outre à l'appartenance à des associations correspondantes. Le ch. 1 couvre donc notamment les données relatives à la confession religieuse ou à la confession d'une personne, à son appartenance à un parti politique ou à une organisation de travailleurs, à une Église libre ou à une association qui défend une certaine position politique ou idéologique (notamment les associations maçonniques, les organisations religieuses de jeunesse). Pour *Glass*, la portée du terme « données religieuses ou idéologiques » n'est pas claire. Toutefois, en ce qui concerne la protection de la liberté de croyance et de conscience, il semble plausible d'inclure toutes les données qui permettent

de tirer des conclusions sur la croyance, la conscience ou les convictions idéologiques d'une personne. La disposition a été reprise telle quelle de l'ancienne loi et correspond à l'art. 3, let. c, ch. 1, aDSG.

Compte tenu des conséquences parfois importantes que peut avoir le traitement de données personnelles particulièrement sensibles (N. 3), il convient de vérifier dans chaque cas si le traitement de telles données est réellement nécessaire et s'il n'est pas possible de s'en abstenir (par exemple en renonçant à mentionner l'appartenance religieuse dans le dossier personnel). 11

Dans le cadre des délibérations politiques sur la LPD, une tentative visant à supprimer les opinions ou activités syndicales du catalogue de l'art. 5, let. c, ch. 1, LPD a échoué. 12

IV. DONNÉES RELATIVES À LA SANTÉ, À LA SPHÈRE INTIME OU À L'APPARTENANCE À UNE RACE OU À UNE ETHNIE (CH. 2)

Conformément à l'art. 5, let. c, ch. 2, LPD, les données relatives à la santé, à la sphère intime ou à l'appartenance à une race ou à une ethnie sont également considérées comme des données personnelles sensibles. 13

Selon le message relatif à l'aDSG (message de 1988), l'ancienne législation considérait comme **données relatives à la santé** toutes les informations qui, au sens large, constituaient un résultat médical et « pouvaient avoir des conséquences négatives pour les personnes concernées ». Au regard de la conception actuelle de la santé et des progrès médicaux et technologiques, cette conception (historique) des données relatives à la santé, en particulier l'exigence d'un effet négatif sur la santé, est trop restrictive. De plus, la caractéristique des effets négatifs n'est guère prise en compte dans la pratique. Il convient donc aujourd'hui de partir d'une définition plus large des données relatives à la santé. *Vokinger* montre que les données relatives à la santé provenaient autrefois principalement de la relation médecin-patient. Aujourd'hui, les patients enregistrent de plus en plus eux-mêmes des données via des applications, des appareils portables ou les réseaux sociaux. Même des entreprises qui ne font pas partie du secteur classique de la santé (Google, Amazon, Apple...) traitent de plus en plus de données de santé. Celles-ci ne se limitent donc pas aux informations cliniques, mais comprennent également de plus en plus de données (génétiques) qui peuvent être disponibles avant 14

même l'apparition de symptômes cliniques. La question de savoir si certaines données doivent être classées comme données de santé ne dépend pas directement des données elles-mêmes, mais dépend largement du contexte d'utilisation. Des informations identiques, telles que le nombre de pas effectués quotidiennement, peuvent être considérées comme des données relatives au mode de vie chez une personne en bonne santé, tandis qu'elles prennent le caractère de données de santé chez un patient atteint, par exemple, de diabète sucré ou d'insuffisance cardiaque.

15 Le DSGVO part également d'une **définition large des données relatives à la santé** : « Les données à caractère personnel relatives à la santé devraient inclure toutes les données qui se rapportent à l'état de santé d'une personne concernée et qui fournissent des informations sur l'état de santé physique ou mental passé, présent et futur de cette personne. »

16 Une conception large des données relatives à la santé est judicieuse, car dans le domaine des soins de santé, en particulier sous l'influence des technologies de l'information en rapide évolution, les frontières entre thérapie et mode de vie deviennent de plus en plus floues (mots clés : Real World Data et Real World Evidence). Par conséquent, les informations sur l'état de santé d'une personne ne doivent pas être qualifiées de données relatives à la santé au sens de l'art. 5, let. c, ch. 2, LPD uniquement lorsqu'elles se rapportent à un état de santé négatif. De même, selon le **contexte**, les informations indiquant qu'une personne n'est *pas* atteinte d'une maladie ou qu'elle mène un certain mode de vie peuvent aujourd'hui constituer des données relatives à la santé au sens de l'art. 5, let. c, ch. 1, LPD. Même l'*exactitude* de ces données n'est pas pertinente pour leur classification en tant que données de santé particulièrement sensibles, car ce sont précisément les informations inexactes (par exemple un diagnostic erroné généré automatiquement par une interprétation incorrecte des données ou une corrélation inexacte) qui peuvent porter atteinte aux droits de la personnalité d'une personne.

17 La notion de données relatives à la santé figure également dans la LRH. À l'art. 3, let. f, de la loi relative à la recherche sur l'être humain, les *données personnelles liées à la santé* sont définies comme « des informations concernant une personne identifiée ou identifiable qui se rapportent à sa santé ou à sa maladie, y compris ses données génétiques ». Selon le message relatif à la LRH, les données personnelles sont liées à la santé lorsqu'elles « ont un rapport avec une maladie physique ou psychique ou fournissent des

informations sur la constitution et le fonctionnement du corps de la personne concernée ». Selon le message relatif à la LRH, la notion de données relatives à la santé correspond à celle de la LPD.

La **sphère intime** comprend les données « qu'une personne ne communique qu'à quelques personnes choisies et qui revêtent pour elle une grande importance émotionnelle ». La sphère intime va au-delà de la vie sexuelle, mais ne s'étend pas, par exemple, à la situation financière. 18

Relèvent notamment de la sphère intime les informations sur les thérapies, les peurs ou autres sentiments, les comportements addictifs, etc. La notion de sphère intime s'appuie sur la « théorie des trois sphères » du Tribunal fédéral, qui distingue la sphère intime ou secrète, la sphère privée et la sphère commune ou publique. La sphère intime englobe les affaires personnelles de la personne concernée qui doivent en principe rester inconnues de tiers, sauf si la personne concernée divulgue elle-même ces informations. Selon le message, l'identité sexuelle d'une personne peut, selon la situation, être considérée comme relevant soit de la sphère intime, soit des données relatives à la santé.

Dans sa version révisée, la LPD conserve également la notion de **données relatives à l'appartenance à une race** à l'art. 5, let. c, ch. 2, LPD. Le message souligne, en se référant à l'UE, que le maintien de la notion d'appartenance raciale ne signifie pas que le législateur approuve la théorie raciale qui classe les personnes dans une « race » selon leurs caractéristiques physiques, de manière évaluative et idéologique. Le maintien de cette notion s'est fait principalement en conformité avec l'art. 6, al. 1, de la Convention 108+, l'art. 10 de la directive UE 2016/680 et l'art. 9, al. 1, du DSGVO, et a été accepté sans discussion par le Parlement. 19

Lors de la révision totale, la notion d'appartenance raciale figurant à l'art. 5, let. c, ch. 2, LPD a été complétée par les **données relatives à l'appartenance à une ethnie**. Cette modification a été effectuée conformément à l'art. 10 de la directive (UE) 2016/680 et à l'art. 9, al. 1, DSGVO. L'origine ethnique se réfère à l'appartenance à un groupe de personnes qui, en raison de leur histoire, de leur langue, de leurs coutumes, de leur culture, de leurs traditions, etc., se sentent liées entre elles et se perçoivent comme une communauté distincte du reste de la population et/ou perçue comme différente par le reste de la population. *Rudin* cite comme 20

exemple les désignations « Tamoul » ou « Kurde ». L'appartenance ethnique n'est pas synonyme de nationalité. Dans certains cas (p. ex. « Serbes »), cette dernière peut coïncider avec l'ethnie.

V. DONNÉES GÉNÉTIQUES (CH. 3)

21 Depuis la révision totale de la LPD, les **données génétiques** sont désormais explicitement couvertes par les données personnelles sensibles au sens de l'art. 5, let. c, LPD. Les données génétiques sont des *informations sur le patrimoine génétique d'une personne* obtenues par un examen génétique. Selon le message, la notion de données génétiques dans la LPD correspond à la définition de l'art. 3, let. l, aLUMG, qui a été reprise à l'art. 3, let. k, LUMG. Selon l'art. 3, let. g, LHRG, les « données génétiques » sont « les informations sur les caractéristiques héréditaires ou acquises pendant la phase embryonnaire obtenues par un examen génétique ».

22 Les données génétiques peuvent être obtenues à partir de presque tous les types de matériel biologique (sang, cheveux, salive, etc.) au moyen d'un **examen génétique**. Selon l'art. 3, let. a, LAGUM, les analyses génétiques sont « les analyses cytogénétiques et génétiques moléculaires visant à déterminer les caractéristiques du patrimoine génétique humain, ainsi que toutes les autres analyses de laboratoire qui ont pour but direct d'obtenir de telles informations sur le patrimoine génétique humain ».

23 Les données génétiques comprennent également les **profils ADN** au sens de l'art. 3, let. j, LAGG : un profil ADN désigne « les caractéristiques spécifiques du patrimoine génétique d'une personne, qui sont déterminées par une analyse génétique et utilisées pour établir sa filiation ou l'identifier ».

24 Selon *Rudin*, l'art. 5, let. c, ch. 3, LPD repose sur une **conception large** des données génétiques. Ainsi, cela comprend non seulement les données obtenues par le séquençage de génomes individuels, mais aussi, entre autres, les informations obtenues lors de l'utilisation de marqueurs génétiques (par exemple en oncologie). Toutefois, seules les données génétiques qui sont qualifiées de données personnelles au sens de l'art. 5, let. a, LPD relèvent du champ d'application de la LPD et, en particulier, de la définition des données personnelles particulièrement sensibles. Le matériel cellulaire et les échantillons biologiques ne constituent pas des données génétiques tant qu'ils ne permettent pas d'obtenir des informations sur le patrimoine génétique des

personnes concernées. *Rudin* soulève à juste titre la question de savoir dans quelle mesure, selon l'état actuel et futur de la science, « les données génétiques ne permettent effectivement pas, dans un certain contexte, de tirer des conclusions sur une personne déterminée ».

VI. DONNÉES BIOMÉTRIQUES PERMETTANT D'IDENTIFIER DE MANIÈRE UNIQUE UNE PERSONNE PHYSIQUE (CH. 4)

Lors de la révision totale de la LPD, les **données biométriques** ont été ajoutées à la liste des données personnelles sensibles de l'art. 5, let. c. 25

Les données biométriques sont des **caractéristiques physiques** qui sont enregistrées, mesurées et documentées. Il s'agit de données personnelles « obtenues par un procédé technique spécifique à partir des caractéristiques physiques, physiologiques ou comportementales d'un individu et qui permettent ou confirment l'identification univoque de la personne concernée ». Elles ne peuvent être modifiées qu'au prix de grands efforts (p. ex. une intervention chirurgicale). Les empreintes digitales, les empreintes veineuses de la main, les enregistrements vocaux, les images faciales ou les images de l'iris font généralement partie des caractéristiques biométriques. 26

L'utilisation de données biométriques comporte le risque que le comportement d'une personne puisse être suivi et qu'un profil complet puisse être établi, ou qu'elle permette de tirer des conclusions sur des données personnelles particulièrement sensibles au sens de l'art. 3, let. c, aDSG. En outre, en cas d'utilisation abusive, par exemple dans le cadre d'une usurpation d'identité, les données biométriques sont **compromises de manière permanente**. Par conséquent, même avant la révision et leur inclusion explicite dans le catalogue des données personnelles sensibles, les données biométriques pouvaient déjà être considérées comme des données sensibles au sens de l'aDSG . 27

Toutes les données biométriques ne font pas partie des données personnelles sensibles. Pour que les données biométriques relèvent de l'art. 5, let. c, ch. 4, LPD, elles doivent être collectées au moyen d'un procédé technique particulier permettant l'identification ou l'authentification **univoque d'une personne**. De ce fait, selon le message, les photographies ordinaires d'une personne, de visages ou de simples parties du corps ne sont par exemple pas 28

concernées. À moins qu'elles n'aient été traitées à l'aide d'un procédé technique spécial permettant une identification claire de la personne (p. ex. logiciel de reconnaissance faciale). Jacot-Guillarmod souligne que les programmes modernes de reconnaissance faciale peuvent générer à partir de photos ordinaires un « modèle biométrique » permettant de reconnaître la personne représentée. Elle soulève la question de savoir s'il est judicieux de protéger un tel modèle biométrique en tant que données sensibles sans étendre simultanément la protection aux photos à partir desquelles le modèle a été obtenu.

VII. DONNÉES RELATIVES AUX POURSUITES OU SANCTIONS ADMINISTRATIVES OU PÉNALES (CH. 5)

29 Les **données relatives aux poursuites ou sanctions administratives ou pénales** continuent d'être classées parmi les données personnelles sensibles au sens de l'art. 5, let. c, ch. 5, LPD. Outre les poursuites et sanctions expressément mentionnées dans le texte de loi, les procédures disciplinaires, les retraits de permis de conduire et les mesures d'exécution des peines relèvent également de cette disposition. Toutefois, les informations relatives à l'ouverture, à la conduite et à la clôture de poursuites et de retraits d'autorisations, etc., ainsi que les mesures d'exécution correspondantes relèvent également de l'art. 5, let. c, ch. 5, LPD.

30 Pour qu'il s'agisse de données personnelles sensibles, il faut qu'il s'agisse de **poursuites ou de sanctions de la part des autorités publiques**. Peu importe qu'il s'agisse de sanctions ou de poursuites engagées par des autorités suisses ou étrangères.

VIII. DONNÉES RELATIVES AUX MESURES D'AIDE SOCIALE (CH. 6)

31 Les données particulièrement sensibles au sens de l'art. 5, let. c, ch. 6, LPD comprennent les **données relatives aux mesures d'aide sociale**. Selon le message relatif à l'art. 3, let. c, aDSG, cela comprend « les prestations des assurances sociales en rapport avec la maladie et les accidents ainsi que les mesures de tutelle et d'assistance ». À première vue, les prestations des assurances sociales sont couvertes dans la mesure où elles permettent de tirer des conclusions sur l'état de santé (cf. art. 5, let. c, ch. 2, LPD). Les mesures

d'aide sociale au sens de l'art. 5, let. c, ch. 6, LPD comprennent notamment les données relatives au recours aux services sociaux, à l'assurance-chômage, ainsi que les informations sur les prestations individuelles de l'aide sociale, sur les mesures d'assistance ou de protection de l'enfant et de l'adulte, sur le placement à des fins d'assistance et sur d'autres prestations sociales liées aux besoins (réductions des primes d'assurance-maladie, contributions au loyer, prestations complémentaires à l'AVS/AI, etc.).

Une majorité de la Commission des institutions politiques du Conseil national souhaitait supprimer les mesures d'aide sociale du catalogue des données personnelles particulièrement sensibles, ce qui aurait affaibli la protection des données dans ce domaine, sans toutefois créer de différence par rapport à la Convention ER 108+ ou à la directive (UE) 2016/680. La proposition a été rejetée à la majorité des deux tiers par le Conseil national. 32

BIBLIOGRAPHIE

Baeriswyl Bruno, Vorbemerkungen zu Art. 5-13, in: Baeriswyl Bruno/Pärli Kurt/ Blonski Dominika (Hrsg.), Handkommentar zum Datenschutzgesetz (DSG), 2. Aufl., Bern 2023.

Blechta Gabor, Kommentierung zu Art. 3, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.), Basler Kommentar Datenschutzgesetz. Öffentlichkeitsgesetz. 3. Aufl., Basel 2014 (zit. BSK-Blechta, Art. 3 aDSG).

Blechta Gabor P./Dal Molin Luca/Wesiak-Schmidt Kirsten, Kommentierung zu Art. 5, in: Blechta Gabor P./Vasella David (Hrsg.), Basler Kommentar Datenschutzgesetz. Öffentlichkeitsgesetz. 4. Aufl., Basel, 2024 (zit. BSK-Blechta/Dal Molin/Wesiak-Schmidt, Art. 5 DSG).

Epiney Astrid/Nüesch Daniela/Rovelli Sophia, Datenschutzrecht in der Schweiz, Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben, Bern 2023.

Glass Philip, Kommentierung zu Art. 5 lit. c, in: Bieri Adrian/Powell Julian (Hrsg.), DSG Kommentar, Kommentar zum Schweizerischen Datenschutzrecht mit weiteren Erlassen, Zürich 2023 (zit. OFK-Glass, Art. 5 DSG).

Jacot-Guillarmod Emilie, Kommentierung zu Art. 5 DSG, in: Benhamou Yaniv/Cottier Bertil (Hrsg.), LPD, Loi fédérale sur la protection des données, Petit Commentaire, Basel 2023 (zit. PC-Jacot-Guillarmod, Art. 5 DSG).

Jöhri Yvonne, Kommentierung zu Art. 3 lit. c, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich/Basel/Genf 2008.

Mathys Roland, Was bedeutet Big Data für die Qualifikation als besonders schützenswerte Personendaten? Das Beispiel der Gesundheitsdaten, Jusletter IT, 21.5.2015, https://jusletter-it.weblaw.ch/issues/2015/21-Mai-2015/was-bedeutet-big-dat_b0807c5f47.html__ONCE, besucht am 18.8.2025.

Meier Philippe, Protection des données. Fondements, principes généraux et droit privé, Bern 2010.

Meier Philippe/Tschumy Nicolas, Kommentierung zu Art. 5 DSG, in: Meier Philippe/Métille Sylvain (Hrsg.), Commentaire Romand, Loi fédérale sur la protection des données, Basel 2023 (zit. CR-Meier/Tschumy, Art. 5 DSG).

Rudin Beat, Kommentierung zu Art. 4, in: Rudin Beat/Baeriswyl Bruno (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Zürich/Basel/Genf 2014.

Rudin Beat, Kommentierung zu Art. 5, in: Baeriswyl Bruno/Pärli Kurt/ Blonski Dominika (Hrsg.), Handkommentar zum Datenschutzgesetz (DSG), 2. Aufl., Bern 2023 (zit. SHK-Rudin, Art. 5 DSG).

Rudin Beat, Kommentierung zu Art. 35 in: Rütsche Bernhard (Hrsg.), Handkommentar zum Humanforschungsgesetz (HFG), Bern 2015.

Rudin Beat, Kommentierung zu Art. 4, in: Baeriswyl Bruno/Rudin Beat (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich (IDG), Zürich/Basel/Genf 2012.

Simitis Spiros, «Sensitive Daten»: zur Geschichte und Wirkung einer Fiktion, in: Brem/Druey/Kramer/Schwander (Hrsg.), FS Mario M. Pedrazzini, Bern 1990, S. 469-494.

Sprecher Franziska, Regulierung von Gesundheitsdaten und Gesundheitsdatenräumen, Medizinrecht 40 (2022), S. 829-838, DOI: https://doi.org/10.1007/s00350-022-6315-6 (zit. Medizinrecht).

Sprecher Franziska, Datenschutz und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen, Zeitschrift des Bernischen Juristenvereins 8 (2018), S. 482-552 (zit. ZBJV).

Vasella Daniel, Widersprüche im Datenschutzrecht, digma 2020, S. 174-179.

Vokinger Kerstin Noëlle, Gesundheitsdaten im digitalen Zeitalter, in: Jusletter 27. Januar 2020, https://jusletter.weblaw.ch/juslissues/2020/1008/gesundheitsdaten-im-_bf12b7abee.html__ONCE&login=false; DOI: 10.38023/c41ccdd8-8614-4ede-9926-a4331d4d6622.

MATÉRIAUX

Botschaft zum Bundesgesetz über den Datenschutz vom 23.3.1988, BBl 1988 II 413 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/de, besucht am 18.8.2025.

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 18.8.2025.

Botschaft zum Bundesgesetz über die Forschung am Menschen vom 21.10.2009, BBl 2009 8045 ff., https://www.fedlex.admin.ch/eli/fga/2009/1423/de, besucht am 18.8.2025.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 5 let. d LPD

Un commentaire de Hannes Meyle

PROPOSITION DE CITATION

Hannes Meyle, Commentaire de l'art. 5 let. d LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Meyle, art. 5 let. d LPD N. XXX.

Chapitre 2 Dispositions générales

Section 1 Définitions et principes généraux

Art. 5 Définitions

On entend par:

d. *traitement:* toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données;

TABLE DES MATIÈRES

I. Généralités 67
II. Le traitement en tant que condition d'application de la LPD 67
III. Types de traitement désignés 69
A. Collecte 69
B. Stockage 70
C. Conservation 70
D. Utilisation 71
E. Modification 71
F. Divulgation 71
G. Archivage 71
H. Effacement ou destruction 72
Bibliographie 73

I. GÉNÉRALITÉS

La notion de traitement doit être comprise au sens large et englobe **tout traitement** de données à caractère personnel – «en gros : tout ce que l'on fait avec des données à caractère personnel». À titre d'exemple, l'art. 5 let. d cite les formes de traitement suivantes : «collecte, enregistrement, conservation, utilisation, modification, communication, archivage, effacement ou destruction». Les termes «enregistrer» et «supprimer» ont été ajoutés afin de rapprocher la formulation de l'art. 5 let. d LPD de celle de l'art. 4 n° 2 DSGVO. Cependant, le contenu du terme «traitement» reste inchangé après la révision de la loi. Le terme «collecte de données» de l'ancienne loi a été intégré dans le terme «traitement». 1

Une harmonisation terminologique complète avec le DSGVO n'a pas été réalisée pour des «raisons pratiques». Ainsi, la LPD parle de *traitement* ou de *traitement*, tandis que le DSGVO parle de *traitement | traitement*. En outre, les exemples de l'article 5 let. d LPD diffèrent clairement de ceux mentionnés à l'article 4 n° 2 DSGVO. Cependant, malgré les différences rédactionnelles, le traitement *au sens de* la LPD et le traitement *au sens du* DSGVO doivent être compris comme **étant identiques**. Lors de l'interprétation du terme de traitement selon l'art. 5 let. d LPD, la jurisprudence relative à l'art. 4 n° 2 DSGVO peut donc être utilisée à titre indicatif. 2

L'un des principes fondamentaux de la LPD est son caractère technologiquement
neutre. C'est pourquoi, pour déterminer s'il y a traitement, **peu importe les moyens et les procédures** utilisés. Les traitements au sens de la LPD peuvent donc être aussi bien manuels qu'automatisés. Le caractère technologiquement neutre de la LPD implique également que celle-ci couvre ou couvrira les formes de traitement futures, encore inconnues à ce jour. 3

II. LE TRAITEMENT EN TANT QUE CONDITION D'APPLICATION DE LA LPD

La notion de traitement est d'une importance capitale, car la LPD n'est applicable que si des données personnelles sont traitées par un service quelconque impliqué dans le traitement de données personnelles. Les obligations qui en découlent dépendent du fait que le service concerné est 4

(conjointement) responsable ou sous-traitant. Le traitement suppose une action qui a pour but et pour conséquence que quelque chose soit fait avec les données, ou une action qui se **rapporte objectivement aux données**. En revanche, les actions qui concernent simplement les données ne constituent pas un traitement, comme le transport de passagers en bus ou en train, si ces passagers transportent avec eux des données personnelles stockées sur des supports de données, par exemple. Peu importe que les données personnelles concernées soient effectivement portées à la connaissance d'une personne ou non, c'est pourquoi le traitement par le biais de programmes informatiques est également couvert. Le traitement purement mental de données personnelles n'est pas un traitement au sens de l'art. 5 let. d. Par conséquent, les informations qui ne sont présentes que dans la mémoire d'une personne ne sont pas non plus couvertes par le droit d'accès prévu par la loi sur la protection des données.

5 Parfois, la **définition du concept de traitement** ou l'attribution de traitements de données à des personnes spécifiques pose problème, comme le montre l'affaire de stockage de dossiers jugée par un tribunal allemand : à la suite d'une procédure d'insolvabilité, une société foncière est devenue propriétaire d'un hôpital désaffecté dans lequel se trouvaient des dossiers de patients. La propriétaire s'est opposée à l'ordre des autorités de stocker les dossiers dans un lieu particulièrement protégé. Le tribunal a finalement jugé qu'il n'y avait pas eu de traitement par la propriétaire, car celle-ci n'avait pas elle-même stocké les dossiers et ne les avait pas non plus manipulés d'une autre manière. Cela n'a bien sûr pas permis de déterminer si un autre organisme avait traité ou fait traiter les données en tant que sous-traitant ou responsable.

6 Des questions sur la portée de la notion de traitement se posent depuis peu également en rapport avec les systèmes d'IA. Le fait que le traitement d'informations – dans la mesure où elles sont à caractère personnel – au moyen de systèmes d'IA constitue un traitement est une conséquence de la définition large du traitement et de la conception technologiquement neutre de la LPD. En revanche, la distinction entre les différents processus de traitement, tels qu'ils se produisent dans le cadre de l'utilisation de systèmes d'IA en partage de tâches, peut être moins claire dans certains cas. Cette distinction est pertinente car elle a une incidence sur la personne responsable du respect de la législation sur la protection des données (en particulier la

protection des droits des personnes concernées) et des éventuelles violations lors du traitement. Le règlement européen sur l'IA différencie les rôles des acteurs, entre autres entre les fournisseurs et les exploitants de systèmes d'IA, afin de définir les obligations. De telles distinctions n'ont pas encore été établies dans le droit de la protection des données. Il serait toutefois logique de faire ici aussi la distinction entre la création d'un système d'IA (c'est-à-dire la formation qui l'accompagne, dans la mesure où des données personnelles sont impliquées) et son utilisation.

III. TYPES DE TRAITEMENT DÉSIGNÉS

La liste des types de traitement désignés est **donnée à titre d'exemple** et les termes se recoupent en partie. Seuls certains des types de traitement désignés sont associés à des instructions spécifiques, par exemple la collecte, la divulgation et la destruction des données. En outre, les principes de traitement de la protection des données doivent être pris en compte pour tout traitement. Lorsqu'une activité ne peut être rattachée à aucune forme de traitement définie, il est toujours possible qu'il s'agisse d'une forme de traitement non définie (voir chapitre I ci-dessus). Les formes de traitement définies sont donc moins importantes pour l'application de la LPD. 7

A. Collecte

Il y a collecte de données lorsque l'organisme qui collecte les données **prend volontairement connaissance** de ces données ou en justifie la disposition. Il n'y a pas collecte de données lorsque les données sont fournies par la personne concernée elle-même ou par des tiers sans qu'elle en fasse la demande et que le destinataire des données ne souhaite pas les traiter (par exemple, lors de la réception d'un e-mail mal acheminé, lors de l'écoute d'une conversation, etc. En revanche, il y a collecte de données personnelles lorsque le service concerné souhaite collecter des données en général et accepte que cela implique également la collecte de données personnelles. Conformément à l'art. 6 al. 3 LPD, la collecte de données ne peut être effectuée qu'à des fins spécifiques et reconnaissables par la personne concernée et entraîne l'obligation d'informer conformément à l'art. 19 LPD. Les exemples typiques d'opérations de collecte sont la compilation de données provenant d'autres sources, l'enregistrement ou la journalisation d'informations. Que les données soient protégées ou librement disponibles n'a 8

pas d'importance. Par conséquent, une recherche ciblée sur Internet peut également constituer une collecte de données personnelles et entraîner l'applicabilité de la LPD. Il n'est pas nécessaire de prendre effectivement connaissance du contenu des données, il suffit que les données parviennent pour la première fois dans le domaine de disponibilité d'un responsable. Ainsi, les formes automatisées de collecte de données, telles que le « data scraping », sont également considérées comme une collecte au sens de la LPD. Les principes ci-dessus s'appliquent également aux systèmes d'IA générative : Lorsque des données personnelles sont collectées par inadvertance, il n'y a généralement pas de collecte, et il n'y en a pas non plus lorsque des données personnelles existantes sont simplement modifiées (par exemple par la génération ou le traitement d'un texte). En revanche, lorsque des systèmes d'IA générative sont utilisés pour obtenir des informations supplémentaires sur une personne ou pour en inventer, il y a généralement collecte de données du point de vue de la protection des données.

B. Stockage

9 La notion de stockage a été introduite afin de se rapprocher de la formulation des sources juridiques **européennes pertinentes**, notamment de l'article 4, paragraphe 2, du DSGVO. Selon l'art. 4 n° 2 DSGVO, le stockage est défini comme la conservation de données sous forme matérielle sur un support de données (disque dur, serveur, clé USB, etc.) dans le but de pouvoir continuer à traiter les données ultérieurement. Selon l'objectif visé, la conservation d'informations dans des systèmes d'IA peut également être considérée comme un stockage (voir ci-dessus n. 6).

10 L'**OPDo** fait référence à la notion de stockage en ce qui concerne les exigences en matière de sécurité des données (art. 3 al. 2 let. b et e OPDo) et l'obligation de journalisation (art. 4 al. 2 et 3 OPDo).

C. Conservation

11 La conservation peut être décrite comme l'activité par laquelle les données sont maintenues **disponibles dans le contexte du traitement**. Contrairement à l'archivage (voir n. 15 ci-dessous), les données conservées peuvent donc toujours être utilisées. En tant que forme de traitement, la conservation est expressément soumise à la LPD, car des atteintes à la personnalité sont encore possibles à ce stade du traitement, par exemple en

raison de lacunes dans la sauvegarde des données. La conservation est abordée à l'art. 12 al. 2 let. e LPD, selon lequel la durée de conservation doit être indiquée dans le registre des traitements, ainsi que dans le cadre du droit d'accès conformément à l'art. 25 al. 2 let. d LPD.

D. Utilisation

L'utilisation des données désigne toute activité ayant pour but d'utiliser le **contenu informatif** des données (y compris la prise de connaissance des données). L'utilisation des données est mentionnée à l'art. 5 let. f LPD (profilage), à l'art. 21 OPDo (exigences techniques relatives à la mise en œuvre de la communication des données) ainsi qu'à l'art. 4 al. 5 OPDo (journalisation). Cependant, la LPD ou l'OPDo ne prévoient pas de consignes spécifiques pour l'utilisation des données. 12

E. Modification

La modification des données peut être décrite comme une « activité par laquelle le contenu informatif des données personnelles est modifié (**remanié quant au contenu**) ». La LPD ne prévoit pas d'instructions particulières, à part le respect des principes de traitement, ni de conséquences juridiques ; la modification des données est mentionnée à l'art. 3 al. 3 let. a OPDo (contrôle de la saisie) et à l'art. 4 al. 2 et 3 OPDo (journalisation). 13

F. Divulgation

La communication de données, qui constitue une **forme de traitement particulièrement délicate**, fait l'objet d'une réglementation distincte dans OK-NN, art. 5 let. e LPD. [Commentaire à paraître] 14

G. Archivage

L'archivage consiste à **maintenir la disponibilité** des données indépendamment du contexte de traitement. Contrairement à la conservation (voir ci-dessus n° 11), l'archivage consiste à retirer les données du contexte de traitement dans lequel elles ont été traitées jusqu'à présent. Il s'ensuit que l'atteinte à la personnalité des personnes concernées est généralement réduite. Cela est exprimé dans l'art. 32 al. 1 let. b et l'art. 41 al. 5 LPD, qui limitent les droits des personnes concernées en cas de traitement à des fins 15

d'archivage. Par ailleurs, l'art. 38 LPD (règle spéciale pour les organes fédéraux concernant la mise à disposition de certaines données personnelles pour les archives fédérales) fait référence aux fins d'archivage ou à l'archivage.

H. Effacement ou destruction

16 Le terme de « **destruction** » implique que les données sont détruites de manière irréversible. Dans le cas d'un stockage physique des données sur papier, le papier doit être brûlé ou déchiqueté. Dans le cas de données stockées électroniquement, le support de données correspondant doit être rendu inutilisable et toutes les copies doivent être traitées de manière à ce que les données ne soient plus lisibles.

17 Le terme d'**effacement de données** est généralement utilisé pour le traitement électronique des données et a une portée plus limitée : pour effacer des données, il suffit en principe d'utiliser les commandes d'effacement du programme concerné, de sorte que les données ne sont plus reconnaissables dans le cadre des processus habituels du programme et ne peuvent être restaurées qu'avec des moyens disproportionnés. En d'autres termes, les données personnelles sont effacées lorsqu'il n'est plus possible d'établir un lien avec une personne. Une anonymisation efficace équivaut donc à un effacement ou constitue une méthode d'effacement des données personnelles. Parallèlement à la notion de données personnelles, il faut appliquer l'approche dite relative, ce qui signifie que le point de vue des personnes ou des organismes qui ont accès aux données est déterminant. Il peut donc être difficile de déterminer si des données personnelles ont été supprimées de manière efficace, car des données peuvent rester dans les systèmes après l'exécution des ordres de suppression et être restaurées dans certaines circonstances. Dans ces cas, la question se pose de savoir si la restauration des données ou l'accès aux données nécessite un effort disproportionné. Cela ne peut être évalué qu'au cas par cas, en fonction des conditions techniques, mais aussi en fonction de l'intérêt que des tiers pourraient avoir à restaurer la référence personnelle.

18 La distinction clairement établie dans les documents législatifs entre les notions d'effacement et de destruction n'est **pas systématiquement appliquée** dans la LPD. Ainsi, l'art. 6 al. 4 LPD exige que les données soient « *détruites* ou rendues anonymes dès qu'elles ne sont plus nécessaires au traitement » - il serait plus juste de mentionner ici également l'effacement.

Même si la loi n'utilise pas les termes de manière cohérente, il convient, par souci de clarté, de veiller à ce que les termes « effacement » et « destruction » ne soient pas confondus par inadvertance lors de la rédaction de contrats, par exemple dans le cadre de contrats de traitement de commandes. Il faut notamment éviter que la destruction de données soit convenue par inadvertance au lieu d'une obligation d'effacement, car la destruction pourrait être difficile à réaliser ou non souhaitable dans le cas d'un traitement électronique des données (voir ci-dessus n. 16).

BIBLIOGRAPHIE

Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023 (zit. SHK DSG, Bearbeiter/-in).

Blechta Gabor/Vasella David, Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, 4. Aufl, Basel 2024 (zit. BSK DSG, Bearbeiter-in).

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988, abrufbar unter https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/en, besucht am 30.6.2023 (zit. Botschaft 1988).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 694, abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 30.6.2023 (zit. Botschaft 2017).

Freund Bernhard, Anmerkung zu OVG Hamburg: Datenlagerung ist keine Datenverarbeitung, Zeitschrift für Datenschutz 2021, S. 283-284 (zit. Freund, ZD 2021).

Griesinger Marcel, Schweizerisches Datenschutzgesetz: Datenschutz-Compliance für Unternehmen beim Einsatz von KI-Anwendungen, CB 2024, S. 485 f. (zit. Griesinger, CB 2004, S. 485).

Kühling Jürgen/Buchner Benedikt, Kommentar Datenschutz-Grundverordnung/BDSG, 4. Aufl, München 2024 (zit. Kühling/Buchner, Bearbeiter-in).

Rosenthal David, Löschen und doch nicht löschen, Zeitschrift für Datenrecht und Informationssicherheit 2019, S. 190-197 (zit. Rosenthal, digma 2019).

Rosenthal David, Das neue Datenschutzgesetz, in: Jusletter vom 16.11.2020 (zit. Rosenthal, Jusletter 2020).

Rosenthal David, Datenschutz beim Einsatz generativer künstlicher Intelligenz, in: Jusletter vom 6.11.2023 (zit. Rosenthal, Jusletter 6.11.2023).

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. Rosenthal/Jöhri).

Taeger Jürgen/Gabel Detlev, DSGVO – BDSG – TTDSG, 4. Aufl., Bremen 2022 (zit. Taeger/Gabel, Bearbeiter-in).

Wolff Heinrich Amadeus/Brink Stefan/v. Ungern-Sternberg Antje, BeckOK Datenschutzrecht, 44. Edition, Stand: 1.11.2024 (zit. BeckOK Datenschutzrecht, Bearbeiter-in).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 5 lit. f und g LPD

Un commentaire de Matthias Glatthaar / Annika Schröder

PROPOSITION DE CITATION

Matthias Glatthaar/Annika Schröder, Kommentierung zu Art. 5 lit. f und g DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Glatthaar/Schröder, N. XXX zu Art. 5 lit. f und g DSG.

Chapitre 2 Dispositions générales

Section 1 Définitions et principes généraux

Art. 5 Définitions

On entend par:

f. *profilage:* toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;
g. *profilage à risque élevé:* tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée,

parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique;

TABLE DES MATIÈRES

En bref ... 78
I. Généralités ... 78
A. Remarque préliminaire ... 78
B. Historique ... 79
C. Systématique et délimitation ... 80
II. profilage (let. f) ... 80
A. Généralités ... 80
B. Processus d'évaluation ... 80
C. Automatisation ... 81
D. Aspects personnels ... 82
E. Lien avec les personnes ... 83
III. profilage à haut risque (let. g) ... 83
A. Généralités ... 83
B. Mise en relation des données ... 85
C. Évaluation des aspects essentiels de la personnalité ... 85
D. Nécessité d'une approche au cas par cas ... 86
IV. Conséquences juridiques ... 87
A. Profilage normal ... 87
B. Profilage à haut risque ... 88
V. Conseils pratiques ... 89
Bibliographie ... 91
Matériaux ... 92

EN BREF

La notion de profilage dans la nouvelle LPD remplace l'ancienne notion de profil de la personnalité. Les dispositions relatives au profilage ont été largement débattues lors des délibérations parlementaires et ont été l'une des raisons de la longueur du processus législatif. Le profilage est défini comme un traitement automatisé des données visant à évaluer des aspects personnels. Ce type de profilage est très répandu dans la pratique, surtout dans le domaine de la personnalisation de l'offre, et n'a pas de conséquences juridiques particulières pour les responsables privés. Outre le profilage normal, la nouvelle LPD connaît également une forme qualifiée de profilage "à haut risque". La LPD s'écarte ainsi du RGPD, qui ne connaît le profilage qualifié qu'en lien avec des décisions individuelles automatisées. Il y a profilage à haut risque lorsque le croisement de données permet d'évaluer des aspects essentiels de la personnalité. La qualification de profilage à haut risque dépend fortement du cas d'espèce et déclenche surtout l'obligation de réaliser une analyse d'impact relative à la protection des données, mais n'entraîne pas une exigence générale de consentement.

I. GÉNÉRALITÉS

A. Remarque préliminaire

1 Le profilage, en tant qu'évaluation automatisée d'aspects personnels, est aujourd'hui un procédé largement utilisé, qui revêt une grande importance pratique, notamment comme base de la personnalisation très répandue des offres dans le commerce de détail. Les offres numériques telles que les services de streaming, les boutiques en ligne et les plateformes de médias sociaux disposent généralement d'une telle quantité de "contenu" qu'elles ne pourraient pas être utilisées de manière judicieuse sans personnalisation. Pour ces offres numériques, les clients exigent aujourd'hui tout naturellement une aide à l'orientation ciblée, par exemple sur la base du comportement d'utilisation antérieur.

2 Le profilage est donc un processus quotidien qui est souvent dans l'intérêt des clients. Étant donné que le profilage implique un jugement de valeur qui est généralement effectué de manière automatisée sur la base de corrélations et

de probabilités, le processus est toutefois considéré comme comportant des risques et nécessitant donc une réglementation. Le profilage implique toujours une évaluation généralisée de la personnalité sur la base de certaines caractéristiques qui, le cas échéant, ne tient pas compte de la personne concrètement concernée ("catégorisation"). La sensibilité accrue du profilage est particulièrement évidente lorsqu'il s'agit d'applications en dehors du commerce avec les clients finaux, par exemple l'utilisation par les autorités dans le domaine de la sécurité et de la poursuite pénale.

B. Historique

La notion de "profilage", nouvellement introduite par la révision, remplace celle de "profil de la personnalité" de l'ancienne LPD. Alors que le profil de la personnalité décrit un état statique, le nouveau terme de profilage se réfère au processus d'évaluation en tant que tel. Le concept de profil de la personnalité était une spécificité suisse et son remplacement par la notion de profilage permet de s'aligner sur le droit européen (bien que le profil de la personnalité ait été réintroduit par analogie sous la forme de "profilage à haut risque"). La nouvelle terminologie doit également refléter les progrès techniques, par exemple dans les domaines du big data et de l'intelligence artificielle, et les possibilités accrues de traitement des données qui en découlent. 3

Au cours du processus législatif, le profilage a été l'un des principaux points de discussion. Les divergences sur le profilage ont été un facteur important du retard dans l'adoption de la loi révisée. La question de savoir si et dans quelle mesure le profilage devait nécessiter un consentement a fait l'objet d'un débat particulièrement vaste. Dans l'avant-projet de LPD, le profilage sans consentement explicite de la personne concernée figurait encore parmi les atteintes à la personnalité. Cette exigence de consentement a toutefois été abandonnée dans la suite du processus législatif. Un droit d'opposition au profilage, qui avait été mis en discussion, n'a pas non plus pu s'imposer au Parlement. Les détails de la définition ont également fait l'objet de discussions, notamment le concept de "profilage à haut risque", qui n'a été créé qu'au cours des débats parlementaires et est resté controversé jusqu'à la fin. 4

C. Systématique et délimitation

5 L'article 5 LPD distingue deux formes de profilage : d'une part, au let. f, le profilage "normal" en tant que traitement automatisé de données visant à évaluer des aspects personnels, et d'autre part, au let. g, un profilage qualifié "à haut risque" fondé sur le profilage normal. Alors que la définition du profilage normal a été reprise telle quelle du DSGVO dans le droit suisse, le profilage qualifié à haut risque constitue une création originale du législateur suisse. En établissant cette gradation, le législateur a voulu tenir compte du fait que les différentes applications du profilage diffèrent parfois considérablement en termes de portée et de conséquences.

6 Le profilage doit être distingué de la décision individuelle automatisée au sens de l'article 21 LPD. Le profilage est le processus d'évaluation qui, le cas échéant, est à la base d'une décision individuelle automatisée, mais qui se situe logiquement en amont de celle-ci. Un profilage ne conduit à une décision individuelle automatisée que si l'évaluation se manifeste par un effet externe concret et que cet effet externe prend la forme d'une conséquence juridique ou d'une atteinte aussi radicale.

II. PROFILAGE (LET. F)

A. Généralités

7 Le changement de notion du profil de la personnalité au profilage devait apporter un alignement sur le droit européen et le législateur a logiquement repris presque mot pour mot la définition légale de l'article 4 point 4 du DSGVO dans le droit suisse. Pour l'essentiel, elle comprend quatre éléments : premièrement, un processus d'évaluation qui, deuxièmement, est automatisé et qui, troisièmement, produit des déclarations sur des aspects personnels qui, quatrièmement, se rapportent à une personne physique. Ces éléments sont illustrés ci-après à l'aide de l'exemple des recommandations de lecture personnalisées dans les librairies.

B. Processus d'évaluation

8 La notion de profilage se concentre sur l'élément d'évaluation. Le profilage est en fait un processus d'évaluation qui permet d'obtenir de nouvelles informations sur une personne par le biais d'une analyse ou d'une prédiction.

"Prévoir" signifie que le profilage est généralement axé sur l'avenir, par exemple, dans le cas des librairies, pour prévoir quels livres les clients pourraient mettre dans leur panier. L'"analyse", la deuxième forme d'évaluation mentionnée dans la définition légale, représente en revanche une évaluation d'aspects passés ou présents, l'analyse ne se suffisant généralement pas à elle-même, mais constituant à son tour la base de déclarations orientées vers l'avenir.

Une évaluation comporte toujours un classement normatif et est donc, dans une certaine mesure, subjective. S'il n'y a pas de marge d'appréciation subjective et qu'il s'agit uniquement de constater objectivement un état de fait, il n'y a pas d'évaluation. Le simple calcul de l'emplacement par un système de navigation, par exemple, ne contient pas plus d'élément d'évaluation que la simple consultation, le filtrage ou le tri de données dans une base de données. Si une libraire trie ses clients en fonction de caractéristiques telles que l'âge ou le lieu de résidence et qu'elle forme des groupes de clients correspondants, il ne s'agit donc pas de profilage. De même, si elle extrait de sa base de données clients les acheteurs d'un certain auteur pour leur signaler une nouvelle parution du même auteur, la libraire procède à un simple filtrage et non à un profilage. En revanche, si la libraire classe par exemple les acheteurs de "1984" de George Orwell dans le segment de clientèle "littérature dystopique", il s'agit d'un jugement de valeur et donc d'un profilage. 9

C. Automatisation

Le profilage selon l'art. 5 let. f LPD ne concerne que le traitement automatisé de données personnelles. Le traitement est automatisé lorsqu'il est effectué à l'aide de techniques assistées par ordinateur. Il n'y a pas d'automatisation lorsque l'évaluation repose exclusivement sur un processus de pensée humain, c'est-à-dire qu'elle a lieu uniquement "dans la tête d'un être humain". 10

Si une libraire connaît par exemple les préférences de ses clients et leur fait des recommandations individuelles sur cette base (elle recommande par exemple "The Handsmaid's Tale" à un lecteur de "1984"), il ne s'agit pas d'un profilage au sens de la loi, faute d'automatisation. Le fait que la libraire prenne des notes sur chaque client dans une base de données électronique n'y change rien. En revanche, si la libraire fait calculer les recommandations par un algorithme, il s'agit d'un processus automatisé et donc de profilage. Dans 11

ce cas, l'automatisation n'est pas supprimée par le simple fait que le libraire définit lui-même les critères jusqu'à un certain point (par exemple en attribuant des auteurs ou des livres à certains genres), tant que l'évaluation est assistée par ordinateur et ne se limite pas à de simples "si-alors".

12 La forme technique concrète de l'opération de profilage n'est pas déterminante. La notion de profilage est neutre sur le plan technologique et la qualification de profilage est indépendante des procédés techniques utilisés. Dans la pratique, les systèmes de recommandation d'offres numériques, en particulier, sont souvent basés sur le "filtrage collaboratif", qui prend en compte non seulement l'historique de l'utilisateur et les informations sur le contenu, mais aussi les préférences et le comportement des autres utilisateurs. Si, par exemple, dans une librairie en ligne, l'utilisateur A et l'utilisateur B aiment des livres similaires et que l'utilisateur A a évalué positivement un certain livre que l'utilisateur B n'a pas encore acheté, le système pourrait recommander ce livre à l'utilisateur B. L'utilisation de telles méthodes basées sur des corrélations n'est toutefois pas essentielle sur le plan conceptuel.

D. Aspects personnels

13 Pour qu'il y ait profilage, l'évaluation doit aboutir à de nouvelles connaissances sur des aspects personnels de personnes physiques. L'article 5 let. f LPD contient une liste d'aspects personnels dont l'évaluation peut justifier un profilage : Performance au travail (p. ex. respect de normes de qualité ou réalisation d'objectifs de productivité), situation économique (p. ex. revenus ou comportement en matière d'épargne), santé (p. ex. mode d'alimentation ou prédisposition à certaines maladies), préférences personnelles (p. ex. préférences d'investissement, genres préférés ou destinations de voyage préférées), intérêts (par exemple, hobbies ou activités de loisirs), fiabilité (par exemple, solvabilité ou types de personnalité), comportement (par exemple, interactions sociales ou comportement d'achat), lieu de séjour ou de déplacement (par exemple, modèles de déplacement, parcours de marche ou comportement de mobilité).

14 L'énumération de l'article 5 let. f est très complète, mais non exhaustive ("notamment"), et d'autres aspects peuvent être pertinents selon le contexte. L'élément de l'aspect personnel n'a donc guère d'effet limitatif. Ce qui est exigé, c'est que l'aspect présente une certaine complexité et soit donc accessible à une évaluation au sens d'un jugement subjectif. Les aspects qui ne

permettent aucune appréciation et qui peuvent donc être constatés de manière purement objective ne relèvent pas du profilage (p. ex. la détermination du poids corporel). Toutefois, en tant que donnée prospective, ces mêmes aspects peuvent, le cas échéant, nécessiter une évaluation (par exemple, le poids corporel futur pronostiqué). En outre, des aspects purement objectifs peuvent servir de base de données pour l'évaluation d'autres aspects dépendant du pouvoir d'appréciation (le poids corporel, par exemple, comme indicateur de certains risques de maladie).

E. Lien avec les personnes

Le profilage au sens juridique suppose enfin que les déclarations produites se rapportent à des personnes individuelles. En revanche, si les déclarations se rapportent uniquement à des groupes de personnes parmi lesquelles aucune personne individuelle n'est identifiable, il n'y a pas de profilage, même si le traitement repose sur des données personnelles en tant qu'"input". Si une libraire se contente d'analyser les auteurs et les genres les plus appréciés par les différents groupes d'âge afin d'optimiser son assortiment, sans faire de déclarations sur des clients individuels, elle ne procède pas à un profilage. Il en va de même pour l'analyse de l'utilisation du site web en vue d'améliorer la convivialité, qui ne donne lieu à aucune évaluation personnelle. 15

Il n'y a pas non plus de profilage lorsque le traitement ne repose que sur des données anonymes ou agrégées, les "données d'entrée" ne présentant donc aucune référence personnelle. Il ne s'agit pas d'un traitement de données personnelles et le droit de la protection des données n'est pas applicable (art. 2 al. 1 LPD). Si le traitement a précisément pour but de désanonymiser les données anonymes et de les (ré)associer à des personnes individuelles, il s'agit à nouveau d'un traitement de données personnelles soumis à la législation sur la protection des données. Dans ce cas, il peut s'agir d'un profilage dont le but est précisément de désanonymiser les données en établissant des liens. 16

III. PROFILAGE À HAUT RISQUE (LET. G)

A. Généralités

Avec le "profilage à haut risque", l'article 5 let. g LPD introduit une forme qualifiée de profilage basée sur le profilage normal. La figure juridique du "profilage à haut risque" n'a été créée qu'au cours du processus législatif et a 17

fait l'objet de débats intenses au Parlement. Les discussions ont notamment porté sur des formulations qui auraient permis de déterminer si le profilage produisait des données personnelles sensibles ou si le profilage s'étendait à différents domaines de la vie de la personne concernée. Enfin, l'approche consistant à reprendre la figure juridique actuelle du "profil de la personnalité", non pas dans son nom, mais dans son contenu, s'est imposée. Le profilage à haut risque est donc en substance un profilage qui conduit à un profil de la personnalité au sens de l'ancienne LPD. Le profil de la personnalité n'a été supprimé qu'en apparence par la nouvelle LPD.

18 Le profilage à haut risque est une particularité suisse. Le RGPD ne connaît pas une telle forme qualifiée de profilage et fait dépendre les conséquences juridiques particulières en cas de profilage du fait que le profilage est effectué en relation avec une décision individuelle automatisée. Il aurait donc été possible de s'aligner davantage sur le RGPD si l'on avait défini comme critère du "profilage à haut risque" le fait que le profilage produise des effets juridiques pour la personne concernée ou l'affecte de manière significative de façon similaire. Il est regrettable que l'ancien profil de personnalité ait été réactivé et qu'une particularité suisse ait été maintenue. Une occasion a été manquée d'établir une plus grande convergence avec le DSGVO.

19 Pour qu'il y ait "profilage à haut risque" au sens de l'article 5 let. g LPD, deux éléments doivent être présents en plus du profilage normal : premièrement, une mise en relation des données et, deuxièmement, des aspects essentiels de la personnalité auxquels se rapportent potentiellement les déclarations générées par le profilage. Ces deux éléments supplémentaires sont à la fois nécessaires et suffisants. Cela signifie tout d'abord que le risque élevé qui donne son nom à l'étude est supposé exister si les deux éléments précités sont présents. Le risque élevé ne constitue pas un élément conceptuel supplémentaire à examiner séparément au cas par cas. En outre, cela signifie qu'un profilage qui ne répond pas à la définition légale ne devient pas un "profilage à haut risque" parce qu'il présente, dans le cas concret, un risque élevé pour les personnes concernées pour d'autres raisons (et nécessite donc, par exemple, la réalisation d'une analyse d'impact relative à la protection des données).

B. Mise en relation des données

Le profilage à haut risque implique tout d'abord une combinaison de données. 20
La mise en relation des données fait référence au processus par lequel deux ou plusieurs ensembles de données distincts sont reliés, fusionnés ou comparés afin d'obtenir une information plus approfondie ou plus complète. Cette mise en relation des données peut s'effectuer de différentes manières, par exemple en combinant des données provenant de différentes sources mais se rapportant à la même personne, ou en reliant des données basées sur des caractéristiques, des critères ou des variables communs.

La mise en relation de données remplace l'expression "compilation de 21
données" utilisée sous l'ancien droit et exprime ainsi le fait que le profilage ne consiste pas en une simple accumulation de données, mais en une mise en relation ciblée de différents ensembles de données. Une simple collecte de données, éventuellement en vue de préparer un profilage, ne constitue pas encore un tel lien. Contrairement à l'ancien profil de la personnalité, une collecte statique de données ne suffit pas.

C. Évaluation des aspects essentiels de la personnalité

Alors que, dans le cadre d'un profilage normal, des connaissances sur 22
n'importe quel aspect de la personnalité suffisent, elles doivent, dans le cadre d'un profilage à haut risque, se rapporter à des aspects essentiels de la personnalité. Il n'est pas nécessaire que ces aspects essentiels de la personnalité soient effectivement évalués. Il suffit que des déclarations sur des aspects essentiels de la personnalité soient en principe possibles ("autorisées") sur la base des données traitées et de la manière dont le traitement a été effectué. Le fait que l'art. 5 let. g LPD utilise le terme "évaluation" au lieu d'"apprécier" n'est pas pertinent. Les deux termes sont synonymes.

Conformément à la volonté du législateur, la jurisprudence "Moneyhouse" du 23
Tribunal administratif fédéral relative au profil de la personnalité doit continuer à servir de référence pour déterminer s'il y a évaluation d'aspects essentiels de la personnalité. L'élément déterminant est donc de savoir si les informations mises en relation forment une image globale de la personne concernée. Les critères essentiels sont ici la quantité et le type de données utilisées, le contexte de leur utilisation ainsi que la dimension temporelle,

c'est-à-dire si les données personnelles sont collectées sur une longue période et donnent ainsi une image quasi biographique en montrant une évolution de la personne concernée. Dans ce contexte, même des données triviales en soi peuvent, le cas échéant, donner une image globale de la personne grâce à un recoupement systématique et fournir des informations potentiellement sensibles sur son identité, ses activités ou ses préférences.

D. Nécessité d'une approche au cas par cas

24 Tout comme le profil de la personnalité utilisé jusqu'à présent, le profilage à haut risque reste globalement difficile à appréhender. Les deux éléments conceptuels que sont la mise en relation des données et l'évaluation d'aspects essentiels de la personnalité fournissent certes un cadre de base, mais ne parviennent pas à conférer à la notion des contours clairs et nécessitent une classification au cas par cas. Le Tribunal administratif fédéral a également reconnu dans sa jurisprudence relative au profil de la personnalité que cela revient en fin de compte à une considération au cas par cas. Dans un certain sens, "on le reconnaît quand on le voit".

25 Dans l'exemple de la librairie, il faudrait par exemple partir du principe qu'il s'agit d'un profilage à haut risque si les données relatives au comportement de lecture étaient combinées avec le comportement d'achat de denrées alimentaires et, le cas échéant, avec d'autres données de transaction ainsi que, par exemple, avec des données d'applications de suivi de la condition physique, afin de tirer des conclusions sur l'état de santé et de soumettre aux personnes concernées de la publicité pour des offres de santé correspondantes ou même de calculer des primes d'assurance individuelles. Il faudrait également qualifier de profilage à haut risque le fait de combiner le comportement de lecture avec des données sur le comportement de navigation et des données de géolocalisation afin d'en tirer des informations sur les opinions philosophiques ou les convictions religieuses. On pourrait également considérer qu'il y a profilage à haut risque si le comportement de lecture était associé à des données de cartes de crédit et à des informations provenant de plateformes de réseaux professionnels, afin d'en déduire des informations sur la fortune et la capacité de paiement et de décider sur cette base quels produits et services seront proposés aux personnes concernées, comment et à quel prix.

IV. CONSÉQUENCES JURIDIQUES

A. Profilage normal

Dans le cadre de la LPD, un profilage normal, c'est-à-dire sans "risque élevé", n'est en principe pertinent que pour les organes fédéraux (étant entendu que les particuliers chargés de tâches publiques sont également considérés comme des organes fédéraux). Et ce, à deux égards : d'une part, il n'existe une base légale suffisante pour un profilage par un organe fédéral que si le profilage est prévu dans une loi au sens formel (art. 34 al. 2 let. b LPD). D'autre part, si une telle base n'existe pas dans une loi au sens formel et que le profilage est fondé sur un consentement, celui-ci n'est valable que s'il est explicite, c'est-à-dire s'il porte sur le profilage en tant que tel (art. 6 al. 7 let. c LPD). 26

En revanche, un profilage normal n'a pas de conséquences juridiques particulières pour les responsables privés et les règles habituelles s'appliquent. En particulier, le profilage doit être suffisamment transparent et les personnes concernées doivent être informées des catégories de données créées au moyen du profilage (p. ex. données de préférence) (art. 19 al. 3 LPD). Le profilage lui-même ne doit toutefois pas être mentionné ou décrit spécifiquement dans la déclaration de protection des données. Ce n'est que si des décisions essentielles sont entièrement automatisées sur la base d'un profilage qu'il existe à cet égard des obligations particulières d'information et de renseignement (art. 21 et art. 25 al. 2 let. f LPD). 27

Comme tout autre traitement de données, le profilage peut nécessiter la réalisation d'une analyse d'impact relative à la protection des données s'il comporte des risques élevés pour les personnes concernées. L'existence de risques élevés doit être déterminée au cas par cas sur la base des circonstances concrètes et peut également être le cas lorsque le profilage n'est pas considéré comme un profilage "à haut risque" selon l'art. 5 let. g LPD en raison de l'absence d'éléments de définition. 28

Dans le cas du profilage également, le consentement n'est requis que s'il y a violation des principes de traitement et qu'il n'existe aucun autre motif de justification pour le traitement des données. A cet égard, le profilage ne se distingue pas d'un traitement de données "normal". L'exigence de 29

consentement pour le profilage, qui figurait encore dans l'avant-projet et qui a fait l'objet de nombreuses discussions, n'a pas survécu au processus législatif.

30 De même, le RGPD ne prévoit guère de conséquences juridiques spécifiques en cas de profilage ou seulement lorsque le profilage est effectué en liaison avec une décision individuelle automatisée. Sans référence à la prise de décision automatisée, le profilage n'est mentionné qu'à l'article 21 al. 1 et 2 du RGPD, mais uniquement à titre d'exemple, car le profilage, comme tout autre type de traitement, serait couvert par le droit d'opposition sans mention particulière. Il convient également de noter que dans le champ d'application du RGPD, tout traitement de données, et donc tout profilage, doit reposer sur une base juridique. Les bases juridiques disponibles ne sont toutefois pas limitées et toutes les bases juridiques possibles de l'art. 6 al. 1 RGPD sont également disponibles pour le profilage.

B. Profilage à haut risque

31 L'intensité avec laquelle les débats sur le profilage à haut risque ont été menés contraste avec le peu de pertinence juridique de cette figure juridique. La nouvelle LPD ne prévoit que trois conséquences juridiques liées au profilage à haut risque.

32 Premièrement, toute opération de profilage à haut risque doit obligatoirement faire l'objet d'une analyse d'impact relative à la protection des données, dans le cadre de laquelle les risques pour les personnes concernées sont systématiquement évalués et, le cas échéant, des mesures correctives sont définies. Certes, l'article 22 al. 2 LPD ne mentionne pas explicitement le profilage à haut risque comme déclencheur de l'obligation de réaliser une analyse d'impact relative à la protection des données. Toutefois, le profilage à haut risque implique par définition un risque élevé pour les personnes concernées et, conformément à l'art. 22 al. 1 LPD, une analyse d'impact relative à la protection des données est obligatoire pour tout traitement présentant un risque aussi élevé. Le "risque élevé" se réfère toutefois uniquement au risque initial qui déclenche la réalisation d'une analyse d'impact relative à la protection des données. Dans le cadre de cette évaluation, le responsable du traitement peut conclure que le risque réel n'est pas élevé dans le cas concret ou qu'il ne doit plus être considéré comme élevé après la prise en compte des mesures correctives prévues. Dans une telle situation, le profilage reste certes un "profilage à haut risque" selon la

définition légale, mais il doit être traité par la suite comme un traitement de données sans risque élevé.

Deuxièmement, le consentement donné dans le cadre du profilage doit être explicite, conformément à l'art. 6 al. 7 let. b LPD, lorsque des responsables privés procèdent à un profilage à haut risque et qu'ils fondent ce profilage sur un consentement. L'article 6 al. 7 let. b, LPD fixe des exigences pour l'octroi d'un consentement valable, mais n'établit pas d'exigence générale de consentement pour le profilage à haut risque. Comme le profilage normal, le profilage à haut risque ne requiert un consentement que si un principe de traitement est violé et qu'il n'existe aucun autre motif justificatif. 33

Troisièmement, enfin, l'intérêt prépondérant n'entre pas en ligne de compte pour les examens de solvabilité lorsque l'examen repose sur un profilage à haut risque (art. 31 al. 2 let. c ch. 1 LPD). 34

Comme indiqué, le RGPD ne connaît pas le profilage à haut risque, mais prévoit certaines conséquences juridiques particulières lorsque le profilage est lié à une décision entièrement automatisée qui produit des effets juridiques à l'égard de la personne concernée ou qui l'affecte de manière significative de façon similaire. Entre autres, dans de telles constellations qualifiées, le RGPD exige également qu'une analyse d'impact sur la protection des données soit obligatoirement effectuée (art. 35 al. 3 let. a RGPD). Étant donné que dans la pratique des entreprises, il est rare que des décisions d'une telle portée soient prises, le seuil pour la réalisation obligatoire d'une analyse d'impact sur la protection des données en cas de profilage est plutôt plus élevé sous le RGPD que dans la LPD suisse. Le RGPD contient encore, de manière isolée, d'autres conséquences juridiques pour le profilage effectué en combinaison avec une décision individuelle automatisée, notamment une obligation d'information et de renseignement élargie, qui comprend également des indications sur la logique impliquée et sur les conséquences pour les personnes concernées. 35

V. CONSEILS PRATIQUES

Dans la pratique des entreprises, c'est surtout l'identification du profilage à haut risque qui est importante, car pour les responsables privés, des conséquences juridiques particulières ne sont liées qu'à de telles opérations de profilage, à commencer par l'obligation de réaliser une analyse d'impact 36

relative à la protection des données. Toutefois, comme nous l'avons vu, la question de savoir si le seuil de profilage à haut risque est atteint ou non dépend fortement des circonstances concrètes du profilage dans chaque cas. Il n'est donc pas facile d'opérationnaliser le concept de profilage à haut risque et de définir des critères généraux. En outre, même les activités de profilage qui ne sont pas qualifiées de "profilage à haut risque" au sens de la définition légale peuvent présenter un risque élevé dans un cas particulier et peuvent donc nécessiter une analyse d'impact relative à la protection des données.

37 Il y a de nombreuses raisons de ne pas utiliser des critères trop détaillés pour déterminer si une analyse d'impact relative à la protection des données doit être effectuée (analyse des seuils). Il est préférable d'intégrer l'évaluation des aspects personnels en tant que facteur de risque dans les processus d'examen et d'approbation des projets et, dans un deuxième temps, de vérifier, sur la base des circonstances concrètes, si l'on est en présence soit d'un profilage à haut risque tel que défini légalement, soit d'un profilage qui, pour d'autres raisons, présente un risque élevé pour les personnes concernées. D'un point de vue pratique, la réalisation d'une analyse d'impact relative à la protection des données est toujours recommandée lorsque le profilage atteint une certaine intensité ou lorsqu'il implique la combinaison de données provenant de différentes sources.

38 La mise en œuvre du profilage a également des répercussions sur la conception et la mise en œuvre des processus réglementaires de protection des données. En particulier, le profilage est important pour la mise en œuvre des processus d'information : tant les données personnelles utilisées dans le profilage ("input") que les nouvelles données et connaissances créées à l'aide du profilage ("output") devraient faire partie des informations fournies aux personnes concernées de manière appropriée et compréhensible. Les catégories de données traitées ou nouvellement créées dans le cadre du profilage ainsi que les finalités de traitement poursuivies par le profilage doivent ensuite être décrites dans la déclaration de protection des données. En revanche, le profilage lui-même ne doit pas être mentionné spécifiquement dans la déclaration de protection des données. Une explication du profilage peut toutefois être recommandée dans un souci de transparence, en tant que mesure de confiance. Les traitements de données en rapport avec le profilage doivent être documentés avec les indications nécessaires dans le registre des traitements conformément à l'art. 12 LPD.

Enfin, il est de bonne pratique de prévoir des possibilités permettant aux personnes concernées de s'opposer au profilage. Dans la pratique, ces possibilités d'opt-out peuvent être mises en œuvre par exemple par des fonctionnalités techniques permettant aux personnes concernées de désactiver ou d'empêcher de manière autonome les traitements de données ou les services liés au profilage - p. ex. la réception de mesures de marketing direct personnalisées. De telles possibilités d'opt-out rendent opérationnel le droit général d'opposition de l'art. 30 al. 2 let. b LPD et tiennent en outre compte de l'idée de "privacy by design". De plus, ces possibilités d'opt-out répondent de plus en plus aux attentes des clients qui souhaitent pouvoir influencer de manière pertinente le traitement de leurs données. 39

BIBLIOGRAPHIE

Artikel-29-Datenschutzgruppe, Leitlinien zur automatisierten Entscheidungsfindung im Einzelfall einschliesslich Profiling für die Zwecke der Verordnung 2016/679, angenommen am 3.10.2017 und zuletzt überarbeitet und angenommen am 6.2.2018, abrufbar unter https://www.dsb.gv.at/dam/jcr:768b9c7f-f0f6-45d7-b2aa-d113d121ea69/Leitlinien%20zu%20automatisierten%20Entscheidungen%20im%20Einzelfall%20einschlie%C3%9Flich%20Profiling%20f%C3%BCr%20die%20Zwecke%20der%20Verordnung%202016-679.pdf, besucht am 25.5.2023.

Buchner Benedikt, Kommentierung zu Art. 4 Nr. 4 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung, 3. Aufl., München 2020.

Bühlmann Lukas/Schüepp Michael, Begriff und Rechtsfolgen des Profilings im nDSG und der DSGVO, in: Jusletter 12.9.2022.

Ernst Stefan, Kommentierung zu Art. 4 DSGVO, in: Paal Boris P./Pauly Daniel A. (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl., München 2021.

Glatthaar Matthias, Keine Angst vor Profiling, in: Jusletter IT 30.9.2021.

Glatthaar Matthias/Schröder Annika, Kommentierung zu Art. 22 DSG, in: Blechta Gabor-Paul/Vasella David (Hrsg.), Basler Kommentar zum Datenschutzgesetz/Öffentlichkeitsgesetz, 4. Aufl., Basel 2023.

Jacot-Guillarmod Emilie, Le profilage à risque élevé de la nLPD : réflexions autour d'un monstre de Frankenstein, swissprivacy.ch, 24.8.2021, abrufbar unter https://swissprivacy.law/86/, besucht am 25.5.2023.

Klabunde Achim, Kommentierung zu Art. 4 DSGVO, in: Ehmann Eugen/Selmayr Martin (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl., München 2018.

Lorentz Nora, Profiling – Persönlichkeitsschutz durch Datenschutz? Eine Standortbestimmung nach Inkrafttreten der DSGVO, Tübingen 2020.

Rosenthal David, Das neue Datenschutzgesetz, in: Jusletter 16.11.2020 (zit. Datenschutzgesetz).

Rosenthal David, Der Entwurf für ein neues Datenschutzgesetz, in: Jusletter 27.11.2017 (zit. Entwurf).

Roth Simon, Das Profiling im neuen Datenschutzrecht, SZW 2021, S. 34 ff.

Rudin Beat, Kommentierung zu Art. 5, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Aufl., Bern 2023.

Scholz Philip, Kommentierung zu Art. 4 Nr. 4 DSGVO, in: Simitis Spiros/Hornung Gerrit/Spiecker gen. Döhmann Indra (Hrsg.), Datenschutzrecht – DSGVO mit BDSG, 1. Aufl., Frankfurt a.M. 2019.

Vasella David, Neues DSG: kein grundsätzliches Einwilligungserfordernis beim Profiling, auch nicht bei hohem Risiko, datenrecht.ch, 25.9.2020, abrufbar unter https://datenrecht.ch/neues-dsg-kein-grundsaetzlicheseinwilligungserfordernis-beim-profiling-auch-nicht-bei-hohem-risiko/, besucht am 25.5.2023 (zit. Einwilligungserfordernis).

Vasella David, Überlegungen zum Profiling mit hohem Risiko, datenrecht.ch, 23.11.2020, abrufbar unter https://datenrecht.ch/ueberlegungen-zum-profiling-mit-hohem-risiko/, besucht am 25.5.2023 (zit. Profiling).

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.7.2017, BBl 2017 S. 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 25.5.2023 (zit. Botschaft DSG).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 6 al. 3-5 LPD

Un commentaire de Caroline Gaul

PROPOSITION DE CITATION

Caroline Gaul, Commentaire de l'art. 6 al. 3-5 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Gaul, Art. 6 al. 3-5 LPD N. XXX.

Art. 6 Principes

[...]

[3] Les données personnelles ne peuvent être collectées que pour des finalités déterminées et reconnaissables pour la personne concernée et doivent être traitées ultérieurement de manière compatible avec ces finalités.

[4] Elles sont détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement.

[5] Celui qui traite des données personnelles doit s'assurer qu'elles sont exactes. Il prend toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Le caractère approprié de la mesure dépend notamment du type de

traitement et de son étendue, ainsi que du risque que le traitement des données en question présente pour la personnalité ou les droits fondamentaux des personnes concernées.

TABLE DES MATIÈRES

En bref ... 96
I. Généralités ... 96
A. Remarques préliminaires ... 96
B. Contexte et objectif de la norme ... 97
C. Destinataire des obligations ... 98
D. Conséquences juridiques et économiques d'une violation ... 98
E. Historique des différents principes de traitement ... 99
1. Principe de finalité et de transparence, art. 6 al. 3 LPD ... 99
2. Limitation dans le temps du traitement des données, art. 6 al. 4 LPD ... 99
3. Principe d'exactitude, art. 6 al. 5 LPD ... 100
II. Objet des dispositions ... 100
A. Principe de finalité et de transparence, art. 6 al. 3 LPD ... 100
1. Exigences ... 100
2. Exemples ... 102
3. Recommandations pour la mise en œuvre ... 105
B. Limitation dans le temps du traitement des données, art. 6 al. 4 LPD ... 106
1. Exigences ... 106
2. Recommandations pour la mise en œuvre ... 107
C. Principe d'exactitude, art. 6 al. 5 LPD ... 108
1. Exactitude des données ... 108
a. Exigences ... 108
b. Exemples ... 110
2. Obligation de s'assurer de l'exactitude des données, obligation de rectification et de suppression ... 111
a. Exigences ... 111
b. Exemples ... 111
3. Recommandations pour la mise en œuvre ... 112
Bibliographie ... 113
Matériaux ... 114

EN BREF

Les dispositions de l'art. 6 al. 3 LPD (**affectation à un usage précis et transparence**), de l'art. 6 al. 4 LPD (**limitation dans le temps du traitement des données**) et de l'art. 6 al. 5 LPD (**exactitude**) font partie des **principes de traitement**, qui sont les principes matériels les plus importants du droit de la protection des données. Ils sont essentiels pour la conception concrète du traitement des données.

Toute violation des principes de traitement constitue une atteinte aux droits de la personnalité des personnes concernées. Toutefois, l'atteinte à la personnalité peut être justifiée par le consentement de la personne concernée, par un intérêt prépondérant privé ou public ou par la loi. Cette différence essentielle par rapport au DSGVO de l'UE, selon lequel tout traitement de données nécessite une base juridique concrète, a également été maintenue dans la nouvelle LPD.

Contrairement au DSGVO de l'UE, la LPD ne prévoit pas d'amendes en cas de violation des principes de traitement des données. Cependant, une telle violation peut avoir de lourdes conséquences, notamment au vu des pouvoirs élargis du Préposé fédéral à la protection des données (PFPDT) dans le cadre de la nouvelle LPD. Celui-ci peut ordonner que le traitement des données soit adapté, interrompu ou même arrêté en tout ou en partie et que les données personnelles soient détruites en tout ou en partie. En outre, il convient de prendre en compte les éventuels droits (civils) des personnes concernées et en particulier les conséquences d'une **perte de confiance** et d'un **préjudice à la réputation**.

I. GÉNÉRALITÉS

A. Remarques préliminaires

1 Les dispositions de l'art. 6 al. 3 LPD (**affectation à une finalité précise et transparence**), de l'art. 6 al. 4 LPD (**limitation dans le temps du traitement des données**) et de l'art. 6 al. 5 LPD (**exactitude**) font partie, avec l'art. 6 al. 1 LPD (licéité), l'art. 6 al. 2 (proportionnalité et bonne foi) et l'art. 8 LPD (sécurité des données) font partie des **principes de traitement**, qui sont les principes matériels les plus importants de la protection des

données et les idées directrices de la loi. Les articles 6 al. 6 et al. 7 LPD (consentement) ne sont pas des principes de traitement, mais expliquent simplement les conditions du consentement.

Les principes de traitement de la LPD s'appliquent aussi bien aux personnes privées qu'aux organes fédéraux. Toute violation des principes de traitement constitue une **atteinte à la personnalité**. Cependant, pour les personnes privées, toute atteinte à la personnalité n'est pas illégale. Elle peut être justifiée par le consentement de la personne concernée, par un intérêt privé ou public prépondérant ou par la loi (art. 31, al. 1, LPD). Cette différence essentielle par rapport au DSGVO de l'UE, selon lequel tout traitement de données nécessite un motif justificatif (interdiction avec réserve d'autorisation), a été maintenue lors de la révision de la LPD. Ainsi, selon la loi suisse sur la protection des données, une base juridique n'est toujours requise pour les responsables privés du traitement des données que s'il y a effectivement atteinte à la personnalité. Contrairement au traitement des données par des personnes privées, le traitement des données par les autorités fédérales est également soumis à une base juridique (interdiction avec réserve d'autorisation) en vertu de la loi suisse sur la protection des données. Même si et dans la mesure où une telle base existe, les principes de traitement s'appliquent également. Ils constituent un droit de comportement directement applicable, dont la violation peut donner lieu à une action en justice de la part de la personne concernée. La question de savoir si et dans quelle mesure les autorités fédérales sont exceptionnellement dispensées de respecter les principes de traitement doit être déterminée sur la base de la législation. 2

Les principes du traitement des données s'appliquent à l'ensemble du cycle de vie du traitement des données, quels que soient les moyens et les procédures utilisés, et sont donc **neutres sur le plan technologique**, c'est-à-dire qu'ils ne font pas référence à des applications techniques ou commerciales spécifiques. 3

B. Contexte et objectif de la norme

Le législateur suisse a toujours souligné que la loi suisse sur la protection des données n'a pas pour but d'empêcher ou de restreindre les possibilités de développement dans le domaine des technologies de l'information. Il s'agit plutôt de développer en Suisse une politique des données cohérente et 4

tournée vers l'avenir. Dans ce contexte, le PFPDT a expressément déclaré que même dans le cadre de la nouvelle loi sur la protection des données, des risques de traitement potentiellement élevés ne constituent pas un argument décisif contre les projets de transformation numérique. Cependant, certaines **règles de base** doivent être respectées. Outre les autres principes de traitement, il s'agit notamment du principe de finalité (art. 6, al. 3 LPD) abordé ici, des dispositions relatives à la durée du traitement des données (art. 6, al. 4 LPD) et des exigences relatives à l'exactitude des données (art. 6, al. 5 LPD). Compte tenu de l'évolution rapide et dynamique des technologies de l'information, le respect de ces principes de traitement vise à empêcher tout traitement excessif, inapproprié ou incorrect des données.

C. Destinataire des obligations

5 Les obligations découlant des principes de traitement s'appliquent en premier lieu au **responsable du traitement** (art. 5 let. j LPD). Le sous-traitant ne traite les données personnelles que sur ordre du responsable du traitement (art. 5 let. k LPD) et peut se fonder sur les mêmes motifs justificatifs que le responsable du traitement (art. 9 al. 4 LPD).

6 Le sous-traitant n'est pas expressément mentionné en tant que tel comme destinataire des principes de traitement de l'art. 6 LPD, contrairement au principe (pénal) de traitement de la sécurité des données (art. 8 LPD, art. 61 let. c LPD) et à d'autres obligations de la LPD, par exemple l'art. 12 al. 1 LPD, art. 17 al. 2 LPD et au chapitre 3 de la LPD, qui obligent explicitement le responsable et/ou le sous-traitant.

D. Conséquences juridiques et économiques d'une violation

7 Les dispositions de l'art. 6 al. 3 LPD (limitation des finalités et transparence), de l'art. 6 al. 4 LPD (limitation dans le temps du traitement des données) et de l'art. 6 al. 5 LPD (exactitude) ne figurent pas dans la liste exhaustive des infractions pénales (art. 60 et suivants LPD). Une violation de ces principes de traitement n'est pas en soi punissable selon la LPD, même si elle n'est pas justifiée. Malgré une révision complète des dispositions pénales, rien n'a été modifié à ce sujet dans le cadre de la révision de la LPD. Cependant, la violation d'autres obligations liées à ces principes de traitement, par exemple l'obligation d'information, art. 19, 21 en relation avec l'art. 60 al. 1 let. b LPD,

est passible de sanctions. Des infractions pénales en dehors de la LPD peuvent également être prises en compte.

Les nouveaux **pouvoirs du PFPDT** découlant de la nouvelle loi sur la protection des données sont d'une importance capitale. En cas de violation des règles de protection des données, ils peuvent notamment conduire à une **interdiction des activités de traitement** ou à une décision de **destruction des données**. Dans son rapport d'activité 2022/2023, le PFPDT a déjà annoncé dans ce contexte qu'il intensifierait son activité de surveillance et augmenterait le nombre d'enquêtes. 8

En outre, une violation peut entraîner des droits légaux en vertu de la LPD (en particulier en vertu des art. 32 et 41 LPD) ainsi que des droits civils pour atteinte à la personnalité (art. 32 al. 2 LPD). 9

Outre les conséquences juridiques potentielles d'une violation des principes de traitement, il convient de prendre en compte dans la pratique la **perte de confiance** et l'**atteinte à la réputation** qui peuvent résulter d'une violation des principes de traitement et avoir un impact négatif à long terme sur le développement des affaires. 10

E. Historique des différents principes de traitement

1. Principe de finalité et de transparence, art. 6 al. 3 LPD

L'art. 6 al. 3 LPD associe les principes de finalité et de reconnaissabilité, qui figuraient dans l'aDSG dans deux alinéas distincts (art. 4 al. 3 aDSG et art. 4 al. 4 aDSG). La nouvelle formulation se rapproche de celle de l'art. 5 al. 4 let. b de la Convention 108 plus, en ce sens que les données personnelles ne peuvent être traitées que dans un but «déterminé» et «identifiable» pour les personnes concernées. Autre nouveauté : les données ne peuvent être traitées que de manière « compatible » avec cette finalité. La terminologie de cette disposition se rapproche ainsi de celle de l'art. 5 al. 1 let. b DSGVO. Cependant, il n'y a pas de changements matériels par rapport à l'aDSG. 11

2. Limitation dans le temps du traitement des données, art. 6 al. 4 LPD

L'art. 6 al. 4 LPD introduit expressément l'obligation de détruire ou d'anonymiser les données personnelles dès qu'elles ne sont plus nécessaires au traitement. Cela correspond aux exigences de la Convention 108 plus ainsi 12

qu'à l'art. 4 al. 1 let. e de la directive (UE) 2016/680 et à l'art. 5 al. 1 let. e DSGVO («limitation de la conservation»). Cette obligation n'est pas non plus nouvelle. Elle découlait déjà auparavant du principe général de proportionnalité (art. 4 al. 2 aDSG, art. 6 al. 2 LPD). En l'inscrivant explicitement dans la loi, le législateur a voulu souligner l'importance particulière de la limitation dans le temps du traitement des données à caractère personnel, qui s'impose dans le contexte du développement technologique et des possibilités de stockage presque illimitées.

3. Principe d'exactitude, art. 6 al. 5 LPD

13 Alors que le principe d'exactitude des données était jusqu'à présent souligné dans un article distinct (art. 5 aDSG), il a été intégré dans l'article 6 LPD en tant qu'alinéa 5 afin de réunir les principes les plus importants de la protection des données dans un seul article. Cette structure s'inspire de l'art. 5 de la Convention 108 plus, de l'art. 4 de la directive (UE) 2016/680 et de l'art. 5 du DSGVO. Le droit de rectification, qui figurait jusqu'à présent à l'art. 5 al. 2 aDSG, est désormais régi par l'art. 32 LPD.

II. OBJET DES DISPOSITIONS

A. Principe de finalité et de transparence, art. 6 al. 3 LPD

1. Exigences

14 Selon le principe de finalité et de transparence, les données personnelles ne peuvent être collectées qu'à des fins déterminées et reconnaissables par la personne concernée. Elles ne peuvent être traitées que de manière compatible avec cette finalité, art. 6 al. 3 LPD.

15 Selon la nouvelle formulation de la loi, l'identité des finalités n'est plus explicitement requise. Le traitement doit simplement être (en permanence) *compatible avec* la finalité initiale. Un traitement ultérieur à d'autres fins n'est autorisé que s'il n'est pas inattendu et ne peut être considéré comme inapproprié ou répréhensible.

16 Avant même l'entrée en vigueur de la nouvelle LPD, le Tribunal fédéral avait relativisé le principe de finalité dans un arrêt du 18 mars 2021 concernant la divulgation de données personnelles par un organe fédéral. Il avait alors

déclaré qu'on ne pouvait exiger une identité absolue des finalités, car cela limiterait trop l'entraide administrative prévue à l'art. 19 al. 1 aDSG. Dans tous les cas, le but de l'assistance administrative doit être au moins *compatible avec* le but de la collecte initiale des données personnelles. Le Tribunal fédéral avait déjà jugé que la «compatibilité» du traitement avec le but initial était suffisante en vertu de l'aDSG.

L'autre condition, à savoir la reconnaissabilité, doit être remplie tant en ce qui concerne la collecte des données personnelles que le but de leur traitement. Elle peut être considérée comme remplie si la collecte des données et la finalité de leur traitement ressortent clairement des circonstances ou si le traitement est prévu par la loi. Cette possibilité existe toujours, même si les termes « ressortent clairement des circonstances » et « ou sont prévus par la loi » de l'art. 4 al. 3 aDSG n'ont pas été repris dans le libellé de l'art. 6 al. 3 LPD. 17

Les exigences en matière de reconnaissabilité doivent être déterminées au cas par cas, en tenant compte des principes de proportionnalité et de bonne foi, art. 6 al. 2 LPD. Des finalités de traitement vagues, non définies ou imprécises ne sont en principe pas suffisantes, bien que cette caractéristique soit à nouveau évaluée en fonction des circonstances et qu'un équilibre doit être trouvé entre les intérêts des personnes concernées et ceux du responsable ou du sous-traitant et de la société. Dans l'affaire «Google Street View», le Tribunal fédéral a par exemple établi que le principe de finalité et de transparence n'était pas respecté si les véhicules de Google, sur lesquels sont installées des caméras, étaient visibles par les passants et les riverains. L'objectif de ces véhicules, qui consiste à parcourir systématiquement des rues (etc.) et à les photographier, puis à publier les photos sur Internet sans le consentement des personnes concernées, n'est pas facilement reconnaissable, même si Google Street View est très connu de la population suisse. 18

L'exigence de reconnaissabilité est étroitement liée à l'obligation d'informer prévue par l'art. 19 et suivants de la LPD. Il ne faut toutefois pas les confondre. Alors que l'exigence de reconnaissabilité est un principe de traitement pour lequel une violation peut éventuellement être justifiée (art. 31 LPD), ce n'est pas le cas pour la violation de l'obligation d'informer. Au contraire, la violation de l'obligation d'informer est punissable en vertu de l'art. 60 al. 1 let. b LPD. 19

2. Exemples

20 Le traitement ultérieur d'adresses à des fins d'**envoi publicitaire** enfreint le principe de finalité et de transparence si les adresses ont été collectées à l'origine dans un tout autre contexte, par exemple dans le cadre d'une campagne politique. L'analyse de données personnelles relatives aux **habitudes de consommation** (à des fins autres que la lutte contre la fraude) sur la base de paiements par carte de crédit ou de débit sans le consentement de la personne concernée est également interdite. De même, l'envoi de publicité non sollicitée par e-mail à des adresses inconnues et collectées de manière aléatoire sur Internet ou l'obtention par une entreprise privée d'adresses IP de titulaires de lignes proposant des téléchargements de copies pirates constitue une violation du principe de finalité et de transparence.

21 En revanche, l'utilisation d'une adresse à des fins publicitaires est autorisée par la loi sur la protection des données si la personne concernée a transmis son adresse dans le but de recevoir une **carte client** ou pour une commande (en ligne ou non) dans le cadre d'une finalité initialement reconnaissable.

22 Lors de l'envoi de newsletters publicitaires, les conditions découlant de la loi contre la concurrence déloyale, notamment l'art. 3 al. 1 let. o LCD («**article anti-spam**») doivent être respectées. Toute infraction peut entraîner des sanctions pénales. Lors de l'envoi de newsletters à l'étranger, il convient en outre de respecter le **droit national** en vigueur et les usages locaux, qui peuvent imposer des exigences encore plus strictes.

23 Le traitement de données «**sur stock**», c'est-à-dire sans finalité, enfreint à la fois le principe de proportionnalité et le principe de finalité et de transparence, et est donc illégal. Cependant, l'enregistrement et la conservation sans motif des **données secondaires de télécommunication** restent autorisés en Suisse. La conservation par la police des enregistrements issus de la **surveillance des lieux publics**, dans le cadre de laquelle les données sont collectées et traitées pour d'éventuelles enquêtes pénales, est également autorisée, du moins pendant un certain temps. En revanche, la Cour fédérale a considéré différemment les faits relatifs à l'utilisation (excessive) de **compteurs d'eau radio**. Dans ce cas, il n'y avait pas de finalité pour le stockage de certaines données et la nécessité de leur transmission.

24 Lors de la **transmission de données à des tiers**, il convient de vérifier si cette divulgation est toujours conforme à l'objectif initial. Cela s'applique

également à l'échange de données au sein des **entreprises d'un groupe**. En l'absence d'un privilège global du groupe, les entreprises du même groupe sont également considérées comme des tiers, à moins qu'elles ne traitent les données uniquement en tant que sous-traitants. Dans la pratique, il est souvent difficile de faire la distinction entre sous-traitant et responsable (commun). En fin de compte, il est essentiel de mettre en place une structure cohérente et de la rendre transparente. Par exemple, dans le **domaine des ressources humaines**, il est recommandé de préciser clairement la relation avec le groupe dans le contrat de travail. Lors du transfert de données à des tiers, il faut également tenir compte du fait que le principe de limitation de la finalité doit être respecté (non seulement, mais aussi) lors du traitement ultérieur des données par le destinataire.

Les **applications Big Data** telles que le **Data Warehousing** et le **Data Mining** sont confrontées à des défis particuliers en matière de limitation de la finalité et de transparence, car la nature même des analyses Big Data est telle que leur finalité concrète ne se révèle qu'une fois les données fusionnées sur la base des nouvelles connaissances acquises. 25

Les Big Data sont également la base la plus importante de l'**intelligence artificielle (IA)**, qui entre ainsi également en conflit avec le principe de limitation de la finalité et de transparence. La recevabilité des applications correspondantes doit être examinée au cas par cas. Souvent, lors du développement de systèmes d'IA et de la saisie de données d'apprentissage, l'objectif de traitement ultérieur ne peut pas encore être défini, par exemple si l'algorithme peut prendre en charge un grand nombre de tâches. En outre, les données d'apprentissage utilisées sont généralement collectées à des fins complètement différentes à l'origine (par exemple, lorsque des données librement disponibles sur Internet sont utilisées comme données d'apprentissage). Il est donc souvent difficile de savoir si leur traitement est encore «compatible» avec l'objectif initial. Une importance particulière sera accordée à une analyse différenciée des différents traitements de données dans le **cycle de vie de l'IA** (développement, saisie de **données d'apprentissage**, utilisation du résultat du système d'IA «**sortie**», etc.) ainsi qu'aux motifs justifiant le consentement, l'exécution du contrat et l'intérêt légitime. Selon la communication du PFPDT, les fabricants, fournisseurs et utilisateurs de systèmes d'IA doivent également rendre transparents les finalités, le fonctionnement et les sources de données des traitements basés 26

sur l'IA. L'autorité de contrôle française CNIL fournit des exemples concrets de finalités selon le DSGVO par les développeurs de systèmes d'IA :

Exemples de finalités considérées comme explicites et spécifiées :

- Développement d'un modèle de langage large (LLM) capable de répondre à des questions, de générer du texte en fonction du contexte (e-mails, lettres, rapports, y compris du code informatique), d'effectuer des traductions, des résumés et des corrections de texte, d'effectuer une classification de texte, une analyse des sentiments, etc. ;
- Développement d'un modèle de reconnaissance vocale capable d'identifier un locuteur, sa langue, son âge, son sexe, etc. ;
- Développement d'un modèle de vision par ordinateur capable de détecter différents objets tels que des véhicules (voitures, camions, scooters, etc.), des piétons, du mobilier urbain (poubelles, bancs publics, abris à vélos, etc.), des panneaux de signalisation, des feux tricolores, des panneaux de signalisation, etc.
- À l'inverse, l'objectif ne serait pas considéré comme suffisamment spécifié s'il ne faisait référence qu'au type de système d'IA, sans mentionner les fonctionnalités et capacités techniquement réalisables.

Exemples d'objectifs qui ne sont pas considérés comme explicites et spécifiés :

- Développement d'un modèle d'IA génératif (les capacités possibles ne sont pas définies) ;
- Développement et amélioration d'un système d'IA (ni le type de modèle ni les capacités possibles ne sont définis) ;
- Développement d'un modèle pour identifier l'âge d'une personne (le type n'est pas défini).

Dans ce cas, la CNIL recommande également, pour des raisons de transparence, que le responsable soit en mesure de déterminer à l'avance les capacités prévisibles du système d'IA qui présentent les risques les plus importants, que la finalité se réfère aux fonctionnalités qui sont exclues d'emblée et que la finalité définisse autant que possible les conditions d'utilisation du système d'IA.

En ce qui concerne les exigences de transparence, il convient également de tenir compte de la loi européenne sur l'IA, qui peut également s'appliquer aux entreprises suisses.

Le législateur suisse a également reconnu le potentiel de réutilisation des données à **des fins d'utilisation secondaire**. Le 12 juin 2023, le Conseil national a adopté en tant que deuxième conseil une motion visant à créer une **loi-cadre pour l'utilisation secondaire** des données. Le Conseil fédéral est ainsi chargé d'élaborer une loi visant à résoudre le conflit entre la protection des données et leur utilisation et à créer des espaces de données fiables. 27

Au niveau européen, il convient en outre de prendre en compte en particulier le Data Governance Act, le Data Act, la réglementation relative à l'espace européen des données de santé et, comme déjà mentionné, l'AI Act. Ces textes peuvent également s'appliquer aux entreprises suisses. 28

3. Recommandations pour la mise en œuvre

Les finalités du traitement des données doivent être définies, respectées en permanence et rendues transparentes. Dans la pratique, cela peut généralement être réalisé dans le cadre de la déclaration de protection des données qui est de toute façon nécessaire, au moins en partie selon le cas, par le biais des conditions générales de vente ou par le biais d'une communication/d'informations individuelles. Il convient de veiller à ce que des finalités de traitement vagues, non définies ou imprécises ne soient pas suffisantes. Le degré de précision requis doit être déterminé au cas par cas, en tenant compte des principes de proportionnalité et de bonne foi. En cas de transmission à des tiers, il est souvent recommandé de prévoir une disposition contractuelle stipulant que les données ne peuvent être traitées qu'à des fins spécifiques et légalement, et comprenant une obligation d'indemnisation. Il convient au moins de mentionner la finalité du traitement. 29

B. Limitation dans le temps du traitement des données, art. 6 al. 4 LPD

1. Exigences

30 Selon le principe de la limitation dans le temps du traitement des données, les données personnelles doivent être **détruites** ou **rendues anonymes** dès qu'elles ne sont plus nécessaires au traitement.

31 Néanmoins, un traitement ultérieur des données peut être justifié, art. 31 al. 1 LPD. C'est notamment le cas lorsque **des obligations de conservation** doivent être respectées, par exemple l'obligation de conserver pendant dix ans les livres comptables, les pièces comptables, le rapport de gestion et le rapport de révision ou les obligations de conservation en vertu du droit fiscal. Un intérêt légitime à la conservation peut également résulter de litiges juridiques potentiels futurs et de dispositions relatives à la prescription.

32 **La destruction** signifie au sens propre la destruction ou l'élimination irréversible des données. Pour les données sur papier, il faut les déchiqueter ou les brûler et s'assurer que des tiers n'ont pas accès aux « reliques ». Pour les données électroniques, il est important de savoir non seulement comment elles ont été stockées, mais aussi comment elles ont été obtenues. Si elles ont été transmises par clé USB, celle-ci doit être rendue inutilisable et toutes les copies doivent être traitées de manière à ce que les données ne puissent plus être lues. Si elles ont été transmises par e-mail, tous les enregistrements intermédiaires de cet e-mail doivent également être détruits. Par ailleurs, la destruction est soumise à des exigences élevées. Selon le message relatif à la LPD, les commandes d'effacement habituelles ou un simple reformatage ne constituent pas une destruction au sens de la législation sur la protection des données.

33 **La destruction** nécessite donc plus qu'**un effacement**. Néanmoins, la littérature considère que l'art. 6 al. 4 LPD est une erreur rédactionnelle et que le principe de limitation dans le temps peut également être respecté par un effacement. Cela est justifié par une reprise inconsidérée du terme « destruction » de la réglementation précédente de l'article 5 aDSG. En outre, les termes « destruction » et « effacement » seraient utilisés comme synonymes dans la LPD. Selon l'opinion locale, cela peut certainement être accepté si le terme d'effacement, qui n'est d'ailleurs défini ni dans la LPD ni

dans la DSGVO, est compris comme signifiant qu'aucune référence personnelle ne peut plus être établie, car alors la LPD n'est de toute façon pas (plus) applicable par définition en l'absence de données personnelles, art. 5 let. a. LPD. Selon l'approche de la LPD basée sur les risques, c'est déjà le cas si la mise en relation avec une personne n'est possible qu'au prix d'efforts considérables qu'aucun intéressé ne serait prêt à consentir. Il convient d'examiner au cas par cas si cela peut également être confirmé dans le cadre d'un **processus d'archivage**. Des mesures organisationnelles telles que le blocage des accès et le principe du double contrôle peuvent également être considérées comme suffisantes.

Le principe de la limitation dans le temps peut également être respecté par l'**anonymisation**. Par anonymisation, on entend toute mesure qui a pour effet que l'identité des personnes concernées ne peut plus être déterminée ou ne peut l'être qu'au prix d'efforts considérables. Il ne faut pas confondre anonymisation et **pseudonymisation**. La pseudonymisation consiste à remplacer le nom et d'autres caractéristiques d'identification par un autre identifiant, par exemple un caractère de remplacement, dans le but d'empêcher ou de rendre difficile l'identification de la personne concernée. En d'autres termes, la pseudonymisation permet de rétablir le lien avec la personne concernée à l'aide de la clé correspondante. Mais cela ne vaut que pour celui qui détient la clé. Cette **approche relative** a pour conséquence que pour celui qui ne détient pas la clé et qui est pratiquement exclu de l'obtenir, il n'existe pas non plus de données personnelles. Cette approche relative a des conséquences considérables dans la pratique, car elle exclut du champ d'application de la législation sur la protection des données celui qui ne détient pas la clé. 34

2. Recommandations pour la mise en œuvre

Dans la pratique, l'obligation de détruire ou d'anonymiser les données peut poser de grands défis aux responsables. Dans un premier temps, il est recommandé d'obtenir une vue d'ensemble des traitements de données habituels dans les différents secteurs d'activité. Il convient ensuite de fixer les délais de conservation et d'effacement respectifs. En pratique, cela se fait sous la forme de listes claires, qui servent également de directives internes («directive de conservation»/«Data Retention Policy»). 35

36 Il est utile pour la mise en œuvre que le logiciel utilisé pour le traitement des données offre déjà des fonctionnalités appropriées pour la suppression automatique, en veillant d'une part à ce qu'elles répondent techniquement aux exigences de la législation sur la protection des données et d'autre part à ce que l'obligation de suppression soit suffisamment couverte par contrat dans le cadre des contrats de traitement des données de commande avec le fournisseur informatique/fournisseur de cloud.

C. Principe d'exactitude, art. 6 al. 5 LPD

1. Exactitude des données

a. Exigences

37 Les données personnelles sont exactes si elles reflètent correctement les circonstances et les faits relatifs à la personne concernée. Elles doivent être exactes dans leur ensemble, en tenant compte de la finalité et de la nature du traitement. Il en résulte déjà que le terme d'exactitude dans le droit de la protection des données ne doit pas être compris de manière absolue, mais qu'une importance considérable est accordée au cas d'application concret.

38 Même des données personnelles correctes peuvent être considérées comme incorrectes au sens de la législation sur la protection des données si l'on tient compte du contexte global et de la finalité du traitement. C'est le cas par exemple lorsqu'une personne est enregistrée comme « poursuivie » dans une base de données sur la solvabilité, alors qu'elle a payé ses factures correctement et dans les délais pendant des années et qu'elle n'a été poursuivie que parce que la facture a été envoyée à une mauvaise adresse. D'un autre côté, les fausses déclarations ne sont pas nécessairement incorrectes au sens de la loi sur la protection des données. Ainsi, selon un arrêt du Tribunal fédéral, certaines informations ne peuvent être considérées comme fausses si l'ensemble des informations reflète correctement les faits réels. De même, les informations peuvent être tout à fait correctes au sens de « clichés instantanés », même si elles deviennent incorrectes par la suite, par exemple si un nom modifié entre-temps est encore mentionné dans un jugement. Dans ce cas, l'objectif pour lequel les données sont encore utilisées est décisif. Dans ce contexte, le principe d'exactitude doit être considéré de manière différenciée, en particulier dans le cadre des activités des archives, des musées, des bibliothèques et d'autres institutions de mémoire. Étant

donné que la mission de ces institutions est de collecter, d'indexer, de conserver et de transmettre des documents de toutes sortes, ceux-ci ne doivent pas être modifiés, car cela irait à l'encontre de l'objectif de l'archivage. Les archives permettent de prendre un instantané du passé à l'aide de documents, dont l'«exactitude» se réfère uniquement au fait que les documents en question sont reproduits fidèlement, indépendamment du fait que cela soit encore considéré comme correct d'un point de vue actuel. De même, la revendication d'exactitude dans les contrôles de police ne se réfère pas aux informations objectivement vérifiables sur les personnes concernées, mais à l'authenticité du procès-verbal. Le facteur décisif est de savoir si les données disponibles reflètent l'observation subjective de la personne autorisée au moment où l'évaluation a été effectuée.

L'exactitude des données ne peut en principe se référer qu'à **des faits** qui peuvent également être objectivement constatés. **Les jugements de valeur** sont subjectifs et peuvent difficilement être classés comme étant corrects ou incorrects. Il est alors difficile de faire la distinction lorsque les jugements de valeur et les faits sont mélangés. Cela a pris une importance particulière dans le contexte des «fake news». Par exemple, il est vrai ou faux d'indiquer qu'un jugement de valeur a été exprimé par une personne donnée ou documenté dans un dossier. Il est également vrai ou faux d'indiquer à qui se réfère le jugement de valeur. L'utilisation ultérieure du fait du jugement de valeur est également régie par les principes généraux de traitement. 39

Le respect du principe d'exactitude des données pose des défis particuliers en ce qui concerne les **systèmes d'IA**. En particulier dans le cas des systèmes d'IA dont les **données d'entraînement** proviennent de sources accessibles au public, notamment d'Internet, il est souvent impossible de vérifier efficacement l'exactitude des données. Les résultats du traitement des données par les systèmes d'IA (« **sortie de données** ») peuvent également être incorrects. D'une part, on ne peut pas supposer qu'une « exactitude statistique » soit suffisante pour le traitement des données dans le cadre des systèmes d'IA. D'un autre côté, les exigences imposées au traitement des données dans le cadre des systèmes d'IA ne doivent pas être plus élevées que pour les autres traitements de données, car la LPD est fondamentalement neutre sur le plan technologique. Cela signifie que la question de l'exactitude des données doit également être évaluée au cas par cas et en tenant compte du contexte global, même dans le cas du traitement des données dans le cadre des systèmes d'IA. 40

L'objectif du traitement des données, l'importance des résultats et les attentes des utilisateurs sont particulièrement pertinents à cet égard. Dans la pratique, il sera décisif d'informer les utilisateurs en conséquence. L'exigence connexe de vérification des résultats devrait également se refléter dans les « **AI Guidelines** » des entreprises.

41 En règle générale, le traitement de données incorrectes n'est pas en soi une atteinte à la personnalité. Ce n'est que si les données incorrectes entraînent une atteinte à la personnalité par leur traitement qu'elles doivent être rectifiées ou détruites. Le principe d'exactitude n'est pas non plus absolu. Une atteinte peut être justifiée pour les personnes privées qui traitent des données en vertu de l'art. 31 LPD. Pour les organes fédéraux, le droit à l'effacement peut également être limité (cf. art. 41 al. 3-5 LPD).

b. Exemples

42 Dans le cas du traitement d'**informations suspectes** concernant la commission d'éventuelles infractions, l'art. 6 al. 5 LPD ne s'oppose pas à un traitement tant que la pertinence de l'information correspondante est connue et que le soupçon ne semble pas être une connaissance confirmée. **Les e-mails archivés** qui, d'après les connaissances actuelles, contiennent des informations erronées sont néanmoins corrects au sens de la législation sur la protection des données, tant qu'ils ne sont pas traités en supposant qu'ils sont encore d'actualité. De même, la conservation de la **correspondance commerciale** est autorisée dans le cadre de l'obligation de conservation, même si elle contient des informations erronées. Si un numéro de rue est mal saisi dans la base de données d'adresses d'une association, qui ne sert pas à l'envoi postal mais uniquement au contrôle de l'effectif des membres, l'information ne doit pas être corrigée. Dans tous les cas, même pour un tel traitement de données, il convient de vérifier le respect des autres principes généraux de traitement, en particulier les principes de proportionnalité et de finalité.

2. Obligation de s'assurer de l'exactitude des données, obligation de rectification et de suppression

a. Exigences

Selon le principe d'exactitude, toute personne qui traite des données personnelles doit s'assurer de leur exactitude, art. 6 al. 5 phr. 1 LPD. L'art. 6 al. 5 phr. 2 LPD stipule en outre explicitement que toutes les mesures appropriées doivent être prises pour rectifier, effacer ou détruire les données inexactes. Cette obligation complète l'obligation de vérification, qui n'aurait sinon aucun sens. L'étendue de l'obligation de vérification dépend de chaque cas particulier. Il convient notamment de prendre en compte la finalité et l'étendue du traitement ainsi que le type de données traitées, la mesure dans laquelle les données sont divulguées et leur degré de sensibilité. C'est dans ce cadre que doit s'exercer l'obligation de vérification du responsable du traitement des données. Plus le risque d'atteinte à la personnalité est élevé, plus les exigences en matière d'obligation de vérification sont élevées. L'obligation de vérification peut donc également conduire à une **obligation d'actualisation**. Toutefois, elle n'implique pas une obligation générale de vérification régulière sans motif. 43

La mise en œuvre des mesures de vérification peut également être **déléguée**, par exemple à la source des données ou à un sous-traitant. En cas de violation de l'obligation de vérification, il y a infraction aux principes de traitement et donc atteinte à la personnalité, conformément à l'art. 30 al. 2 let. a LPD. Selon l'esprit et l'objectif de la loi, une telle violation de l'obligation ne peut donner lieu à des demandes de rectification et de dommages-intérêts que si les données sont effectivement incorrectes. Les mesures à prendre dépendent, entre autres, de la nature, de l'étendue et de la finalité du traitement des données, de la sensibilité des données et du risque pour les droits de la personnalité de la personne concernée. Cela doit à nouveau être déterminé au cas par cas. En outre, les obligations légales peuvent s'opposer aux mesures de rectification, de suppression ou d'actualisation. 44

b. Exemples

Si le traitement des données à des fins de marketing est basé sur **les propres informations de la personne concernée**, le responsable n'a pas à s'assurer de leur exactitude. De même, il n'y a pas d'obligation générale de vérifier en 45

permanence si les adresses figurant dans un fichier clients sont obsolètes à des fins de marketing. Cependant, si un assuré informe l'assureur d'un changement d'adresse, qui indique également un changement d'état civil, l'assureur doit ajouter l'état civil, dans la mesure où cela a des répercussions sur le versement de la prestation d'assurance. D'un autre côté, les informations déjà fournies dans une police d'assurance ne doivent pas être vérifiées à nouveau, dans la mesure où elles n'ont aucune influence sur la prime ou la prestation d'assurance. En ce qui concerne les agences de renseignements commerciaux, il convient de prendre en compte, lors de la vérification des données, en particulier le volume des données, l'existence de profils de personnalité et de consentements ainsi que le nombre de requêtes effectuées. Si une compagnie d'assurance souhaite utiliser l'**intelligence artificielle** (**IA)** pour établir un profil des clients qui souscrivent une assurance et utiliser ce profil comme base pour ses décisions lors du calcul du risque d'assurance, elle doit non seulement utiliser les données des clients existants provenant de sources de données contenant des informations correctes et à jour comme données d'entraînement, mais aussi utiliser un groupe de clients représentatif de la population afin d'éviter les distorsions.

3. Recommandations pour la mise en œuvre

46 Les exigences relatives aux mesures requises en vertu de l'art. 6 al. 5 LPD doivent être proportionnelles aux risques et aux conséquences de l'utilisation concrète. Voici quelques exemples de mesures à prendre, qui représentent également des aspects centraux dans le cadre de la conception technique selon les principes de **Privacy by Design** et **Privacy by Default** :

- vérification de la fiabilité de la source de données
- Détermination du degré d'exactitude en fonction des circonstances générales du cas individuel
- Le cas échéant, nouveaux contrôles des données en fonction des circonstances générales et des différentes phases du traitement des données
- Réduction des faux positifs / faux négatifs, par exemple pour réduire les erreurs dans la prise de décision automatisée et l'utilisation de l'intelligence artificielle
- Mise à jour des données si nécessaire pour les besoins du traitement

- Mise en place de solutions en libre-service permettant aux personnes concernées de vérifier elles-mêmes leurs données et de les corriger si nécessaire
- Introduction de contrôles de plausibilité et de qualité
- Mise en place de contrôles automatiques des saisies, par exemple pour éviter les saisies erronées de codes postaux
- Menus déroulants au lieu de saisie de texte libre

Du point de vue des responsables, il est également recommandé d'imposer par contrat aux personnes concernées l'obligation de fournir des données correctes et de les tenir à jour, et d'exclure toute responsabilité à cet égard, dans la mesure du possible. En principe, une obligation d'indemnisation devrait également être envisagée pour les sources de données externes. Selon le cas, cela peut être pris en compte dans le cadre d'un concept global qui comprend l'attribution des données et des responsabilités ainsi que d'autres droits et obligations connexes. 47

BIBLIOGRAPHIE

Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 3. Auflage, Basel 2014 (zit. BSK DSG-Bearbeiter:in [3. Auflage]) sowie 4. Auflage, Basel 2024 (zit. BSK DSG-Bearbeiter:in).

Basler Kommentar zum Geldwäschereigesetz, Basel 2021 (zit. BSK GWG-Bearbeiter:in).

Fischer Joel A./Bornhauser Jonas, Elektronische Board Portale: Hosted in Switzerland als neuer rechtlicher Qualitätsstandard, GesKR 2016, S. 425-448.

Gola/Heckmann, Datenschutzgrundverordnung/Bundesdatenschutzgesetz, 3. Auflage 2022 (zit. Gola/Heckmann DS-GVO/BDSG-Bearbeiter:in).

Hartmann Damian, Text and Data Mining and Copyright in Switzerland and the European Union, sic! 2023, S. 157-167.

Lobsiger Adrian, Hohes Risiko – kein Killerargument gegen Vorhaben der digitalen Transformation, SJZ 119 (2023), S. 311-319.

Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, 2023 (zit. OFK DSG- Bearbeiter:in).

Rosenthal David, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, Jusletter vom 17.6.2019.

Rosenthal David, Löschen und doch nicht löschen, digma 2019, S. 190-197.

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Rossnagel Alexander, Pseudonymisierung personenbezogener Daten, ZD 2018, 243 ff.; Stämpflis Handkommentar zum Datenschutzgesetz, 2. Auflage (zit. SHK DSG- Bearbeiter:in).

Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019 (zit. Specht/Mantz DSGVO/BDSG-Bearbeiter:in).

MATÉRIAUX

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988 II 413 ff. (zit. Botschaft DSG 1988).

Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8.11.2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19.2.2003 BBl 2002 2101 ff. (zit. Botschaft DSG 2003).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.12.2017, BBl 2017 6941 ff. (zit. Botschaft DSG 2017).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 6 al. 6 et 7 LPD

Un commentaire de Gaspare T. Loderer

PROPOSITION DE CITATION

Gaspare Loderer, Commentaire de l'art. 6 al. 6 et 7 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la Loi fédérale sur la protection des données

Citation abrégée: OK-Loderer, art. 6 LPD N. XXX.

Art. 6 Principes

[...]

6 Lorsque le consentement de la personne concernée est requis, celle-ci ne consent valablement que si elle exprime librement sa volonté concernant un ou plusieurs traitements déterminés et après avoir été dûment informée.

7 Le consentement doit être exprès dans les cas suivants:

a. il s'agit d'un traitement de données sensibles;

b. il s'agit d'un profilage à risque élevé effectué par une personne privée;

c. il s'agit d'un profilage effectué par un organe fédéral.

TABLE DES MATIÈRES

EN BREF ... 117
I. Généralités ... 117
A. Historique ... 117
B. Systématique et délimitation ... 118
C. Champ d'application ... 119
D. Comparaison avec le DSGVO ... 119
II. Conditions du consentement (art. 6 al. 6 LPD) ... 120
A. Généralités ... 120
B. Capacité de discernement ... 120
D. Un ou plusieurs traitements déterminés ... 121
E. Information adéquate ... 122
F. Caractère volontaire ... 124
G. Unicité ... 127
H. Forme ... 128
III. Consentement explicite (art. 6 al. 7 LPD) ... 129
IV. Révocation ... 130
V. Conséquences juridiques en cas d'absence de consentement, de consentement non valable ou de consentement révoqué ... 131
VI. Conseils pratiques ... 132
VII. Critique de la norme ... 132
Bibliographie ... 132
Matériaux ... 136

EN BREF

L'art. 6 al. 6 et 7 LPD statuent les conditions de validité des consentements en matière de protection des données. Les cas dans lesquels un consentement est requis sont par contre réglés dans d'autres dispositions. Le contenu des nouvelles dispositions relatives au consentement est pour l'essentiel identique à celui de l'art. 4 al. 5 aDSG. Il a simplement été précisé qu'un consentement doit être donné pour un ou plusieurs traitements déterminés, ce qui était déjà le cas jusqu'à présent. En ce qui concerne le consentement explicite, le profilage nouvellement introduit a remplacé le profil de la personnalité prévu par l'ancien droit. Pour le reste, la situation juridique ne devrait pas être modifiée. Dans la mesure où un consentement est requis, il doit donc, comme auparavant, être donné librement pour un ou plusieurs traitements déterminés, après une information appropriée. Si un consentement est requis pour le traitement de données personnelles sensibles, pour un profilage à haut risque par une personne privée ou pour un profilage par un organe fédéral, il doit en outre être explicite. Toutefois, même dans ces cas, il n'y a pas d'exigence générale de consentement, bien que certains soutiennent le contraire. Dans le champ d'application du RGPD, le consentement est plus souvent utilisé comme base juridique d'un traitement en raison de la différence de concept (principe d'interdiction avec réserve d'autorisation) et les exigences relatives à un consentement valable sont globalement plus élevées que sous la LPD.

I. GÉNÉRALITÉS

A. Historique

Le contenu de l'art. 6, al. 6 et al. 7 LPD correspond pour l'essentiel à celui de l'art. 4, al. 5 aDSG, quelques modifications rédactionnelles ayant toutefois été apportées dans le cadre de la révision totale. Le consentement explicite a été séparé du consentement "ordinaire" et réglé dans un alinéa séparé. En outre, il a été précisé que le consentement doit porter sur un ou plusieurs traitements déterminés. Cette concrétisation a été effectuée dans l'optique d'un rapprochement avec la convention STE 108 révisée. Il n'en résulte toutefois aucune modification de la situation juridique. En outre, comme la notion de profil de la personnalité a été remplacée par celle de profilage dans le cadre 1

de la révision totale, le consentement doit désormais être donné expressément pour un profilage à haut risque par des personnes privées ainsi que pour un profilage par des organes fédéraux.

2 Le critère du caractère univoque du consentement, introduit dans le projet, a été abandonné lors des débats parlementaires. Il avait également été introduit à l'origine dans l'optique d'un rapprochement avec la convention STE 108 révisée.

B. Systématique et délimitation

3 La loi suisse sur la protection des données est basée sur le principe de l'autorisation avec réserve d'interdiction. Selon ce principe, un traitement est en principe autorisé pour autant que les principes de traitement de l'art. 6 et la sécurité des données selon l'art. 8 LPD soient respectés, que les données personnelles ne soient pas traitées contrairement à la déclaration de volonté expresse de la personne concernée ou que des données personnelles sensibles ne soient pas communiquées à des tiers (art. 30 al. 2 LPD). Dans le cas contraire, il y a atteinte à la personnalité, qui peut être justifiée notamment par le consentement de la personne concernée (art. 31 al. 1 LPD).

4 L'art. 6 al. 6 et 7 LPD ne statuent donc pas sur une exigence générale de consentement, mais définissent uniquement les conditions dans lesquelles un consentement est valable. En revanche, la question de savoir si un tel consentement est nécessaire et dans quels cas est réglée ailleurs. De même, les cas visés à l'art. 6 al. 7 LPD (traitement de données personnelles sensibles, profilage à haut risque par une personne privée et profilage par un organe fédéral) ne requièrent pas en soi un consentement, même si certains soutiennent le contraire.

5 Malgré la position systématique des dispositions relatives au consentement sous l'art. 6 LPD intitulé "Principes", les conditions de validité des consentements ne constituent pas un principe de traitement en matière de protection des données. En particulier, il n'y a pas d'atteinte à la personnalité si les conditions du consentement ne sont pas respectées, bien que l'art. 30 al. 2 let. a LPD renvoie aux "principes" de l'art. 6 LPD. Pour cette raison, il aurait été préférable de déplacer les dispositions relatives au consentement vers les définitions de l'article 5 LPD.

C. Champ d'application

Pour les personnes privées, le consentement peut notamment justifier une atteinte à la personnalité (art. 31 al. 1 LPD). En outre, le consentement peut être pertinent pour les personnes privées dans les cas suivants : Pour la communication de données personnelles à l'étranger, en dérogation à l'article 16, al. 1 et 2 LPD (art. 17, al. 1, let. a LPD) ; pour des décisions individuelles automatisées, sans devoir respecter les conditions de l'article 21, al. 1 et 2 LPD (art. 21, al. 3, let. b LPD) ; dans le cadre du droit d'accès, pour la communication de données relatives à la santé par un professionnel de la santé (art. 25, al. 3 LPD). 6

Pour les organes fédéraux, le consentement peut remplacer au cas par cas l'exigence générale d'une base légale (art. 34 al. 4 let. b LPD) et ce, même en cas de communication de données personnelles à l'étranger (art. 36 al. 2 let. b LPD). 7

En outre, le consentement est également mentionné ailleurs dans la LPD et peut également être prévu par une loi spéciale. La question de savoir si et dans quelle mesure les conditions de la LPD s'appliquent dans ce cas n'est pas entièrement clarifiée, en particulier à l'intersection avec l'interdiction du spam selon l'art. 3 al. 1 let. o LCD. On part toutefois du principe que c'est le cas, du moins implicitement. 8

D. Comparaison avec le DSGVO

Le concept suisse se distingue fondamentalement du concept inverse du DSGVO. Celui-ci applique le principe d'interdiction avec réserve d'autorisation, selon lequel tout traitement de données personnelles est interdit, sauf s'il existe une base juridique pour le traitement (art. 6 RGPD). L'une de ces bases juridiques possibles est le consentement (art. 6 al. 1 let. a DSGVO). Ses conditions sont généralement décrites plus en détail à l'art. 4, point 11, et à l'art. 7 du RGPD, en ce qui concerne le consentement des enfants à l'art. 8 du RGPD et pour le traitement de catégories particulières de données personnelles, le consentement doit être explicite (art. 9, al. 2, let. a du RGPD). 9

Les conditions d'un consentement valable selon le RGPD sont plus strictes que celles de la LPD. Ainsi, un consentement valable selon le RGPD remplit 10

en principe les exigences de la LPD, tandis qu'un consentement valable selon la LPD ne satisfait pas nécessairement aux exigences accrues du RGPD.

II. CONDITIONS DU CONSENTEMENT (ART. 6 AL. 6 LPD)

A. Généralités

11 Le consentement est soumis aux "limites" générales du droit de la personnalité, dont font partie les dispositions des art. 16 ss. CC (capacité de discernement) et l'art. 27 CC (engagement excessif). Le consentement doit être qualifié d'acte juridique unilatéral, raison pour laquelle le CO s'applique en particulier dans le domaine de l'interprétation du consentement (principe de confiance), des limites des art. 19 et 20 CO ainsi que des vices du consentement (art. 23 ss. CO).

B. Capacité de discernement

12 L'octroi d'un consentement en matière de protection des données constitue l'exercice d'un droit strictement personnel et peut donc être exercé de manière autonome par des personnes incapables de discernement (art. 19c al. 1 CC). En revanche, pour les personnes incapables de discernement, c'est en principe leur représentant légal qui agit (art. 19c al. 2 CC). Les parents peuvent donner un consentement pour les enfants incapables de discernement dans le cadre de leur représentation légale et dans la mesure de l'autorité parentale qui leur revient (art. 304 CC).

13 Est capable de discernement toute personne qui n'est pas dépourvue de la faculté d'agir raisonnablement en raison de certains états (enfance, handicap mental, troubles psychiques, ivresse ou autres) (art. 16 CC). En règle générale, la capacité de discernement est présumée chez les mineurs à partir de 13 ans. En raison de la relativité de la capacité de discernement, les exigences doivent être plus élevées, par exemple en cas de traitements complexes, de données personnelles sensibles et d'atteintes graves à la personnalité.

C. Moment

14 Le consentement doit en principe être donné avant le traitement des données, ce qui peut être par exemple avant la collecte ou la communication des données (cf. art. 5 let. d LPD). Si un consentement est requis et qu'il n'existe pas, le traitement de données correspondant est illégal.

Un consentement a posteriori au sens propre du terme est exclu. Toutefois, une autorisation a posteriori peut être envisagée, qui doit être interprétée comme une renonciation à faire valoir des droits. Jusqu'au moment de l'autorisation a posteriori, le traitement des données est toutefois illégal. En outre, l'autorisation a posteriori ne s'étend qu'au traitement de données pour lequel une information appropriée a été fournie initialement ou ultérieurement. 15

D. Un ou plusieurs traitements déterminés

Le critère selon lequel le consentement doit porter sur un ou plusieurs traitements déterminés a été ajouté lors de la révision totale. De ce fait, la formulation s'aligne globalement sur l'article 5 al. 2 de la convention STE 108 révisée, sans toutefois entraîner une modification de la situation juridique. 16

Comme dans l'ancien droit, il est nécessaire que le traitement soit suffisamment défini, notamment en ce qui concerne son étendue et sa finalité. La personne concernée doit pouvoir comprendre pour quels traitements elle donne son consentement. La portée concrète du consentement résulte de la déclaration de consentement et de l'information appropriée. Les descriptions de finalités générales telles que "l'amélioration de l'expérience de l'utilisateur", "à des fins publicitaires", "à des fins de sécurité informatique" ou "de recherche future", par exemple, ne sont pas suffisantes sans autres informations. Les traitements peuvent être limités ou non dans le temps. Toutefois, un consentement au cas par cas est parfois nécessaire. 17

Le consentement à plusieurs traitements n'implique pas que ceux-ci soient tous de même nature, mais il est également possible de consentir à différents traitements. Par ailleurs, un but de traitement tel que le traitement médical chez un médecin peut nécessiter différents traitements, par exemple l'échange de données personnelles sensibles avec d'autres spécialistes ou des assurances ainsi que le traitement à des fins de facturation. 18

La question de savoir dans quelle mesure les consentements généraux sont admissibles est controversée. Dans tous les cas, les limites du consentement doivent être claires et, en vertu du principe de proportionnalité, celui-ci doit être d'autant plus clair que le type et l'étendue du traitement sont sensibles. Ne sont donc pas admissibles les déclarations de consentement illimitées à n'importe quelle fin, pour n'importe quel traitement ou pour toutes les 19

catégories de données personnelles par des responsables de traitement illimités. En revanche, il est par exemple permis d'autoriser l'ancien employeur à fournir des renseignements généraux à des employeurs potentiels, ce qui requiert un consentement exprès en cas de communication de données personnelles sensibles (comme des informations sur des absences dues à des maladies).

E. Information adéquate

20 Le consentement en matière de protection des données s'oriente vers le "consentement éclairé du patient", de sorte que toutes les informations doivent être communiquées dans un cas concret pour que la personne concernée puisse prendre une décision libre. En d'autres termes, il s'agit de faire en sorte que la personne concernée sache clairement ce à quoi elle consent, c'est-à-dire qu'elle connaisse la portée de son consentement. La question de savoir quelles informations concrètes doivent être fournies ne faisait déjà pas l'objet d'une appréciation uniforme sous l'ancien droit et ne le sera pas non plus sous le nouveau droit.

21 Selon l'avis défendu ici, les exigences en matière d'information adéquate peuvent s'inspirer du devoir d'information selon l'art. 19 LPD. En effet, l'information adéquate requise pour un consentement peut conduire à une exception au devoir d'information selon l'art. 19 LPD, car la personne concernée dispose déjà des informations correspondantes (art. 20 al. 1 let. a LPD).

22 Cela ne signifie pas pour autant que toutes les informations visées à l'art. 19 LPD doivent être fournies dans tous les cas comme base de l'information adéquate selon l'art. 6 al. 6 LPD, même si une telle approche intégrative peut s'imposer dans la pratique. Selon le point de vue défendu ici, l'information adéquate dans le cadre des consentements nécessite au moins les données suivantes :

- Identité du responsable ;
- Finalité du traitement ;
- (catégories) de données personnelles traitées.

23 Le degré de détail de ces informations et la nécessité de fournir des informations supplémentaires dépendent des circonstances du cas d'espèce.

En application du principe de proportionnalité, l'information adéquate doit en principe être d'autant plus claire que les données personnelles concernées sont sensibles. Par exemple, l'art. 16 al. 2 LRH concrétise, entre autres, pour les consentements à des projets de recherche, qu'il faut également informer sur les risques et les contraintes prévisibles ainsi que sur les mesures de protection des données personnelles collectées. Selon l'art. 8 al. 1 OHF, il faut en outre informer sur le droit de refus ou de révocation et sur les conséquences d'une révocation ainsi que, de manière générale, sur d'autres contenus nécessaires à la décision.

Contrairement à l'art. 7 al. 3 RGPD, la LPD n'exige en principe aucune information sur le droit de révocation et sur le fait que la révocation n'affecte pas la légalité du traitement fondé sur le consentement jusqu'à la révocation. L'absence d'information à ce sujet n'invalide donc pas le consentement donné. 24

Le RGPD exige en outre que le consentement puisse être révoqué aussi facilement qu'il a été donné. Le PFPDT a également exigé cela pour l'aDSG en se fondant sur le principe de la bonne foi. La loi ne contient toutefois aucun fondement à cet égard et cette opinion doit donc être rejetée. En revanche, le caractère volontaire du consentement peut être remis en question si celui-ci ne peut pas être retiré de manière raisonnable. 25

Certains estiment, conformément aux explications du message 2003, qu'il faut informer des conséquences négatives ou des inconvénients du refus du consentement. Selon le point de vue défendu ici, cela ne constitue pas le contenu nécessaire d'une information appropriée, mais peut, selon les conséquences négatives, remettre en question la validité du consentement en raison de son caractère non volontaire. En revanche, il convient d'informer sur les risques éventuels du traitement des données. 26

L'information adéquate doit en principe être fournie par le responsable du traitement. Il est toutefois possible d'obtenir le consentement pour le traitement par un tiers. Cela nécessite régulièrement la mention du nom du tiers, à moins que cette indication ne ressorte suffisamment clairement des circonstances, comme cela peut être le cas par exemple dans le cas de sociétés de groupe. 27

Les informations mises à disposition doivent être interprétées selon le principe de confiance, c'est-à-dire comme la personne concernée pouvait et devait les comprendre. Il faut partir du principe qu'il s'agit d'une personne 28

moyennement compréhensive parmi les destinataires visés. Il faut donc rejeter l'opinion de la doctrine qui souhaite plutôt se baser sur les capacités de la personne concernée individuellement.

29 L'information appropriée doit être précise, transparente et compréhensible. Elle devrait être rédigée dans la langue dans laquelle le responsable fournit les prestations qui sont à la base du traitement. La forme de l'information peut être orale ou écrite ; pour des raisons de preuve, il est toutefois recommandé de fournir une preuve sous forme de texte. Si les informations relatives au traitement auquel le consentement est donné doivent être morcelées et rassemblées dans un document à partir de plusieurs endroits, cela peut constituer un argument contre l'existence d'une information adéquate.

30 Il doit être possible de prendre connaissance de l'information avant de donner le consentement. Un délai de réflexion peut être indiqué en fonction de la sensibilité du traitement. Ainsi, l'art. 16 al. 3 LRH exige par exemple l'octroi d'un délai de réflexion raisonnable avant que la personne concernée ne donne son consentement à un projet de recherche.

31 Le fait que l'information soit effectivement prise en compte n'a pas d'importance. Seul est déterminant le fait qu'il y ait eu une possibilité raisonnable de prendre connaissance de l'information. En cas d'acceptation globale, c'est-à-dire de consentement donné sans avoir pris connaissance de l'information (parce que celle-ci ne figure par exemple que dans des conditions générales liées ou dans une déclaration de protection des données), les clauses inhabituelles ne sont pas applicables (règle de l'inhabituel). Il peut donc être utile de mettre en évidence les aspects inhabituels.

F. Caractère volontaire

32 Le consentement doit être donné volontairement, c'est-à-dire être l'expression de la libre volonté de la personne concernée. Il existe une interaction avec la nécessité d'une information adéquate. En l'absence d'informations appropriées, le consentement ne peut pas être considéré comme volontaire. En outre, le consentement n'est pas libre lorsqu'il a été obtenu par tromperie, menace ou contrainte.

33 La LPD ne connaît pas d'interdiction de couplage inspirée de l'art. 7 al. 4 RGPD, dont l'existence et la portée sont controversées dans le cadre du

RGPD. Néanmoins, le droit suisse connaît également des formes de couplage illicite du consentement, dont les obstacles sont toutefois plus élevés que dans le cadre du RGPD. Un consentement ne doit notamment pas être libre lorsqu'un refus de consentement entraîne un désavantage qui n'a aucun rapport avec la finalité du traitement ou qui est disproportionné par rapport à celle-ci. En revanche, un autre inconvénient résultant d'un refus de consentement n'affecte pas la validité du consentement.

Exemples : Le consentement à la vérification de la solvabilité en vue de l'obtention d'une carte de crédit est donné volontairement et est admissible, car sans consentement, le désavantage de ne pas obtenir la carte de crédit est proportionnel. L'impossibilité de participer à un programme d'assurance a un rapport direct avec le traitement des données pour lequel un consentement est demandé ; et le fait que l'on fasse de la publicité pour des avantages pécuniaires et des bonus en espèces d'un montant maximal de 75 CHF par an pour les personnes ayant uniquement une assurance de base ne remet pas non plus en question le caractère volontaire du consentement. En revanche, la menace de licenciement en cas de non-consentement à un traitement de données non prévu dans le contrat de travail est considérée comme non volontaire, car disproportionnée. 34

Le caractère volontaire n'est parfois admis que lorsqu'il existe une alternative raisonnable. Selon le point de vue défendu ici, il n'est pas nécessaire de disposer d'une alternative pour admettre le caractère volontaire, sauf dans des situations exceptionnelles (notamment en cas de position dominante sur le marché ou de dépendance sociale ou factuelle). C'est pourquoi la personne concernée peut en principe se voir refuser l'accès à une prestation si elle ne donne pas son consentement. 35

La question du caractère volontaire du consentement est particulièrement controversée dans les relations de travail. Certains affirment que le caractère volontaire nécessaire fait défaut dans ce contexte ou que tout traitement de données allant au-delà de l'art. 328b CO est illicite. D'autres auteurs considèrent que le cadre du caractère volontaire est simplement plus étroit, dans la mesure où, par exemple, les employés doivent disposer d'une alternative raisonnable. La doctrine dominante et le PFPDT considèrent qu'un traitement de données allant au-delà de l'art. 328b al. 1 CO n'est admissible que s'il est avantageux pour les employés ou dans leur intérêt (art. 362 CO). D'autres auteurs considèrent que des consentements dérogeant à 36

l'art. 328b CO, même en défaveur des employés, sont valables dans certaines circonstances. Selon le Tribunal fédéral, un traitement de données contraire à l'art. 328b CO est certes illégal, mais peut être fondé sur un motif justificatif selon l'art. 13 aDSG. Selon ce point de vue, l'art. 328b CO est donc un principe de traitement et non une norme d'interdiction. Les explications succinctes à ce sujet sont toutefois critiquées par la doctrine. Le Tribunal fédéral a par la suite confirmé son point de vue, sans toutefois se référer à sa décision antérieure.

37 Selon l'opinion défendue ici, les consentements ne sont pas exclus en soi dans les rapports de travail et il est possible de consentir à des traitements qui vont au-delà de l'art. 328b al. 1 CO. L'élément déterminant est de savoir si l'on a été informé de manière adéquate et si l'on peut partir du principe que le consentement est effectivement libre, c'est-à-dire qu'il peut être refusé sans conséquences négatives. Par exemple, il est possible de consentir à la publication sur Internet de photos de collaborateurs sans contact avec la clientèle, voire à des fins publicitaires, dans la mesure où l'on a été informé du traitement correspondant et où les employés disposent d'une liberté de choix effective. La position de l'employé ainsi que le cycle de vie de l'employé (candidature, contrat de travail en cours, fin du contrat) peuvent être déterminants pour cette évaluation. En revanche, il faudrait partir du principe qu'il n'y a pas de libre choix dans le dernier exemple cité au n. 34.

38 Dans le contexte européen, il convient de prendre en compte la question du caractère volontaire, surtout dans le domaine des bannières de cookies, de ce que l'on appelle les dark patterns ou le nudging. Le fait d'inciter l'utilisateur à donner son consentement, par exemple en utilisant des couleurs et des tailles différentes pour les boutons "Accepter" et "Refuser" ou en augmentant la charge de travail pour le refus (par exemple en ne proposant un bouton "Refuser tout" qu'au deuxième niveau de présentation, après avoir cliqué sur "Continuer"), remet en question le caractère volontaire selon la jurisprudence et l'avis des autorités de surveillance. Il n'est pas certain que cette évolution prenne de l'importance en Suisse. En effet, selon le droit suisse, il n'est en principe pas nécessaire d'obtenir le consentement pour les cookies. L'art. 45c let. b LTC, déterminant à cet égard, exige seulement que les utilisateurs soient "informés du traitement et de son but et qu'ils soient avertis qu'ils peuvent refuser le traitement". A cet égard, il convient toutefois d'observer l'évolution future, car le PFPDT et d'autres voix s'accordent à dire que le tracking

constitue en règle générale une atteinte à la personnalité qui doit être justifiée.

Le DSGVO exige que le consentement puisse être donné de manière granulaire pour différentes opérations de traitement. C'est l'une des raisons pour lesquelles les bannières de cookies conformes au droit européen offrent souvent la possibilité de donner son consentement séparément pour chaque cookie. On peut certes discuter de la pertinence d'une telle granularité pour les cookies. Il est en effet peu probable qu'une personne souhaite donner son consentement pour certains cookies et pas pour d'autres. Comme une telle exigence de granularité ne peut en tout cas pas être déduite de la LPD, elle peut tout au plus être exigée dans des cas exceptionnels. 39

G. Unicité

Le projet de LPD prévoyait encore que le consentement devait être donné "sans équivoque". Le message précise à ce sujet que la déclaration de la personne concernée doit faire apparaître sa volonté sans équivoque, ce qui dépend des circonstances du cas d'espèce, et que le consentement doit être d'autant plus clair, en vertu du principe de proportionnalité, que les données personnelles en question sont sensibles. 40

Le Parlement a toutefois abandonné l'exigence de clarté et ne l'a donc pas reprise dans le texte de l'art. 6 al. 6 LPD. Le fait que le message se réfère à ce critère a apparemment semé la confusion dans la doctrine. 41

Le message de 2003 avait déjà précisé qu'en vertu du principe de proportionnalité, le consentement devait être d'autant plus clair que les données personnelles en question étaient sensibles. La clarté de la déclaration de volonté est donc concernée, ce qui établit des parallèles avec le critère de "l'acte confirmant sans équivoque" que l'on trouve dans le DSGVO. En tant qu'alternative à la "déclaration", il s'agit du deuxième cas d'application de la "manifestation de volonté sans équivoque" selon l'article 4, point 11, du DSGVO. En l'absence d'un critère correspondant dans la LPD, on ne peut toutefois pas en déduire, contrairement au RGPD, que le consentement au moyen de cases pré-cochées, par exemple, n'est pas admissible. Cela n'est pas non plus nécessairement en contradiction avec la condition du "privacy by default" selon l'art. 7 al. 3 LPD. 42

43 En revanche, une interprétation du critère de clarté conforme à la convention STE 108 révisée exigerait qu'un consentement soit donné "sans équivoque". Cette exigence peut se rapporter tant à la forme qu'au contenu de la déclaration. Le message laisse entendre que l'élément se référait à la forme. Dans la mesure où cela devrait être le cas, le législateur a tenu compte de cette exigence de forme en précisant qu'un consentement donné par silence n'est en principe pas suffisant. Dans la mesure où le contenu doit être concerné, le principe selon lequel les exigences varient en fonction du principe de proportionnalité s'applique de toute façon. En droit suisse, le critère de l'unicité n'aurait donc pas de signification propre.

H. Forme

44 Le consentement peut être donné sans forme particulière. Hormis les exceptions prévues par la loi, les consentements oraux sont donc également possibles. Étant donné que la charge de la preuve d'un consentement incombe au responsable du traitement des données, un consentement pouvant être documenté s'impose toutefois. Cela relativise, du moins dans les faits, la liberté de forme fondamentale.

45 En principe, les consentements peuvent également être obtenus dans le cadre de conditions générales. Si une reprise globale est effectuée, la règle de l'inhabituel s'applique, selon laquelle les consentements inhabituels au détriment de la personne concernée ne sont pas valables. En outre, la règle de l'ambiguïté s'applique, selon laquelle les formulations peu claires sont en cas de doute à la charge de l'auteur.

46 Hormis le cas où l'art. 6 al. 7 LPD exige une expression explicite, le consentement peut également être donné de manière implicite. Dans ce cas, la déclaration de volonté ne résulte pas de la déclaration elle-même, mais d'un comportement qui, au vu des circonstances, peut être compris comme une expression claire de la volonté. C'est le cas, par exemple, lorsque la personne concernée rend elle-même ses données accessibles.

47 Pour le consentement implicite, on utilise souvent le synonyme de consentement tacite, ce qui est toutefois à éviter. En effet, le silence ou l'inaction n'entraîne en principe pas un consentement valable (cf. art. 6 CO), à moins que les parties n'aient convenu que le silence valait consentement.

Dans des cas exceptionnels, un consentement présumé est envisageable en cas d'urgence, par exemple dans le cas de patients inconscients. L'importance de tels consentements est toutefois négligeable, car dans ces cas, une justification fondée sur l'intérêt prépondérant de la personne concernée s'appliquerait de toute façon. Une distinction est parfois faite entre le consentement présumé et le consentement hypothétique. Ainsi, le consentement est valable malgré l'absence d'informations adéquates, car la personne concernée aurait donné son consentement même si elle avait été informée de manière complète. Il n'y a en revanche guère de place pour cela, sauf si la personne concernée l'autorise ultérieurement sous la forme d'une renonciation à faire valoir ses droits. 48

III. CONSENTEMENT EXPLICITE (ART. 6 AL. 7 LPD)

Si un consentement est requis pour le traitement de données personnelles sensibles, un profilage à haut risque par une personne privée ou un profilage par un organe fédéral, celui-ci doit être explicite. Il n'y a donc pas non plus d'exigence générale de consentement pour ces opérations de traitement. Bien que des déclarations faites lors des débats parlementaires aient parfois suggéré le contraire, que le libellé de l'art. 6, al. 7, LPD ne l'anticipe pas en introduction, contrairement à celui de l'art. 6, al. 6, LPD, et que le PFPDT et la doctrine défendent en partie le contraire, cela résulte de la clarification apportée lors des débats parlementaires et du fait qu'aucune modification de la situation juridique ne devrait intervenir. 49

Le critère de l'expressivité doit être pris en compte en plus des conditions de l'art. 6 al. 6 LPD. L'art. 4 al. 5 aDSG ainsi que l'avant-projet de LPD l'exprimaient mieux, car le consentement "normal" ainsi que le consentement explicite étaient réglés dans le même alinéa et l'ajout "en outre" l'avait précisé. 50

La question de savoir si l'élément de renforcement de l'expressivité se rapporte uniquement à la forme ou également au contenu du consentement est controversée. En ce qui concerne la forme, l'expression est comprise comme le contraire de l'implicite. Un consentement écrit n'est toutefois pas exigé. En vertu de l'art. 1 CO, la question de l'expressivité est déterminée par le fait que la volonté exprimée ressort directement de la déclaration de volonté sous forme de mots écrits ou parlés ou d'un signe. En d'autres termes, l'expression de la volonté en tant que telle doit déjà, par sa manière, apporter une clarté sur la volonté. Des exemples de signes explicites sont le fait de 51

cocher activement une case, de sélectionner activement certains paramètres techniques pour des services informatiques, de hocher la tête en signe de consentement dans le cadre de traitements médicaux ou d'ouvrir la bouche pour prélever la muqueuse de la joue après avoir été informé en conséquence. Pour des raisons de charge de la preuve, un consentement pouvant être documenté s'impose toutefois à nouveau.

52 Selon une partie de la doctrine et le PFPDT, l'expressivité se réfère également au contenu. Dans le cas d'un consentement explicite, le comportement affirmatif doit se référer au traitement de données concerné et non pas seulement à l'acte qui a pour seule conséquence ce traitement de données. Un consentement à la réception de publicité personnalisée n'impliquerait donc pas un consentement explicite au profilage à haut risque sur lequel repose la publicité.

53 Selon le point de vue défendu ici, l'exigence d'expressivité se réfère à la forme du consentement et non à son contenu. Le message 2003 précise que "le consentement n'est pas lié à une forme particulière et peut être donné tacitement ou de manière implicite, pour autant qu'il ne s'agisse pas du traitement de données sensibles ou de profils de la personnalité. Aujourd'hui déjà, conformément au principe de proportionnalité, on part du principe que le consentement doit être d'autant plus clair que les données personnelles en question sont sensibles". Pour la deuxième phrase, le message renvoie à une référence bibliographique qui comprend expressément comme terme opposé à implicite. L'élément d'interprétation historique confirme cette constatation, d'autant plus que, selon le message de 2017, il ne faut pas s'écarter de la situation juridique actuelle.

IV. RÉVOCATION

54 Un consentement peut être révoqué à tout moment et sans justification. Une révocation en temps inopportun peut toutefois entraîner une obligation de dédommagement. Une révocation n'a d'effet que pour l'avenir, de sorte que la légalité des traitements déjà effectués n'est pas affectée par la révocation. Les traitements de données effectués jusqu'à présent peuvent toutefois être contestés en raison de vices de consentement. Les données traitées sur la base d'un consentement doivent être effacées le cas échéant, dans la mesure où il n'existe pas d'autre justification pour la poursuite du traitement sous la forme d'une conservation permanente.

Selon le Tribunal fédéral, les biens de la personnalité qui ne font pas partie du noyau de l'existence humaine, tels que le nom, la voix ou l'image, peuvent être aménagés de manière irrévocable, dans la mesure où les intérêts économiques sont au premier plan de l'engagement contractuel. Il n'est toutefois pas évident de savoir dans quelle mesure ces considérations sur le droit à l'image peuvent être généralisées. En effet, dans le cas à juger, il était notamment décisif qu'une révocation soit possible contre le paiement d'une indemnité de résiliation modérée sous forme de peine conventionnelle. 55

V. CONSÉQUENCES JURIDIQUES EN CAS D'ABSENCE DE CONSENTEMENT, DE CONSENTEMENT NON VALABLE OU DE CONSENTEMENT RÉVOQUÉ

Si un traitement déterminé nécessite un consentement et que celui-ci n'est pas donné (à temps) ou qu'il ne remplit pas les conditions de validité, le traitement correspondant est illicite ou constitue une atteinte à la personnalité. Si un traitement est poursuivi malgré la révocation d'un consentement, il s'agit également d'une atteinte à la personnalité (art. 30 al. 2 let. b LPD). 56

Dans ces cas, un responsable peut invoquer subsidiairement d'autres motifs justificatifs (art. 31 LPD). En revanche, si aucun autre motif justificatif ne s'applique, il existe des droits à l'encontre des responsables privés (art. 32 al. 2 LPD) ou des organes fédéraux (art. 41 LPD) et, le cas échéant, des mesures d'enquête et administratives sont prises par le PFPDT (art. 49 ss LPD). 57

Une violation de l'art. 6 al. 6 et 7 LPD n'est pas directement punissable. Une sanction indirecte est toutefois envisageable, notamment en cas de communication de données personnelles à l'étranger sur la base d'un consentement non valable ou révoqué, dans la mesure où la communication s'est poursuivie sur la base de cette situation de consentement (art. 61 let. a en relation avec l'art. 17 al. 1 let. a LPD). En outre, notamment dans le domaine de la publicité de masse électronique, une sanction selon l'art. 23 LCD est possible en cas d'absence de consentement conformément à l'art. 3 al. 1 let. o LCD. 58

VI. CONSEILS PRATIQUES

59 Dans la pratique, un consentement est parfois demandé pour des traitements qui n'en nécessitent pas. Certains argumentent que le principe de transparence ou le principe de la bonne foi s'opposent à l'obtention de consentements non nécessaires. Une telle sévérité n'est généralement pas indiquée, car la question de la nécessité d'un consentement est souvent liée à une insécurité juridique. Toutefois, étant donné qu'un consentement peut être révoqué à tout moment, il convient d'examiner d'abord d'autres motifs de justification.

60 Sur Internet, on trouve souvent des formules telles que "J'accepte la déclaration de confidentialité", "J'accepte la déclaration de confidentialité" ou des formules similaires. Or, une déclaration de protection des données ne doit informer qu'unilatéralement et ne doit pas constituer un contrat bilatéral. En cas de reprise globale, la règle de l'inhabituel a en outre un effet restrictif. La déclaration de protection des données ne devrait donc être mise en lien et les consentements devraient être obtenus séparément et avec retenue.

VII. CRITIQUE DE LA NORME

61 Selon le message relatif à la nouvelle loi sur la protection des données, l'une des lignes directrices de la révision était de renforcer les droits des personnes concernées, ce à quoi devait également contribuer la définition plus précise des conditions d'un consentement valable de la personne concernée. Il est peu probable que cet objectif soit atteint par la précision des conditions du consentement. En effet, d'une part, la situation juridique n'a pas été modifiée. D'autre part, les déclarations de consentement, tout comme les déclarations de protection des données, sont rarement lues. Il peut en résulter une "surcharge d'informations" ainsi qu'une fatigue du clic, surtout si, en plus d'une déclaration de consentement relevant du droit de la protection des données, un consentement est demandé dans les conditions générales et que la déclaration de protection des données est portée à la connaissance des personnes concernées.

BIBLIOGRAPHIE

Aebi-Müller Regina E., Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Bern 2005.

Aebi-Müller Regina E. Grenzen des Bildnisschutzes – überwiegendes Interesse des Versicherers an der Observation eines Geschädigten und Rückzug einer Einwilligung zur Publikation erotischer Bilder im Internet, ZBJV 147 (2011), S. 330-354 (zit. ZBJV).

Baeriswyl Bruno, Kommentierung zu Art. 6, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Aufl., Bern 2023.

Bühlmann Lukas/Schüepp Michael, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, Jusletter 15.3.2021.

Dal Molin Luca, in: Dal Molin Luca/Wesiak-Schmidt Kirsten (Hrsg.), Datenschutz im Unternehmen, Zürich et al. 2023.

Domenig Benjamin/Mitscherlich Christian/Lutz Chantal, Datenschutzrecht für Schweizer Unternehmen, Stiftungen und Vereine, Bern 2022.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Datenbearbeitung durch den Arbeitgeber, 24.4.2023, abrufbar unter https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeit_wirtschaft/datenbearbeitung-arbeitgeber.html, besucht am 14.10.2023 (zit. Arbeitgeber).

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Schlussbericht und Empfehlungen vom 3.3.2023 mit Ergänzungen vom 17.5.2023 in Sachen Once Dating AG (zit. Schlussbericht Once Dating).

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Schlussbericht vom 11.4.2006 sowie Anhang vom 6.11.2006 in Sachen Erhebung biometrischer Daten beim Erwerb einer Dauerkarte in den Sport- und Freizeitanlagen KSS Schaffhausen (zit. Schlussbericht KSS Schaffhausen).

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Tracking, 12.4.2023, abrufbar unter https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/internet_technologie/tracking.html, besucht am 14.10.2023 (zit. Tracking).

European Data Protection Board (EDPB), Leitlinien 05/2020 zur Einwilligung gemäss Verordnung 2016/679, Version 1.1, angenommen am 4.5.2020, abrufbar unter https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf, besucht am 14.10.2023.

Fasnacht Tobias, Die Einwilligung im Datenschutzrecht, Zürich 2017.

Ferrari-Visca Reto/Reichlin Jeremy, in: Dal Molin Luca/Wesiak-Schmidt Kirsten (Hrsg.), Datenschutz im Unternehmen, Zürich et al. 2023.

George Damian, Prinzipien und Rechtmässigkeitsbedingungen im privaten Datenschutzrecht, Zürich 2021.

Glatthaar Matthias/Schröder Annika, Kommentierung zu Art. 19 DSG, in: Steiner Thomas/Morand Anne-Sophie/ Hürlimann Daniel (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz, 20.8.2023, abrufbar unter https://onlinekommentar.ch/de/kommentare/dsg19, besucht am 14.10.2023, DOI: https://doi.org/10.17176/20230820-133017-0.

Haas Raphaël, Die Einwilligung in eine Persönlichkeitsverletzung nach Art. 28 Abs. 2 ZGB, Zürich 2007.

Kasper Gabriel, People Analytics in privatrechtlichen Arbeitsverhältnissen, Zürich et al. 2021.

Klaus Samuel/Thomann Kenzo, Kommentierung zu Art. 6 Abs 6 und 7 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023.

Kurt Pärli, Kommentierung zu Art. 328b OR, in: Baeriswyl Bruno/Pärli Kurt/ Blonski Dominika (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Aufl., Bern 2023.

Kurt Pärli, BGer 4A_518/2020: Rechtswidrige Beschaffung von Arbeitnehmerpersonendaten, Jusletter 14.2.2022 (zit. Arbeitnehmerpersonendaten).

Kunz Christian, Kommentierung zu Art. 16 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023.

Maurer-Lambrou Urs/Steiner Andrea, Kommentierung zu Art. 4 aDSG, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.), Basler Kommentar zum Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014.

Meier Philippe/Tschumy Nicolas, Kommentierung zu Art. 6 DSG, in: Métille Sylvain/Meier Philippe (Hrsg.), Commentaire Romand, Loi sur la protection des données, Basel 2023.

Pellascio Michael, Kommentierung zu Art. 328b OR, in: Kren Kostkiewicz Jolanta/Wolf Stephan/Amstutz Marc/Fankhauser Roland, Orell Füssli Kommentar zum Schweizerischen Obligationenrecht, 3. Aufl., Zürich 2016.

Pfaffinger Monika, Kommentierung zu Art. 31 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Aufl., Bern 2023.

Pietruszak Thomas, Kommentierung zu Art. 328b OR, in: Honsell Heinrich (Hrsg.), Kurzkommentar Obligationenrecht, Basel 2014.

Portmann Wolfgang/Rudolph Roger, Kommentierung zu Art. 328b OR, in: Widmer Lüchinger Corinne/Oser David (Hrsg.), Basler Kommentar Obligationenrecht I, 7. Aufl., Basel 2020.

Rampini Corrado, Kommentierung zu Art. 13 DSG, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.), Basler Kommentar zum Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014.

Rehbinder Manfred/Stöckli Jean-Fritz, Kommentierung zu Art. 328b OR, in: Hausheer Heinz/Walter Hans Peter (Hrsg.), Berner Kommentar, Einleitung und Kommentar zu den Art. 319-330b OR, Zürich 2010.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16.11.2020 (zit. nDSG).

Rosenthal David, Der Entwurf für ein neues Datenschutzgesetz, Jusletter 27.11.2017 (zit. Entwurf).

Rosenthal David, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, Jusletter 20.2.2017 (zit. Vorentwurf).

Rosenthal David/Jöhri Yvonne, Kommentierung zu Art. 4 und 13 DSG, Art. 328b OR, Art. 45c FMG, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Schulz Sebastian, Kommentierung zu Art. 7 DSGVO, in: Gola Peter/Heckmann Dirk, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl., München 2022.

Spacek Dirk, Kommentierung zu Art. 7 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023.

Steiner Thomas, Zwischen Autonomie und Angleichung: Eine Analyse zur Anwendung des neuen DSG im Lichte der DSGVO, in: Widmer Michael (Hrsg.), Datenschutz: Rechtliche Schnittstellen, Zürich 2023, S. 51-138.

Steiner Thomas/Laux Christian, Kommentierung zu Art. 30 und 31 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023.

Streiff Ullin/von Kaenel Adrian/Rudolph Roger, Arbeitsvertrag, Praxiskommentar zu Art. 319-362 OR, 7. Aufl., Zürich 2012.

Uttinger Ursula/Geiser Thomas, Das neue Datenschutzrecht, Basel 2023.

Vasella David, Kommentierung zu Art. 3 Abs. 1 lit. o UWG, in: Heizmann Reto/Loacker Leander D., UWG Kommentar, Zürich et al. 2018.

Vasella David, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, Jusletter 16.11.2015 (zit. Einwilligung).

Vasella, EDÖB: Schlussbericht und Empfehlungen iS Once Dating, datenrecht.ch, 19.6.2023, abrufbar unter https://datenrecht.ch/edoeb-schlussbericht-und-empfehlungen-is-once-dating, besucht am 14.10.2023 (zit. Once Dating).

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.7.2017, BBl 2017 S. 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 14.10.2023 (zit. Botschaft 2017).

Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8.11.2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19.2.2003, BBl 2003 S. 2101 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2003/267/de, besucht am 14.10.2023 (zit. Botschaft 2003).

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988 II S. 413 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/de, besucht am 14.10.2023 (zit. Botschaft 1988).

Bundesgesetz über die Umsetzung der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (Weiterentwicklung des Schengen-Besitzstands), BBl 2017 S. 7193 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2058/de, besucht am 14.10.2023 (zit. Entwurf DSG).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 7 LPD

Un commentaire de Samuel Klaus

PROPOSITION DE CITATION

Samuel Klaus, Kommentierung zu Art. 7 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Klaus, N. XXX zu Art. 7 DSG.

Art. 7 Protection des données dès la conception et par défaut

[1] Le responsable du traitement est tenu de mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données, en particulier les principes fixés à l'art. 6. Il le fait dès la conception du traitement.

[2] Les mesures techniques et organisationnelles doivent être appropriées au regard notamment de l'état de la technique, du type de traitement et de son étendue, ainsi que du risque que le traitement des données présente pour la personnalité ou les droits fondamentaux des personnes concernées.

[3] Le responsable du traitement est tenu de garantir, par le biais de préréglages appropriés, que le traitement des données personnelles soit

limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement.

TABLE DES MATIÈRES

En bref ... 142
I. Généralités ... 142
A. Remarques préliminaires et contexte ... 142
B. Destinataire ... 143
II. Protection des données par la technique / Privacy by Design (al. 1-2) ... 144
A. Notion et contexte ... 144
B. Contenu et portée (al. 1) ... 146
C. Adéquation (al. 2) ... 146
D. Mise en œuvre dans la pratique ... 148
1. Normes internationales ... 149
2. Guides et orientations ... 150
3. Exemples de mesures possibles ... 153
III. Préférences en matière de protection des données / Privacy by Default (al. 3) ... 156
A. Notion ... 156
B. Contenu et portée ... 156
C. Mise en œuvre dans la pratique ... 157
IV. Conséquences en cas de violation des obligations ... 160
V. Dispositions transitoires ... 160
Bibliographie ... 161
Matériaux ... 163

EN BREF

Privacy by Design et Privacy by Default servent de principes directeurs pour la mise en œuvre de la protection des données. Selon le principe de Privacy by Design, des mesures appropriées doivent être prévues dès la planification d'un traitement de données afin de garantir une protection systémique des données. Si les personnes concernées ou les utilisateurs disposent de plusieurs possibilités de réglage/choix, le principe du privacy by default doit garantir que le réglage par défaut reflète la combinaison de possibilités de réglage la plus favorable à la protection des données.

I. GÉNÉRALITÉS

A. Remarques préliminaires et contexte

1 La prémisse selon laquelle les prescriptions du droit de la protection des données doivent être mises en œuvre au moyen de mesures techniques appropriées était déjà valable sous l'ancien droit, car les prescriptions de l'art. 4 aLPD (principes) et de l'art. 7 aLPD (sécurité des données) ne pouvaient pas être atteintes autrement. La loi révisée sur la protection des données l'exprime désormais explicitement à l'art. 7 LPD avec les deux principes "Privacy by Design" (protection des données par la technique, art. 7 al. 1-2 LPD) et "Privacy by Default" (paramètres par défaut favorables à la protection des données, art. 7 al. 3 LPD). Du point de vue du contenu, l'art. 7 LPD doit être lu en relation avec l'art. 6 LPD (principes) et l'art. 8 LPD (sécurité des données) : Les mesures techniques et organisationnelles mises en œuvre dans le cadre du Privacy by Design ("PbDesign") doivent notamment permettre la mise en œuvre des principes énoncés à l'art. 6 LPD, et la garantie de la sécurité des données (art. 8 LPD) constitue - parmi d'autres - l'un des points essentiels. L'art. 7 al. 3 LPD mentionne également un sous-aspect important de la conception de la protection des données, à savoir le principe de "Privacy by Default" ("PbDefault").

2 L'objectif normatif de l'article 7 LPD est fortement programmatique et donc difficile à saisir dans sa mise en œuvre concrète : L'intention qui sous-tend le PbDesign est de créer les conditions systémiques nécessaires à la réalisation et à la garantie (durable) de la protection des données. L'avenir nous dira si

cela est efficace compte tenu du cercle restreint de destinataires (voir ci-dessous, section B).

D'un point de vue juridique, l'introduction de PbDesign et PbDefault remonte à l'art. 10 al. 2-4 de la Conv. 108+, qui sera ratifiée lors de l'entrée en vigueur de la LPD révisée. Pour les organes fédéraux, PbDesign et PbDefault ont déjà été prescrits dans le champ d'application de la LPD depuis le 1er mars 2019 (art. 5 LPD). La LPD sera abrogée à l'entrée en vigueur de la LPD révisée, l'obligation de PbDesign et PbDefault sera alors réglée dans la LPD pour tous les destinataires. L'art. 7 LPD met en œuvre les prescriptions de l'art. 10 al. 2-4 de la CCE 108+ (cf. à ce sujet l'art. 4 al. 1 de la CCE 108+), de manière similaire mais non identique à ce qui est prévu à l'art. 25 RGPD pour les Etats membres de l'UE. 3

L'article 25 du RGPD (protection des données par la conception technique et par des paramètres par défaut favorables à la protection des données) met donc en œuvre les mêmes dispositions générales, en utilisant les mêmes termes et avec la même orientation - mais dans le contexte légèrement différent de la systématique du RGPD. Lors de l'application, de l'interprétation et de la mise en œuvre de l'article 7 LPD, la littérature et la jurisprudence relatives à l'article 25 RGPD peuvent donc être utiles, tout en tenant compte de certaines différences : Il convient notamment de tenir compte de la situation de départ différente en ce qui concerne les traitements de données (principe d'interdiction avec réserve d'autorisation dans le cadre du RGPD par rapport au traitement de données en principe autorisé avec restrictions et possibilité de justification dans le cadre de la LPD) lors de l'application par analogie des lignes directrices élaborées pour la mise en œuvre de l'article 25 du RGPD. Il faudra voir si, au fil du temps, la mise en œuvre des principes de PbDesign et de PbDefault dans le cadre de la LPD présente des différences significatives par rapport à celle du RGPD. D'un point de vue pragmatique, il faudrait éviter cela au profit d'une application aussi uniforme que possible de ces principes fondamentaux. 4

B. Destinataire

Les destinataires des prescriptions de l'article 7 LPD sont les responsables de traitement, les particuliers comme les organes fédéraux étant visés. En revanche, les personnes qui traitent les commandes, les prestataires de services en amont ou les fabricants ne sont pas concernés : les concepteurs, 5

les fabricants et les distributeurs de systèmes, d'applications et d'autres outils utilisés pour le traitement des données devraient en particulier être concernés par l'idée de base et le but de la norme PbDesign. Or, ces derniers ne sont pas concernés par le champ d'application de l'article 7 LPD ou ne le sont qu'indirectement par l'obligation des responsables.

6 Alors que les responsables sont donc directement tenus de mettre en œuvre les prescriptions de l'art. 7 LPD, l'idée fondamentale de la "protection systémique des données" n'est appliquée qu'indirectement vis-à-vis des acteurs situés en amont de la chaîne de création de valeur : En vertu de l'art. 7 LPD, les responsables sont tenus de veiller, par des mesures appropriées, à ce que les services et produits en amont soient conçus de manière à ce qu'ils (les responsables) puissent remplir leur obligation de PbDesign et PbDefault conformément à l'art. 7 LPD. Les responsables doivent en tenir compte, par exemple au moyen d'exigences contractuelles vis-à-vis des prestataires de services ou des fournisseurs, de la conception correspondante des directives d'achat, etc.

II. PROTECTION DES DONNÉES PAR LA TECHNIQUE / PRIVACY BY DESIGN (AL. 1-2)

A. Notion et contexte

7 Le concept de PbDesign repose sur l'idée que les moyens techniques ne devraient pas empêcher la mise en œuvre des dispositions relatives à la protection des données, mais plutôt la rendre possible et même la favoriser. Initialement discuté sous le terme de "Privacy Enhancing Technologies" (PET) spécifiques, le PbDesign a évolué au fil du temps vers un concept plus large. Il n'existe pas de définition générale obligatoire, le terme est plutôt utilisé en fonction du contexte.

8 Le contenu de la notion de PbDesign a été marqué de manière déterminante par Ann Cavoukian (commissaire à la protection de la vie privée de l'Ontario, Canada, de 1997 à 2014), avec un concept de PbDesign basé sur 7 principes (principes en italique, mises en évidence en gras selon l'implémentation de Cavoukian) :

1. *Proactive* not *Reactive*; **Preventative** not *Remedial*: PbDesign doit être compris comme un concept proactif et anticipatif, visant à prévenir les

violations de la protection des données (et non à remédier aux violations survenues).

2. *Privacy as the Default Setting*: même si la personne concernée n'entreprend aucune action particulière, la protection des données doit être garantie de la manière la plus complète possible, voir ci-dessous III - Privacy by Default / Préférences en matière de protection des données (al. 3).

3. *Privacy Embedded into Design*: la protection des données doit être intégralement prise en compte dès la conception et la mise en œuvre des systèmes et des processus.

4. *Full Functionality - Positive Sum, not Zero-Sum*: la protection des données ne doit pas empêcher ou conduire à des restrictions fonctionnelles, mais créer une valeur ajoutée par sa prise en compte intégrale.

5. *End-to-End Security - Full Lifecycle Protection*: la sécurité des données doit être garantie tout au long du cycle de vie des données concernées.

6. *Visibility and Transparency - Keep it Open*: la transparence et la vérifiabilité doivent être garanties.

7. *Respect for User Privacy - Keep it User-Centric*: les intérêts des personnes concernées (sujets des données) doivent être pris en compte.

Ces principes de base peuvent servir de lignes directrices et d'aides à la compréhension. En raison de leur orientation plutôt programmatique, ils ne sont guère utiles comme aides concrètes à la mise en œuvre. Dans le texte de loi, on peut au moins trouver des références au principe 1 - Proactive/ Preventative (à l'art. 7 al. 1 LPD avec l'approche préventive et la référence à la prise en compte dès la planification), au principe 2 - Default Setting (à l'art. 7 al. 3 LPD concernant les préréglages favorables à la protection des données), et au principe 3 - Embedded (à l'art. 7 al. 1 LPD avec l'obligation d'aménager le traitement des données en fonction des prescriptions de protection des données et la prise en compte dès la planification). Le principe 5 - Full Lifecycle Protection est ensuite abordé à l'art. 8 al. 2 LPD et le principe 1 - Proactive/Préventive à l'art. 8 al. 1 LPD. 9

Lors de la mise en œuvre pratique, les lignes directrices existantes de nature générale (telles que les lignes directrices 4/2019 de l'EDSA relatives à l'article 25 du DSGVO ou la norme ISO 31700 sur le respect de la vie privée dès la 10

conception) ainsi que les lignes directrices spécifiques à un secteur ou à une application peuvent être utiles (voir à ce sujet la section D ci-dessous - Mise en œuvre dans la pratique). Lors de leur mise en œuvre, il convient de tenir compte des éventuelles différences résultant du fait que de nombreuses lignes directrices de ce type sont axées sur le DSGVO.

B. Contenu et portée (al. 1)

11 PbDesign vise à exclure ou du moins à réduire, par des mesures techniques, le risque de violation des dispositions relatives à la protection des données, sans toutefois viser une technologie particulière. Il s'agit plutôt de mettre en œuvre des mesures techniques et organisationnelles appropriées ("TOM") lors de la conception des systèmes, applications et processus utilisés. Il ne faut pas seulement considérer un système, une application ou un aspect technique spécifique, mais, dans le sens d'une "approche holistique", l'ensemble du traitement des données, en mettant l'accent sur la mise en œuvre des principes énoncés à l'article 6 LPD.

12 D'un point de vue temporel, la PbDesign doit être prise en compte dès le moment de la planification du traitement des données (art. 7 al. 1, 2e phrase LPD). Si une analyse d'impact sur la protection des données ("AIPD") doit être effectuée conformément à l'art. 22 LPD, les TOM prévues pour la mise en œuvre de la PbDesign peuvent être intégrées dans le processus de l'AIPD et y figurer en tant que mesures au sens de l'art. 22 al. 3 LPD. L'obligation de PbDesign et l'obligation de procéder à une DSFA sont toutefois indépendantes l'une de l'autre, c'est-à-dire que l'obligation de PbDesign existe même s'il n'y a pas de "risque élevé" au sens du critère d'intervention de l'art. 22 al. 1 LPD pour procéder à une DSFA.

C. Adéquation (al. 2)

13 Les MTD à mettre en œuvre dans le cadre de la PbDesign doivent être "adéquates", ce qui traduit l'approche basée sur les risques de cette disposition. L'art. 7 al. 2 LPD mentionne "notamment" (a) l'état de la technique, (b) le type et l'ampleur du traitement des données, et (c) le risque pour la personnalité ou les droits fondamentaux des personnes concernées comme critères déterminants pour évaluer le caractère adéquat. Cette énumération n'est pas exhaustive, c'est la vision globale tenant compte des circonstances spécifiques qui est déterminante.

L'état de la technique désigne un niveau de développement technique avancé qui a fait ses preuves dans l'application pratique ou qui s'est imposé sur le marché. En fait également partie la possibilité de mise en œuvre économique d'un point de vue général et objectif (pas celui du responsable concerné). Comme l'état de la technique évolue constamment, en particulier dans le domaine numérique, la mise en œuvre de la PbDesign implique également l'obligation de vérifier régulièrement si les TOM mises en œuvre correspondent toujours à l'état actuel de la technique ou si elles doivent être adaptées si nécessaire : L'art. 7 al. 1 LPD stipule à cet égard que la PbDesign doit être prise en compte "dès" (et pas seulement "lors") de la planification. 14

Le type et l'étendue du traitement des données se réfèrent aux composantes du contenu et de la quantité du traitement : du point de vue du contenu, il est notamment déterminant de savoir quelles (catégories de) données sont traitées, de quelle manière et dans quel but. Du point de vue quantitatif, il faut prendre en considération tant le volume des sujets de données (c'est-à-dire le nombre de personnes concernées) que le volume des catégories de données traitées (c'est-à-dire le nombre d'enregistrements de données concernés). 15

Le risque pour les personnes concernées est le critère général pour évaluer l'adéquation de la MOT. Plus le risque est élevé, c'est-à-dire plus la probabilité d'occurrence et les conséquences potentielles sont importantes, plus les exigences posées aux mesures techniques sont élevées pour qu'elles puissent être considérées comme adéquates. Des outils clairement structurés et à orientation mathématique et probabiliste peuvent servir d'aide à l'évaluation des risques. Ils ne devraient toutefois servir que de point de départ, car l'évaluation des risques doit être effectuée d'un point de vue global, axé sur le contenu et en tenant compte de tous les aspects (pas seulement probabilistes). 16

Lors de l'évaluation de l'adéquation, il convient généralement d'appliquer un critère basé sur le risque et non sur l'absolu. Le risque lié à un traitement doit être mis en relation avec les possibilités techniques permettant de le réduire. Le principe de PbDesign vise à créer un équilibre approprié pour le conflit d'objectifs entre le traitement des données et la protection des données. Dans l'esprit du principe 4 - Positive Sum, not Zero-Sum - formulé par Cavoukian (cf. ci-dessus n. 8), il ne s'agit pas d'empêcher le traitement des données, mais de le rendre possible en tenant compte des exigences de la protection des 17

données, afin de créer une valeur ajoutée pour les responsables et les personnes concernées.

D. Mise en œuvre dans la pratique

18 Il n'existe pas de recette simple permettant de mettre en œuvre PbDesign de manière universelle. Le PbDesign doit être considéré comme un processus spécifique au projet. Par conséquent, il n'existe pas de procédure universelle qui puisse couvrir tous les cas d'application. Les TOM à mettre en œuvre doivent plutôt être adaptées (1) aux particularités des traitements de données concernés, (2) à l'environnement sectoriel dans lequel ils ont lieu et (3) aux systèmes et processus existants dans lesquels ils sont intégrés (ceux-ci devant également être adaptés si nécessaire). La réussite de la mise en œuvre de la PbDesign présuppose donc que les risques et les exigences spécifiques au projet ou au traitement soient identifiés et traités par des mesures concrètes adaptées à ces derniers. Les mesures de mise en œuvre de la sécurité des données (art. 8 LPD, art. 1 à 6 OLPD) ne couvrent qu'une partie (bien que très importante) du domaine (voir à ce sujet N. 30 ci-dessous).

19 Il est recommandé de procéder de manière clairement structurée à l'aide des orientations pertinentes pour le cas d'application, complétées par des clarifications et des directives propres plus approfondies en raison des particularités spécifiques au projet. Cette procédure devrait être suffisamment documentée pour permettre une vérification et une actualisation ultérieures (p. ex. en raison de modifications techniques, de l'évolution de l'état de la technique, d'adaptations du business case, etc.

20 Différents outils peuvent être utilisés à titre d'orientation, tels que les normes internationales, les meilleures pratiques des associations sectorielles, les guides des autorités de protection des données, etc. Lors de la mise en œuvre, il convient de noter que de telles orientations peuvent être utiles comme point de départ, mais qu'elles doivent dans tous les cas être complétées par les exigences du cas d'application spécifique et par l'état actuel de la technique. Il convient également de tenir compte du fait que nombre de ces orientations ont été formulées dans l'optique de l'article 25 du DSGVO. Lors de leur utilisation, il convient donc de tenir compte d'éventuelles différences dans le cadre de la LPD, notamment de la situation de départ différente en ce qui concerne les traitements de données (principe d'interdiction avec réserve d'autorisation dans le cadre du RGPD par rapport au traitement de données

en principe autorisé avec restrictions et possibilité de justification dans le cadre de la LPD).

1. Normes internationales

L'International Organization for Standardization (ISO) a publié en février 2023 la norme ISO 31700 sur le respect de la vie privée dès la conception. Celle-ci est divisée en deux parties : ISO 31700-1:2023 (https://www.iso.org/standard/84977.html) et ISO/TR 31700-2:2023 (https://www.iso.org/standard/84978.html). 21

La première partie (ISO 31700-1:2023 - Protection des consommateurs - Respect de la vie privée dès la conception pour les biens et services de consommation - Partie 1 : Exigences de haut niveau) contient, outre des conseils généraux et des définitions (sections 1 à 3), un aperçu des exigences et des procédures générales pour la conception d'un produit/service tout au long de son cycle de vie (comme par exemple la section 4-8). Section 4.4 - Designing human computer interface (HCI) for privacy, section 7.2 - Integrating the design and operation of privacy controls into the product development and management lifecycles, ou section 8.2 - Designing privacy controls for retirement and end of use). Étant donné que la norme ISO ne repose pas sur un fondement juridique précis en matière de protection des données, elle contient, outre ces exigences spécifiques à la conception, des prescriptions relatives à des aspects fortement marqués par le droit (local) applicable en matière de protection des données (comme par exemple la section 5.2 - Provision of privacy information, la section 5.4 - Responding to consumer inquiries and complaints, ou la section 6.2 - Conducting a privacy risk assessment). De telles directives doivent donc toujours être lues en relation avec les dispositions légales correspondantes, comme par exemple l'art. 19 ss. LPD concernant l'obligation d'information, art. 22 f. LPD concernant l'analyse d'impact relative à la protection des données, etc. Mais ils peuvent également servir de base à une procédure structurée à cet égard. 22

La deuxième partie (ISO/TR 31700-2:2023 - Consumer protection - Privacy by design for consumer goods and services - Part 2 : Use cases) contient trois cas d'application illustratifs qui montrent la mise en œuvre des prescriptions de la première partie : (1) On line retailing (boutique en ligne de commerce électronique) ; (2) Fitness company (centre de fitness avec des appareils reliés par des capteurs à une application de fitness des utilisateurs) ; et (3) Smart 23

locks (ligne de produits de serrures de porte électroniques IoT avec connexion en ligne et application de commande correspondante). Les cas d'utilisation couvrent de nombreux aspects pertinents pour la pratique. La mise en œuvre clairement structurée des directives de la première partie dans les cas d'utilisation peut donc non seulement servir à se familiariser avec la thématique, mais aussi directement de liste de contrôle lors de la mise en œuvre de certains aspects pertinents.

24 En conclusion, on peut dire que les normes ISO 31700-1/2 sont certes maintenues à un niveau d'abstraction élevé en raison de leur orientation générale. Néanmoins, grâce à leur structure claire, elles peuvent servir de bonne base. Les cas d'utilisation orientés vers la pratique peuvent également être utiles en tant que listes de contrôle pour des aspects comparables dans des cas d'utilisation différents.

2. Guides et orientations

25 Les guides généraux et les aides à l'orientation sont nombreux. La liste suivante peut servir d'aide initiale et de point de départ pour vos propres recherches. La ligne directrice 4/2910 de l'EDSA sur l'article 25 [RGPD] du Comité européen de la protection des données (EDSA) convient par exemple pour un aperçu conceptuel, tandis que les Privacy Patterns peuvent être utilisés pour une introduction plus pragmatique :

- **Ligne directrice 4/2019 de l'EDSA sur l'article 25 - Protection des données par la conception technique et par des paramètres par défaut respectueux de la vie privé**e (EDPB - European Data Protection Board / EDSA - Comité européen de la protection des données, version 2.0 du 20.10.2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_d consulté le 11.6.2023).
- **Privacy Patterns (privacybydesign.digital**) (Bayern Innovativ [Bayerische Gesellschaft für Innovation und Wissenstransfer mbH], Bayrisches Landesamt für Datenschutzaufsicht [BayLDA], 2023, https://privacybydesign.digital/, visité le 20.5.2023).
- **Data Processing by Design and Default** (ICO - Information Commissioner's Office [UK], https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-

accountability-and-governance/accountability-and-governance/data-processing-by-design-and-default/, consulté le 21.5.2023).

- **Protection des données par la conception technique et par des paramètres par défaut favorables à la protection des données (article 25 du RGPD**) (bvitg - Bundesverband Gesundheits-IT e.V. Arbeitsgruppe Datenschutz & IT-Sicherheit, GMDS - Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. Arbeitsgruppe Datenschutz und IT-Sicherheit im Gesundheitswesen, GDD - Gesellschaft für Datenschutz und Datensicherheit e.V. Arbeitskreis Datenschutz
und Datensicherheit im Gesundheits- und Sozialwesen, 2018, https://www.gesundheitsdatenschutz.org/html/privacy_design_default.php, consulté le 21.5.2023).
- **OIPC (Office of the Information and Privacy Commissioner) - Privacy by Design Resources** (IAPP - Association internationale des professionnels de la vie privée), https://iapp.org/resources/article/oipc-privacy-by-design-resources/, consulté le 21.5.2023).
- **Manage a privacy programme - Privacy by Design (PbD)** (Digital.govt.nz - Digital Government New Zealand, 2021, https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/manage-a-privacy-programme/privacy-by-design-pbd/, consulté le 21.5.2023).
- **Operationalizing Privacy by Design : A Guide to Implementing Strong Privacy Practices** (Ann Cavoukian, 2012, https://collections.ola.org/mon/26012/320221.pdf, consulté le 21.5.2023).
- **Privacy and Data Protection by Design - from policy to engineering** (ENISA - Agence de l'Union européenne pour les réseaux et la sécurité de l'information, 2014, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design, visité le 21.5.2023).

C'est précisément dans le domaine du développement de logiciels et d'applications que se posent diverses questions sur la mise en œuvre de PbDesign et PbDefault. Les guides des autorités de protection des données ainsi que les aides à l'orientation spécifiques au secteur, comme par ex : 26

- **Privacy by Design and Privacy by Default - A Guide for Developers** (Autorité catalane de protection des données, 2023, https://

apdcat.gencat.cat/web/.content/03-documentacio/documents/guiaDesenvolupadors/GUIA-PDDD_EN.pdf, consulté le 20.5.2023).

- **Guide pratique : Développement d'apps conformes à la protection des données** (Commissaire à la protection des données du canton de Zurich, 2022, https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_entwicklung_datenschutzkonformer_apps.pdf, consulté le 20.05.2023).
- **eHealth Suisse - Guide pour les développeurs d'apps, les fabricants et les responsables de la mise en circulation** (eHealth Suisse - centre de compétence et de coordination de la Confédération et des cantons, 2022, https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/D/Leitfaden_e-Health_Suisse_fuer_App_Entwickler.pdf, visité le 21.5.2023).
- **Apps mobiles dans le domaine de la santé : Exigences issues de la protection des données** (GMDS - Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V., DIG - Arbeitsgruppe Datenschutz und IT-Sicherheit im Gesundheitswesen, BvD - Berufsverband der Datenschutzbeauftragten Deutschlands e.V., 2022, https://gesundheitsdatenschutz.org/html/datenschutz_med_apps.php, visité le 21.5.2023).
- **American Medical Association (AMA) - Privacy is Good Business - A case for privacy by design in app developme**nt (2021), https://www.ama-assn.org/system/files/privacy-principles-by-design.pdf, visité le 11.6.2023).
- **An Engineer's Guide to Privacy by Design** (Rachel Dulberg, 2021, https://www.linkedin.com/pulse/engineers-guide-privacy-design-rachel-dulberg, consulté le 21.5.2023).
- **Privacy Design Guidelines for Mobile Application Developme**nt (GSMA - Système mondial pour les communications mobiles, 2018, https://www.gsma.com/publicpolicy/wp-content/uploads/2018/02/GSMA-Privacy-Design-Guidelines-for-Mobile-Application-Development.pdf, consulté le 21.5.2023).
- **Guidelines on Software development with Data Protection by Design and Default** (autorité norvégienne de protection des données Datatilsynet, 2017, https://www.datatilsynet.no/en/about-privacy/

virksomhetenes-plikter/data-protection-by-design-and-by-default/, consulté le 21.5.2023).

- **Privacy by Design in Big Data** (ENISA - Agence européenne pour la sécurité des réseaux et de l'information, 2015, https://www.enisa.europa.eu/publications/big-data-protection, consulté le 21.5.2023).

3. Exemples de mesures possibles

Les mesures concrètes doivent être déterminées à chaque fois en fonction du cas d'application spécifique et du profil de risque correspondant. La liste suivante peut servir d'exemple de mesures possibles et indiquer les premiers points de départ. Il peut également être utile de s'orienter sur des cas d'utilisation concrets, voir à ce sujet p. ex. Tamò-Larrieux, p. 203 ss, ainsi que les cas d'utilisation dans ISO/TR 31700-2:2023 (cf. N. 23). 27

Les mesures possibles peuvent être regroupées en aspects d'ordre systémique, plutôt techniques, et en aspects d'ordre organisationnel. Les aspects systémiques se réfèrent (comme les principes de traitement selon l'art. 6 al. 1-5 LPD) à l'ensemble du business case dans une perspective holistique. Les aspects techniques et organisationnels se situent à l'intersection avec les exigences en matière de sécurité des données (art. 8 LPD). Les aspects systémiques, techniques et organisationnels se recoupent dans de nombreux domaines et ne peuvent guère être délimités de manière nette. Toutefois, le fait que les aspects systémiques permettent de mettre certains thèmes supérieurs "entre parenthèses" par rapport à la mise en œuvre technique et organisationnelle peut faciliter une approche structurée, notamment en permettant d'intégrer très tôt les aspects généraux supérieurs dans toutes les réflexions et de les prendre en compte dans toutes les phases du projet. 28

D'un point de vue général et systémique supérieur, il convient par exemple d'examiner les aspects suivants : 29

- **Minimisation des données (LPD 6 al. 2)** : Les données personnelles saisies doivent être limitées, en termes de contenu (quelles (catégories de) données) et de volume (combien de données, p. ex. en termes de temps), à ce qui est nécessaire au traitement de la transaction concernée (business case) ; il ne doit pas y avoir de "collecte de données en réserve".

- **Ségrégation des données** : retenue dans la mise en relation ou le pooling de données, la centralisation de la gestion des données et l'agrégation de fichiers de données, etc.
- **Pseudonymisation** : la pseudonymisation peut créer une protection supplémentaire (dans le sens d'une ségrégation des informations d'identification par rapport à d'autres catégories de données), en particulier si la mise en relation de certaines données avec une personne déterminée n'est nécessaire que pour certaines étapes de traitement.
- **Déclaration des données** : identification des enregistrements (par ex. au moyen de métadonnées ou de descripteurs), par ex. concernant l'origine, le niveau de protection, la durée de conservation ("date d'expiration"), etc.
- **Anonymisation et/ou effacement (art. 6 al. 4 LPD)** : pour mettre en œuvre le principe de minimisation des données (p. ex. au moyen de "dates d'expiration" pour certains jeux de données, par des cycles réguliers d'anonymisation/d'effacement, etc.)

30 D'un point de vue technique, on peut se référer en premier lieu aux mesures techniques nécessaires à la mise en œuvre de la sécurité des données (voir à ce sujet l'article 8 LPD et les explications à ce sujet aux articles 1 à 6 OLPD). D'autres mesures techniques sont également envisageables, qui ne servent pas (uniquement) à la sécurité des données, mais aux objectifs généraux de protection des données en général. Les mesures techniques visant à mettre en œuvre les principes généraux de traitement (art. 6, al. 1 à 5, LPD) et le principe de minimisation des données (art. 6, al. 2, LPD) peuvent par exemple être particulièrement pertinentes. On peut penser par exemple à la mise en œuvre technique des concepts d'effacement (voir ci-dessus) ou à la pixellisation automatique des visages/caractéristiques d'identification pour les images/vidéos non personnelles, etc.

31 D'un point de vue organisationnel, les conditions internes doivent être créées pour mettre en œuvre les exigences systémiques et techniques. Cela peut comprendre, par exemple, les aspects suivants :

- **Culture d'entreprise et vision globale**: la culture d'entreprise doit considérer la protection des données comme faisant partie intégrante de l'activité de l'entreprise (et non comme une restriction imposée de l'extérieur, comme c'est encore souvent le cas). Il est donc nécessaire d'avoir une "mentalité favorable à la protection des données". En outre, la

protection des données doit être considérée dans son ensemble, c'est-à-dire non seulement de manière ponctuelle par rapport à ses propres traitements, mais aussi, par exemple, en tant que partie de la gestion des contrats / des fournisseurs.

- **Processus, responsabilités et documentation**: la mise en œuvre des procédures et des processus pertinents en matière de protection des données doit être définie et suffisamment documentée. Il est notamment important de définir clairement les responsabilités et de disposer d'une documentation suffisante. Même si la LPD ne prévoit pas de principe général de responsabilité ("accountability") et qu'il n'existe pas d'obligation légale d'établir un document spécifique (p. ex. un registre des traitements, cf. art. 12 en relation avec l'art. 24 OLPD), son établissement (au moins sous une forme éventuellement simplifiée) peut néanmoins être nécessaire ou du moins utile pour pouvoir mettre en œuvre les principes de PbDesign, les vérifier au fil du temps et les adapter si nécessaire.
- **Formation et sensibilisation**: pour que les MTD prévues soient effectivement appliquées, les collaborateurs doivent être formés en conséquence et sensibilisés aux thèmes de la protection des données, par exemple par des formations à la protection des données, des directives et des règlements internes, etc.
- **Mise en œuvre technique**: les mesures techniques (N. 30) doivent être complétées par des mesures organisationnelles appropriées afin de garantir leur mise en œuvre. Ainsi, pour une limitation effective de l'accès, il faut également un processus permettant d'octroyer les autorisations d'accès, de vérifier régulièrement leur actualité et de garantir leur suppression (p. ex. en cas de changement de poste ou de tâches des collaborateurs). De même, la prescription d'une limitation de la durée de conservation de certaines données nécessite un processus permettant de procéder régulièrement à un contrôle correspondant et à une éventuelle suppression.

III. PRÉFÉRENCES EN MATIÈRE DE PROTECTION DES DONNÉES / PRIVACY BY DEFAULT (AL. 3)

A. Notion

32 PbDefault est un contenu partiel de PbDesign (cf. ci-dessus N. 8 ch. 2) et a été formulé à l'art. 7 al. 3 LPD. Le libellé est à cet égard ambigu, car il n'existe aucune obligation de créer des possibilités de réglage spéciales (cf. à ce sujet n. 35 ci-dessous). L'obligation prévue à l'art. 7 al. 3 LPD se rapporte uniquement au fait que, lorsqu'il existe plusieurs possibilités de réglage, il convient de définir les paramètres par défaut de manière à mettre en œuvre le traitement de données le "moins invasif" possible du point de vue de la protection des données.

33 Le message décrit les préréglages comme "les réglages, en particulier de logiciels, qui sont appliqués par défaut, c'est-à-dire si l'utilisateur ne les modifie pas". Il faut donc entendre par là le réglage de base, le réglage par défaut ou la "configuration par défaut" qui s'applique lorsque les utilisateurs ne choisissent pas eux-mêmes activement un autre réglage.

B. Contenu et portée

34 Même si le message mentionne spécifiquement les logiciels comme cas d'application, le champ d'application ne se limite pas aux réglages des logiciels ou des systèmes, mais concerne tous les traitements de données. Toutes les possibilités de réglage qui existent lors du traitement des données et en particulier lors de la saisie des données sont donc couvertes de manière générale. Lorsqu'il existe différentes possibilités de réglage ou de choix, la combinaison de réglages la plus favorable à la protection des données doit être prévue comme réglage de base.

35 Les réglages par défaut favorables à la protection des données ne peuvent être effectués que si différentes possibilités de réglage sont prévues. Il convient d'examiner si de telles possibilités doivent être prévues sous l'angle de PbDesign (n. 7 ss). Les prescriptions relatives à PbDefault (art. 7 al. 3 LPD) ne prévoient en tout cas pas d'obligation spécifique de prévoir dans tous les cas certaines possibilités de réglage pour graduer l'intensité de l'atteinte à la protection des données.

Sur le plan du contenu, il faut se baser qualitativement sur le degré d'atteinte aux droits de la personnalité ou aux droits fondamentaux des personnes concernées et non pas uniquement (quantitativement) sur le nombre et le volume des données traitées. La référence dans le message au principe de la minimisation des données doit être comprise comme un renvoi à l'idée directrice de PbDefault et non comme une indication selon laquelle sa mise en œuvre devrait être abordée de manière purement quantitative et technique. 36

La finalité du traitement sert de critère (voir à ce sujet le libellé concernant la limitation "au minimum nécessaire pour l'utilisation prévue"). Le responsable reste libre de déterminer cette finalité, c'est-à-dire qu'il n'est pas obligé de proposer certaines prestations même sans collecte ou traitement de données. Si, par exemple, une prestation en ligne est financée par une publicité personnalisée, il n'existe aucune obligation de proposer une version sans publicité de cette prestation. Toutefois, lors de la mise en œuvre de la prestation en ligne et des traitements de données correspondants pour la publicité personnalisée, les principes de PbDesign et PbDefault doivent être respectés. 37

En partant de la configuration par défaut la plus respectueuse de la protection des données, les personnes concernées peuvent faire un autre choix et autoriser ainsi des traitements de données plus étendus. Il n'existe pas d'obligation de prévoir de telles possibilités de choix plus étendues. Toutefois, le responsable devrait généralement le prévoir dans son propre intérêt, afin de donner aux personnes concernées la possibilité de consentir à des traitements de données plus étendus qui ne seraient pas strictement nécessaires à la réalisation de la finalité étroitement limitée. 38

C. Mise en œuvre dans la pratique

Le point de départ est la finalité et le traitement de données "le moins invasif" nécessaire pour la mettre en œuvre ou l'atteindre. Le responsable doit décider, sur la base du cas d'affaires ou du cas d'utilisation et en appliquant les principes de PbDesign (n. 7 ss.), s'il existe différentes variantes de mise en œuvre ou différentes possibilités de réglage/de choix. Si c'est le cas, il convient de prévoir comme préréglage ou réglage de base la combinaison de réglages/choix la plus favorable à la protection des données, c'est-à-dire le 39

préréglage ayant le moins d'impact sur la personnalité ou les droits fondamentaux des personnes concernées.

40 Si les personnes concernées ont la possibilité de s'écarter de ces réglages les plus favorables à la protection des données et d'autoriser des traitements plus poussés, il convient d'examiner si un consentement au sens de l'art. 6 al. 6 LPD est nécessaire pour de tels traitements plus poussés et si les conditions prévues par cet article (et éventuellement aussi celles de l'art. 6 al. 7 LPD) doivent être respectées.

41 Alors que (sous l'angle du droit suisse, contrairement à la situation sous le RGPD), du point de vue du consentement, des champs de sélection pré-activés ("cases cochées") peuvent aussi, selon les circonstances, être considérés comme un consentement (explicite), cela semble douteux du point de vue de PbDefault : le sens et le but de PbDefault et sa formulation à l'art. 7 al. 3 LPD réside précisément dans le fait que les personnes concernées doivent pouvoir compter sur le fait que toutes les possibilités de réglage/choix dans le réglage de base mettent en œuvre la variante la plus favorable à la protection des données.

42 Ceci doit être pris en compte sous les mots-clés du principe de confiance et de la règle de l'inhabituel, par analogie avec les règles d'interprétation développées pour les reprises globales de CG. Le sens et le but de PbDefault selon l'art. 7 al. 3 LPD résident précisément dans le fait que l'on ne doit pas exiger des personnes concernées qu'elles étudient individuellement chaque possibilité de réglage, qu'elles vérifient si elle est favorable à la protection des données et qu'elles doivent ensuite l'activer ou la désactiver individuellement ou la sélectionner ou la désélectionner. Au contraire, ils doivent pouvoir compter sur le fait que la combinaison de réglages/choix qui leur est présentée lors de la première utilisation représente la combinaison de réglages la plus économe en données, la plus respectueuse de la protection des données et donc la plus "peu invasive".

43 Selon la formulation concrète des différentes possibilités de paramétrage, cela peut bien entendu avoir pour conséquence que certains champs de sélection doivent déjà être activés au préalable : Si une possibilité de sélection consiste par exemple en une option telle que "Je ne souhaite pas recevoir d'informations sur les produits", un tel champ de sélection devrait être activé par défaut selon le principe de PbDefault (même si la remise d'informations

sur les produits serait éventuellement autorisée en vertu de l'art. 3 al. 1 let. o LCD en raison d'une relation préexistante avec le client).

En fonction de la formulation concrète des différents paramètres/choix, il se peut donc que certaines options doivent être activées sous l'aspect de PbDefault, tandis que d'autres doivent être désactivées. L'essentiel est que la combinaison d'options activées/désactivées permette de mettre en œuvre, dans chaque cas, la combinaison de paramètres/choix la plus respectueuse de la protection des données. Les personnes concernées doivent pouvoir être sûres que si elles ne modifient pas ces paramètres, elles bénéficieront toujours du réglage le plus favorable à la protection des données. 44

Selon le point de vue défendu ici, cela doit également s'appliquer aux paramètres par défaut dans le cadre de la demande de consentement. Les prescriptions relatives à PbDefault ne se limitent pas à des paramètres purement techniques, mais visent, conformément à l'art. 7 al. 3 LPD, "le traitement des données personnelles" en général. Dans le cadre d'une approche globale, telle que la supposent les concepts de PbDesign et de PbDefault, il faut également tenir compte des éventuelles demandes de consentement. Il convient ici de se référer à la règle de l'inhabituel : si les utilisateurs confirment les CG dans le cadre d'une acceptation globale, ils sont alors protégés de conséquences inattendues par la règle de l'inhabituel. Il devrait en être de même lors de l'adaptation des possibilités de réglage et de la demande de consentement : Le principe de PbDefault crée chez les personnes concernées l'attente légitime de pouvoir bénéficier à tout moment du réglage le plus favorable à la protection des données sans devoir procéder à leurs propres adaptations. Ce principe ne devrait pas être contourné par l'autorisation de champs de sélection préactivés pour des traitements supplémentaires ne correspondant pas au réglage de base le plus favorable à la protection des données. Les personnes concernées devraient plutôt être protégées dans leur confiance en la mise en œuvre complète du principe de PbDefault. Les circonstances concrètes de chaque cas d'application sont déterminantes pour l'évaluation. 45

IV. CONSÉQUENCES EN CAS DE VIOLATION DES OBLIGATIONS

46 La violation des obligations de l'article 7 LPD n'a pas de conséquences directes en termes de sanctions (cf. article 60 et suivants LPD). De même, une telle violation de l'obligation de mettre en œuvre PbDesign et PbDefault ne constitue pas (encore) en soi une atteinte à la personnalité : L'art. 30 al. 2 let. a LPD ne renvoie explicitement qu'aux art. "6 et 8" (et non "6 à 8") : "Il y a atteinte à la personnalité notamment lorsque : (a) des données personnelles sont traitées en violation des principes énoncés aux articles 6 et 8".

47 En revanche, une violation des obligations de l'article 7 LPD peut avoir des conséquences indirectes en termes de sanctions si les systèmes, applications et processus à la base d'un traitement rendent impossible ou limitent le respect des prescriptions de protection des données en raison d'une planification et/ou d'une mise en œuvre inappropriées. Si, par exemple, les données personnelles enregistrées ne peuvent pas être consultées (et, si nécessaire, traitées, corrigées ou effacées) en fonction de la personne et que le responsable en a connaissance (ou doit en avoir connaissance), il n'y a qu'un pas à franchir pour fournir (éventuellement) intentionnellement un renseignement faux ou incomplet au sens de l'art. 60, al. 1, let. a LPD.

48 Une mise en œuvre insuffisante des principes de PbDesign et de PbDefault peut en outre avoir pour conséquence que les traitements de données effectués enfreignent de manière générale les prescriptions en matière de protection des données, notamment les principes de l'article 6 LPD. S'il existe suffisamment d'indices de telles violations, le PFPDT peut ouvrir une enquête d'office ou sur dénonciation (art. 49 al. 1 LPD) et émettre des injonctions correspondantes (art. 51 LPD), y compris l'injonction de mettre en œuvre les principes de PbDesign et PbDefault (art. 51 al. 3 let. b LPD). Si une décision du PFPDT n'est alors pas respectée, une sanction selon l'art. 63 LPD (non-respect des décisions) est encourue.

V. DISPOSITIONS TRANSITOIRES

49 En principe, la LPD est directement applicable à tous les traitements de données dès son entrée en vigueur, pour autant que les art. 69 ss. LPD ne prévoient pas de dispositions transitoires spéciales. Selon l'art. 69 LPD (dispositions transitoires concernant les traitements en cours), les

prescriptions de l'art. 7 LPD ne sont pas applicables aux traitements de données déjà existants qui se poursuivent sans changement : "Les art. 7, 22 et 23 ne sont pas applicables aux traitements de données commencés avant l'entrée en vigueur de la présente loi si le but du traitement reste inchangé et si aucune nouvelle donnée n'est collectée".

La disposition d'exception de l'article 69 LPD ne concerne donc que les 50
traitements de données dont les données sont purement statiques et dont la finalité de traitement reste la même, et uniquement les traitements de données déjà existants, et non les systèmes, applications, processus ou autres aspects du traitement de données en tant que tels utilisés à cet effet : Dès qu'un système, une application ou un processus existant est utilisé pour traiter de nouvelles données ou à de nouvelles fins, ce système, cette application ou ce processus (ou tout autre aspect du traitement des données) doit être évalué à l'aune des nouvelles exigences de PbDesign et PbDefault. Ainsi, les systèmes existants qui continuent à être exploités sans modification (comme par exemple une application d'archivage purement statique sans nouveaux flux de données) tombent sous le coup des dispositions transitoires, tandis que les systèmes, applications et processus opérationnels existants doivent être conçus conformément aux principes de PbDesign et PbDefault et être continuellement adaptés à l'état de la technique correspondant.

BIBLIOGRAPHIE

Baeriswyl Bruno, Kommentierung zu Art. 7 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023 (zit. SHK DSG-Baeriswyl, Art. 7).

Baeriswyl Bruno/Pärli Kurt, DSG und europäisches Datenschutzrecht, in (S. 1 ff): Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023 (zit. SHK DSG-Baeriswyl/Pärli).

Cavoukian Ann, Privacy by Design - The 7 Foundational Principles, Kanada 2011, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf, besucht am 25.4.2023 (zit. Cavoukian-Principles).

Cavoukian Ann, Privacy by Design - The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices, Kanada 2011, https://www.ipc.on.ca/wp-content/uploads/resources/pbd-

implement-7found-principles.pdf, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf, besucht am 25.4.2023 (zit. Cavoukian-Implementation).

Harasgama Rehana/Tamò Aurelia, Smart Metering und Privacy by Design im Big-Data-Zeitalter: Ein Blick in die Schweiz, in: ZIK - Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, Band/Nr. 59 (2014), Big Data und Datenschutz - Gegenseitige Herausforderungen, S. 117-149.

Kasper Gabriel, People Analytics in privatrechtlichen Arbeitsverhältnissen - Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, in: RnT - Schriften
zum Recht der neuen Technologien Band/Nr. 02, Zürich 2021, https://www.alexandria.unisg.ch/handle/20.500.14171/111087 (Hauptseite) sowie https://www.alexandria.unisg.ch/bitstreams/8a467009-dc08-4740-8d49-b8810c31fd35/download (PDF), besucht am 27.4.2023.

Langheinrich Marc, Mehr Datenschutz durch Technik? - Die Umsetzung der technikbezogenen Bestimmungen der EU-Datenschutzgrundverordnung (DSGVO) in der Praxis, digma 2017, S. 14 ff.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter vom 16.11.2020, https://www.rosenthal.ch/downloads/Rosenthal-revidiertesDSG.pdf, besucht am 1.7.2023.

Spacek Dirk, Kommentierung zu Art. 7 DSG, in: Bieri Adrian/Powell Julian, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Orell Füssli, Zürich 2023 (zit. OFK-Spacek zu Art. 7 DSG).

Reber Yannick, Die AGB-Kontrolle von Datenschutzerklärungen, ius.full - Forum für juristische Bildung 2/2023, S. 40-53.

Tamò-Larrieux Aurelia, Designing for Privacy and its Legal Framework - Data Protection by Design and Default for the Internet of Things, in: Law, Governance and Technology Series - Issues in Privacy and Data Protection, Vol. 40, Springer, Cham 2018.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.09.2017, BBl 2017 S. 6941 ff., https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 26.6.2023.

Revidierte Europaratskonvention zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 10.10.2018, BBl 2020 S. 599 ff., https://www.fedlex.admin.ch/eli/fga/2020/62/de, besucht am 2.7.2023 (zit. ER-Konv 108+), basierend auf ER-Konv 108 (SR 0.235.1).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 10 LPD

Un commentaire de Michèle Balthasar

PROPOSITION DE CITATION

Michèle Balthasar, Kommentierung zu Art. 10 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Balthasar, N. XXX zu Art. 10 DSG.

Art. 10 Conseiller à la protection des données

[1] Les responsables du traitement privés peuvent nommer un conseiller à la protection des données.

[2] Le conseiller à la protection des données est l'interlocuteur des personnes concernées et des autorités chargées de la protection des données en Suisse. Il a notamment les tâches suivantes:

a. former et conseiller le responsable du traitement privé dans le domaine de la protection des données;

b. concourir à l'application des prescriptions relatives à la protection des données.

[3] Les responsables du traitement privés peuvent se prévaloir de l'exception prévue à l'art. 23, al. 4, lorsque les conditions suivantes sont réunies:

a. le conseiller à la protection des données exerce sa fonction de manière indépendante par rapport au responsable du traitement et sans recevoir d'instruction de celui-ci;

b. il n'exerce pas de tâches incompatibles avec ses tâches de conseiller à la protection des données;

c. il dispose des connaissances professionnelles nécessaires;

d. le responsable du traitement publie les coordonnées du conseiller à la protection des données et les communique au PFPDT.

[4] Le Conseil fédéral règle la désignation de conseillers à la protection des données par les organes fédéraux.

TABLE DES MATIÈRES

En bref ... 169
I. Généralités ... 169
A. Introduction ... 169
B. Remarque de droit comparé ... 170
1. Obligation de désigner un délégué à la protection des données selon le DSGVO ... 170
2. Obligation de désigner un délégué à la protection des données en vertu de la réglementation spécifique à chaque pays. ... 171
C. Notion ... 172
II. Conseiller à la protection des données du responsable privé ... 172
A. Nomination du conseiller à la protection des données (art. 10 al. 1 LPD) ... 172
1. Caractère volontaire de la nomination d'un conseiller à la protection des données ... 172
2. Désignation d'un conseiller interne ou externe en matière de protection des données. ... 173
3. Désignation d'un conseiller à la protection des données commun pour un groupe d'entreprises ... 174
B. Tâches du conseiller à la protection des données (art. 10 al. 2) ... 174
1. être le point de contact pour le PFPDT et les autres autorités compétentes en matière de protection des données en Suisse, ainsi que pour les personnes concernées. ... 174
2. Formation et conseil du responsable privé en matière de protection des données (al. 2 let. a) ... 175
3. Participer à l'application des dispositions relatives à la protection des données (al. 2 let. b). ... 176
4. Digression : pas de responsabilité du conseiller à la protection des données .. 177
C. Exigences posées au conseiller à la protection des données (al. 3) ... 178
1. être professionnellement indépendant et ne pas être soumis à des instructions (let. a) ... 178
2. Pas d'incompatibilité avec d'autres tâches (let. b) ... 179
3. Connaissances spécialisées requises (let. c) ... 179
4. Publication des coordonnées (let. d) ... 180
D. Obligations du responsable privé (art. 23 RGPD) ... 180
1. Mise à disposition des ressources nécessaires (let. a) ... 181
2. l'octroi d'un accès à tous les renseignements, documents, registres des activités de traitement et données personnelles (let. b) ... 181
3. l'octroi du droit d'informer l'organe supérieur de direction ou d'administration dans les cas importants (let. c). ... 182

III. Conseiller à la protection des données auprès des organes fédéraux (art. 10 al. 4 LPD) 182
A. Nomination (art. 25 OLPD) 182
B. Exigences et tâches (art. 26 OLPD) 183
C. Obligations de l'organe fédéral (art. 27 OLPD) 184
D. Point de contact du PFPDT (art. 28 OLPD) 184
Bibliographie 185
Matériaux 185

EN BREF

L'art. 10 LPD règle la nomination et les tâches du conseiller à la protection des données ainsi que les conditions d'utilisation de la réglementation d'exception selon l'art. 23 al. 4 LPD. L'institution du conseiller à la protection des données permet aux entreprises privées de s'autoréguler. La nomination d'un conseiller à la protection des données est facultative pour le responsable privé, mais en cas de désignation, il peut bénéficier de la dérogation qui permet, sous certaines conditions, de renoncer à la consultation du PFPDT lors d'une analyse d'impact relative à la protection des données (AIPD).

I. GÉNÉRALITÉS

A. Introduction

L'art. 10 LPD règle la nomination et les tâches du conseiller à la protection des données ainsi que les conditions d'utilisation de la réglementation d'exception prévue à l'art. 23 al. 4 LPD. L'art. 23 OLPD concrétise les exigences posées à un responsable privé qui fait appel à un conseiller à la protection des données. L'institution du conseiller à la protection des données permet aux entreprises privées de s'autoréguler ou d'engager une personne chargée de piloter la protection des données dans l'entreprise. 1

Avec l'introduction de la nouvelle disposition relative au conseiller à la protection des données à l'art. 10 LPD, la consultation - obligatoire sous certaines conditions - du PFPDT dans le cadre d'une AIPD est désormais facilitée. Ainsi, un projet de traitement de données d'un responsable privé qui présente encore un "risque élevé" malgré la réalisation de la DSFA ne doit plus être soumis au PFPDT si le conseiller à la protection des données a déjà été consulté (art. 23 al. 4 LPD). Une entreprise qui a nommé un conseiller à la protection des données peut donc se baser uniquement sur le conseil interne en matière de protection des données, sans devoir consulter le PFPDT. 2

La nomination d'un conseiller à la protection des données est facultative pour le responsable privé. Sous l'ancien droit, la nomination d'un "responsable de la protection des données" (comparable dans sa conception) dispensait les entreprises de l'obligation de déclarer au PFPDT leurs fichiers, par ailleurs 3

soumis à l'obligation d'enregistrement. Avec la révision, l'obligation d'enregistrement disparaît de manière générale pour les particuliers.

4 Alors que la désignation d'un conseiller à la protection des données est facultative pour le responsable privé, elle est obligatoire pour les organes fédéraux (art. 10 al. 4 LPD en relation avec les art. 25 ss OLPD). Le Conseil fédéral règle à l'art. 25 OLPD la nomination, à l'art. 26 OLPD les exigences et les tâches du conseiller à la protection des données des organes fédéraux. L'art. 27 OLPD définit les obligations des organes fédéraux envers le conseiller à la protection des données et l'art. 28 OLPD définit le conseiller à la protection des données comme point de contact avec le PFPDT.

B. Remarque de droit comparé

1. Obligation de désigner un délégué à la protection des données selon le DSGVO

5 Avec l'entrée en vigueur du DSGVO, l'Union européenne a introduit dans certains cas l'obligation de nommer un soi-disant délégué à la protection des données. L'art. 37 al. 1 RGPD mentionne trois groupes de cas dans lesquels un délégué à la protection des données doit être désigné.

6 Tout d'abord, selon l'art. 37 al. 1 let. a du RGPD, cette obligation s'applique aux autorités et aux organismes publics, à l'exception des tribunaux, dans la mesure où ils agissent dans le cadre de leur activité judiciaire. Il s'agit par exemple des autorités de construction, des fournisseurs d'eau et d'énergie ou des entreprises de transport.

7 En outre, l'art. 37 al. 1 RGPD prescrit à la let. b une obligation de désignation lorsque l'activité principale du responsable du traitement ou du sous-traitant consiste à effectuer des opérations de traitement qui, en raison de leur nature, de leur portée et/ou de leurs finalités, exigent une surveillance régulière et systématique étendue des personnes. Le considérant 97 du RGPD explique que l'activité principale d'un responsable du traitement se rapporte à "ses activités principales et non au traitement de données à caractère personnel en tant qu'activité secondaire". Le groupe de travail "Article 29" de la Commission européenne a publié des lignes directrices sur ce sujet dans les WP 243 concernant les délégués à la protection des données ("DPD"). L'"activité principale" est donc le flux de travail principal nécessaire pour atteindre les

objectifs du responsable du traitement ou du sous-traitant. La surveillance est "régulière" si elle est continue ou périodique et "systématique" si elle suit une approche méthodique ou organisée ou si elle fait partie d'une stratégie plus large. On peut citer comme exemple les entreprises de sécurité privées qui surveillent les centres commerciaux privés et les lieux publics, ou les applications dont la fonctionnalité principale nécessite l'analyse de données de localisation (par exemple les applications sportives ou de navigation).

Enfin, l'article 37 al. 1 let. c du RGPD prévoit l'obligation de désigner un délégué à la protection des données dans les cas où l'activité principale du responsable du traitement ou du sous-traitant consiste en un traitement à grande échelle de catégories particulières de données à caractère personnel conformément à l'article 9 du RGPD ou de données à caractère personnel relatives à des condamnations pénales et à des infractions conformément à l'article 10 du RGPD. Le caractère étendu d'un traitement au sens de cette disposition doit être déterminé au cas par cas, en tenant compte par exemple de la quantité de données traitées ou du nombre de personnes concernées. On peut citer comme exemple le traitement de données de patients dans le cadre des activités habituelles d'un hôpital ou le traitement de données de clients dans le cadre des activités habituelles d'une compagnie d'assurance. 8

2. Obligation de désigner un délégué à la protection des données en vertu de la réglementation spécifique à chaque pays.

Les réglementations spécifiques aux Länder peuvent prévoir des dispositions plus étendues en vertu desquelles un délégué à la protection des données doit être désigné. Ainsi, la loi fédérale allemande sur la protection des données (BDSG) prévoit l'obligation de désigner un délégué à la protection des données si au moins 20 personnes sont employées en permanence pour le traitement automatisé de données à caractère personnel (article 38 al. 1, phrase 1 BDSG). Par ailleurs, la BDSG mentionne à l'article 38 al. 1, 2e phrase, deux autres scénarios dans lesquels les entreprises doivent désigner un délégué à la protection des données, quel que soit le nombre de personnes impliquées dans le traitement : D'une part, dans les cas où une DSFA est nécessaire en vertu de l'article 35 du DSGVO et, d'autre part, dans les constellations où elles traitent des données à caractère personnel à des fins commerciales pour les transmettre de manière anonyme ou à des fins d'études de marché ou d'opinion. 9

C. Notion

10 L'ancienne LPD utilisait en allemand le terme de "Datenschutzverantwortlicher" et en italien celui de "responsabile per la protezione dei dati", alors que la version française parle de "conseiller à la protection des données", c'est-à-dire de "Datenschutzberater" (art. 11a al. 5 let. e aDSG). Afin d'éviter toute confusion avec le "responsable" au sens de l'art. 5 let. i LPD ou avec le "responsabile", la révision de la LPD a introduit en allemand le terme de "Datenschutzberaterin und Datenschutzberater" ou en italien celui de "consulente per la protezione dei dati". La terminologie de l'article 10 LPD a ainsi été uniformisée dans les trois langues.

11 Parallèlement, il a été précisé que la responsabilité du traitement des données personnelles conforme à la protection des données n'incombe pas au conseiller à la protection des données, mais à l'entreprise responsable, le "responsable".

II. CONSEILLER À LA PROTECTION DES DONNÉES DU RESPONSABLE PRIVÉ

A. Nomination du conseiller à la protection des données (art. 10 al. 1 LPD)

1. Caractère volontaire de la nomination d'un conseiller à la protection des données

12 L'art. 10 al. 1 LPD stipule que la désignation d'un conseiller à la protection des données est facultative pour les responsables privés. Selon la LPD, le responsable privé est donc libre de désigner ou non un conseiller à la protection des données. Toutefois, une entreprise qui a désigné un conseiller à la protection des données conformément à l'art. 10 al. 3 LPD peut, après avoir effectué une AIPD, se fonder uniquement sur le conseil interne en matière de protection des données, même si le risque reste élevé, sans devoir en outre consulter le PFPDT (art. 23 al. 4 LPD).

13 Les entreprises actives au niveau international doivent toutefois respecter les dispositions du RGPD et sont donc souvent tenues de désigner un délégué à la protection des données conformément à l'art. 37 RGPD.

En outre, il est dans l'intérêt de chaque entreprise de garantir une protection des données efficace et effective au sein de son organisation, dans le sens d'une conformité appropriée. Il est donc souvent recommandé de désigner au moins un service de protection des données en interne et de lui confier des tâches relatives à la protection des données. Cette personne ne doit pas remplir les exigences de l'art. 10 al. 3 LPD. Toutefois, si elle ne remplit pas les exigences de l'art. 10 al. 3, l'entreprise ne peut pas non plus bénéficier des allégements de l'art. 24 al. 3 LPD. 14

En cas de désignation d'une telle personne ou d'un tel service, il convient d'éviter toute ambiguïté quant à l'intitulé de sa fonction, son statut, sa position et son champ d'action. La désignation de la fonction au sein de l'entreprise ainsi qu'à l'égard du PFPDT et des personnes concernées devrait donc déjà indiquer clairement qu'il ne s'agit pas d'un conseiller à la protection des données au sens de l'art. 10 al. 3 LPD. Il est recommandé de choisir une autre désignation pour cette fonction, par exemple service de protection des données, personne de contact pour la protection des données, coordinateur de la protection des données ou privacy officer. L'entreprise responsable est libre de répartir les tâches comme elle l'entend. Les tâches doivent néanmoins être clairement définies dans un cahier des charges. 15

2. Désignation d'un conseiller interne ou externe en matière de protection des données.

L'entreprise responsable peut désigner comme conseiller à la protection des données une personne interne ou une personne ou un service externe. 16

Le conseiller à la protection des données interne est un employé ou un service d'une entreprise qui s'occupe de manière ciblée de la protection des données dans l'entreprise concernée. Dans les grandes entreprises, il est régulièrement assisté, à un niveau hiérarchique inférieur, par ce que l'on appelle des gestionnaires de la protection des données ou des propriétaires de données (data owners), qui sont responsables de la protection des données dans leur domaine respectif, par exemple pour l'établissement et la tenue du registre des activités de traitement (art. 12 LPD). 17

Les conseillers à la protection des données externes sont en revanche des personnes physiques ou morales qui proposent la prestation de protection des données (Data Protection as a Service) et agissent sur la base d'un contrat de 18

mandat. Dans ce cas également, il convient de désigner en interne une personne de contact qui servira d'interlocuteur à l'entreprise et aux collaborateurs pour les questions de protection des données.

19 L'avantage d'un conseiller interne en matière de protection des données est son intégration dans l'entreprise elle-même, ce qui lui permet d'avoir une meilleure vue d'ensemble des processus internes. Il peut en outre vérifier directement et influencer le fait que la protection des données est "vécue" dans la culture de l'entreprise et n'existe pas seulement sur le papier. En revanche, le fait d'être trop proche de l'entreprise et des collaborateurs peut être un inconvénient, car cela peut entraîner des conflits d'intérêts. Souvent, les ressources et le savoir-faire correspondants font également défaut ou il existe des conflits d'intérêts pour garantir une protection adéquate des données dans l'entreprise. Dans de telles situations, il est judicieux de confier le mandat du conseiller à la protection des données à l'extérieur.

3. Désignation d'un conseiller à la protection des données commun pour un groupe d'entreprises

20 Pour un groupe d'entreprises, il est possible de désigner un conseiller à la protection des données commun. Celui-ci doit cependant être facilement accessible aux personnes concernées et au PFPDT en tant qu'interlocuteur interne à l'organisation par le biais de canaux de communication appropriés. Il doit être en mesure de communiquer efficacement avec les personnes concernées et de coopérer avec les autorités de contrôle compétentes. Il n'y a toutefois pas d'obligation d'être établi en Suisse tant que le conseiller à la protection des données peut exercer ses fonctions de manière efficace. Néanmoins, la connaissance d'une langue nationale devrait être nécessaire.

B. Tâches du conseiller à la protection des données (art. 10 al. 2)

1. être le point de contact pour le PFPDT et les autres autorités compétentes en matière de protection des données en Suisse, ainsi que pour les personnes concernées.

21 Le conseiller à la protection des données est un interlocuteur important en ce qui concerne les traitements de données effectués par l'entreprise responsable. Il/elle est intégré(e) dans les processus de l'entreprise visant à respecter la protection des données. Un interlocuteur spécialisé peut ainsi

être directement identifié, ce qui facilite l'exercice des droits du PFPDT ou des personnes concernées.

Il ou elle sert donc de point de contact pour le PFPDT et les autres autorités compétentes en matière de protection des données en Suisse (par exemple la FINMA ou les autorités cantonales de protection des données) en cas de questions liées au traitement de données personnelles dans l'entreprise. Il sert également de point de contact pour les personnes concernées, par exemple en cas de demande de renseignements selon les articles 25 et suivants de la LPD. LPD. 22

2. Formation et conseil du responsable privé en matière de protection des données (al. 2 let. a)

Afin de garantir une protection efficace des données dans l'entreprise concernée, le conseiller à la protection des données doit former, instruire et sensibiliser le responsable privé ou ses collaborateurs en conséquence. Il faut au moins impliquer tous les collaborateurs qui sont en contact avec des données personnelles. L'accent devrait être mis sur les principes de la protection des données (art. 6 LPD). D'autres thèmes de formation sont par exemple les directives relatives à la communication à l'étranger ainsi que le traitement des données personnelles sensibles au sein de l'entreprise. En outre, les collaborateurs doivent également être formés aux exigences en matière de sécurité des données (art. 8 LPD). 23

La formation des collaborateurs en matière de protection et de sécurité des données par le conseiller à la protection des données devrait être répétée à intervalles réguliers, de préférence chaque année. Grâce à une sensibilisation régulière, le thème de la protection des données reste présent dans l'esprit des collaborateurs. De plus, les nouveautés actuelles, par exemple en ce qui concerne l'environnement informatique de l'entreprise, peuvent être transmises en temps réel aux collaborateurs. 24

Dans sa fonction de conseiller, le conseiller à la protection des données a pour mission de conseiller sur le respect des dispositions légales en matière de protection des données lors des traitements de données, de mettre en évidence les faits pertinents de la question relevant de la protection des données et de présenter des alternatives de décision sur la base de ces faits. 25

3. Participer à l'application des dispositions relatives à la protection des données (al. 2 let. b).

26 Une autre tâche du conseiller à la protection des données est sa participation à l'application des dispositions relatives à la protection des données. Cela implique notamment de participer à l'adoption de conditions d'utilisation et de règles de protection des données. En outre, il ou elle doit vérifier le traitement des données personnelles et recommander des mesures correctives lorsqu'une violation des dispositions relatives à la protection des données est constatée. En outre, elle ou il doit aider les responsables privés à établir des DSFA et à vérifier leur exécution. En outre, il est important que le conseiller à la protection des données soit perçu comme un interlocuteur au sein de l'institution et qu'il fasse partie des groupes de travail concernés par les activités de traitement des données au sein de l'entreprise. Le conseiller à la protection des données du responsable privé n'a toutefois pas pour mission de signaler au PFPDT ou aux personnes concernées les violations de la sécurité des données. Bien qu'il soit souvent utile d'impliquer le conseiller à la protection des données en cas de violation de la sécurité des données, la loi ne le prescrit pas.

27 Le conseiller à la protection des données doit être considéré comme un organe de soutien et non comme un organe de surveillance. En ce qui concerne l'examen des traitements de données et la recommandation de mesures correctives, il ne s'agit donc pas d'introduire une obligation d'examen actif ou de prescrire des contrôles systématiques de tous les traitements de données. Il suffit plutôt qu'il soit actif si, par exemple, le responsable demande l'examen d'un traitement de données ou si des informations lui parviennent selon lesquelles les prescriptions en matière de protection des données ont été violées. Bien entendu, le responsable reste libre d'exiger que le conseiller à la protection des données vérifie de manière proactive les traitements de données. Il est envisageable et fréquent dans la pratique qu'il effectue une fois par an un audit de protection des données.

28 D'autres tâches du conseiller à la protection des données peuvent être envisagées :

- Elaboration et contrôle de la mise en œuvre de mesures de sécurité des données (art. 8 LPD) ;
- Vérification du traitement effectué par le sous-traitant (art. 9 LPD) ;

- Elaboration et vérification des registres des activités de traitement (art. 12 LPD) ;
- Examen de la communication de données à l'étranger (art. 16 ss. LPD) ;
- Soutien dans l'accomplissement des obligations d'information (art. 19 ss. LPD) ;
- Élaboration et mise en œuvre de processus pour le traitement des demandes des personnes concernées (art. 25 LPD) ;
- Élaboration de processus appropriés pour la défense des droits des personnes concernées et le respect des prescriptions en matière de protection des données (art. 25 ss. LPD) ;
- Réalisation d'évaluations des risques (par exemple, risque de transmission, de suppression ou de traitement involontaire/non autorisé des données, de perte de données ou d'erreur technique, etc.), par exemple dans le cadre d'une DSFA ;
- établissement de rapports annuels sur les activités à l'attention du responsable.

4. Digression : pas de responsabilité du conseiller à la protection des données

On suppose souvent que le conseiller à la protection des données est responsable de la protection des données et de son respect dans l'entreprise. Or, le conseiller à la protection des données n'a aucune compétence d'action découlant de la LPD elle-même, au-delà de sa fonction de formation, de conseil et de participation. Le seul pouvoir de décision - et donc la seule responsabilité pour un traitement des données personnelles conforme à la protection des données - revient à l'entreprise responsable. Le conseiller à la protection des données devrait être subordonné au niveau de management le plus élevé de l'entreprise concernée. La situation ne serait différente que si le conseiller à la protection des données agissait en tant qu'organe de fait et participait ainsi de manière déterminante à la formation de la volonté du responsable, en décidant des moyens et de la finalité des traitements. En raison de l'indépendance professionnelle et de l'absence d'instructions exigées par l'art. 10 al. 3 LPD, cela ne serait toutefois pas admissible. Si un conseiller à la protection des données décide néanmoins de la finalité et des

29

moyens d'un traitement de données, une responsabilité (obligatoire et/ou pénale) serait possible.

30 Si le conseiller à la protection des données émet des recommandations, l'entreprise devrait veiller à ce que ces recommandations soient mises en œuvre. Si elle ne le fait pas et que la recommandation était justifiée, l'entreprise peut subir un préjudice d'image non négligeable si un tel incident devait être rendu public. Le cas échéant, cela peut même conduire à des sanctions à l'encontre d'un collaborateur. Si la recommandation était fausse ou erronée, le conseiller à la protection des données est responsable dans le cadre de son contrat de travail ou de son mandat.

C. Exigences posées au conseiller à la protection des données (al. 3)

31 Pour qu'une entreprise soit dispensée de consulter le PFPDT lorsqu'un risque élevé subsiste malgré la réalisation de la DSFA (art. 23 al. 4 LPD), le conseiller à la protection des données doit remplir les conditions de l'art. 10 al. 3 LPD.

1. être professionnellement indépendant et ne pas être soumis à des instructions (let. a)

32 Le conseiller à la protection des données doit être suffisamment indépendant dans l'exercice de son activité pour que ses tâches ne soient pas soumises à des instructions et qu'il ne puisse pas être sanctionné par l'entreprise en raison de son activité. Cela signifie qu'il ne doit pas recevoir d'instructions sur la manière de procéder dans une situation donnée, par exemple sur le résultat à obtenir, sur la manière de traiter une plainte ou sur l'opportunité de consulter le PFPDT. En outre, il ne doit pas être chargé de défendre un point de vue particulier sur une question relevant de la protection des données (par exemple en ce qui concerne l'interprétation d'une loi).

33 En outre, il faut garantir que le conseiller à la protection des données puisse formuler librement ses recommandations - même si elles peuvent parfois être désagréables - sans craindre de subir des préjudices. Cette indépendance implique également que le conseiller à la protection des données puisse s'adresser à la direction supérieure (par exemple le conseil d'administration d'une société anonyme) pour les questions importantes (art. 23 let. c OLPD).

En principe, il devrait donc également être directement subordonné à la direction, voire au conseil d'administration du responsable du traitement.

2. Pas d'incompatibilité avec d'autres tâches (let. b)

Pour que le conseiller à la protection des données puisse exercer ses fonctions au sein de l'entreprise, il ne doit pas exercer d'autres activités incompatibles avec ses tâches. Le conseil en matière de protection des données doit être exercé séparément des tâches de l'entreprise. Il convient d'éviter tout conflit d'intérêts. Il pourrait en exister un, par exemple, si le conseiller à la protection des données est membre de la direction, chef de la division opérationnelle ou chef du département informatique, ou s'il exerce des fonctions de gestion des ressources humaines ou des systèmes d'information (par exemple, responsable informatique). Le conseiller à la protection des données ne peut pas occuper simultanément une fonction dans laquelle il décide lui-même des moyens et des finalités des traitements de données effectués par le responsable du traitement ou a un intérêt dans ces traitements. Il est également recommandé de ne pas mélanger le conseil en matière de protection des données avec les autres activités de conseil et de représentation juridiques. 34

Un éventuel conflit d'intérêts doit donc être évité dès le départ grâce à la position organisationnelle du conseiller à la protection des données. En principe, il convient de veiller à ce qu'aucune responsabilité hiérarchique ne soit liée au poste de conseiller à la protection des données. Il est donc recommandé à une entreprise d'attribuer la fonction de conseiller à la protection des données à un poste d'état-major par exemple. Il est important qu'il ne s'agisse pas d'une fonction exécutive dans un secteur d'activité. Une autre possibilité serait de regrouper la tâche du conseiller à la protection des données avec celle du responsable de la sécurité de l'information. 35

Les conflits d'intérêts étant difficilement évitables dans la pratique, le conseiller à la protection des données devrait en règle générale être un prestataire de services externe, sauf dans les grandes entreprises disposant de leur propre service de protection des données. 36

3. Connaissances spécialisées requises (let. c)

Pour pouvoir assumer ses tâches en toute indépendance, le conseiller à la protection des données doit disposer des compétences professionnelles 37

nécessaires. Il ou elle doit avoir des connaissances suffisantes dans tous les domaines pour pouvoir évaluer les recommandations et les mesures proposées et les apprécier dans le cadre de la stratégie de protection des données de l'entreprise.

38 Les exigences ne portent pas seulement sur les connaissances dans le domaine de la protection et de la sécurité des données, mais aussi sur les connaissances techniques spécifiques à l'entreprise. S'il est possible qu'il ait des connaissances moins développées dans certains domaines, il doit au moins avoir la possibilité d'accéder à de telles connaissances. Des connaissances interdisciplinaires, en particulier dans les domaines de l'informatique et du droit, sont nécessaires. Les systèmes de gestion doivent être compris.

4. Publication des coordonnées (let. d)

39 Il incombe au responsable de publier les coordonnées du conseiller à la protection des données et de les communiquer au PFPDT. Le PFPDT a créé un portail de communication à cet effet. Comme pour le responsable privé, il n'est pas nécessaire que l'entreprise publie le nom du conseiller à la protection des données. Il suffit par exemple d'indiquer l'adresse électronique de l'organe compétent sur le plan technique. Le service compétent peut également être une équipe entière ou une entreprise. Le conseiller à la protection des données est une personne de contact importante en ce qui concerne les traitements de données effectués par l'entreprise en question. La publication des données de contact garantit que les personnes concernées ou le PFPDT peuvent s'adresser directement au conseiller à la protection des données.

40 Il n'est pas nécessaire que l'entreprise publie le nom du conseiller à la protection des données. Il suffit d'indiquer, par exemple, l'adresse électronique du service compétent sur le plan technique.

D. Obligations du responsable privé (art. 23 RGPD)

41 Pour qu'une entreprise soit dispensée de consulter le PFPDT si un risque élevé subsiste malgré la réalisation de la DSFA (art. 23 al. 4 LPD), le responsable privé doit également remplir certaines obligations. Le contenu de ces obligations correspond aux anciennes dispositions de la législation sur la

protection des données ; seule la terminologie a été adaptée à la nouvelle LPD.

1. Mise à disposition des ressources nécessaires (let. a)

Conformément à l'art. 23 let. a OLPD, le responsable privé doit mettre à la disposition du conseiller à la protection des données les ressources nécessaires - le plus souvent sous forme de temps de travail - pour qu'il puisse accomplir ses tâches. Les exigences varient certes en fonction de la taille de l'entreprise, mais il ou elle doit toujours disposer de ressources suffisantes pour pouvoir assumer sa fonction de manière adéquate. Cela signifie que plus les opérations de traitement des données sont complexes et/ou sensibles, plus les ressources mises à la disposition du conseiller à la protection des données doivent être importantes. 42

2. l'octroi d'un accès à tous les renseignements, documents, registres des activités de traitement et données personnelles (let. b)

Pour pouvoir exercer sa fonction, le conseiller à la protection des données doit avoir accès, sur demande, à tous les renseignements, documents, listes d'activités de traitement et données personnelles dont il a besoin pour accomplir ses tâches. Outre l'accès, cela implique également qu'il ou elle ait connaissance de tous les traitements de données effectués au sein de l'entreprise. Pour ce faire, il est nécessaire de disposer d'un droit de regard étendu sur les documents, d'un droit de présentation des systèmes de traitement des données et d'un droit d'accès à toutes les personnes responsables des traitements de données. Il serait recommandé d'introduire une obligation de notification au sein de l'entreprise, ce qui signifie que tous les traitements de données doivent être notifiés au conseiller à la protection des données. 43

L'accès aux informations est toutefois limité dans la mesure où il ne s'applique qu'aux documents dont le conseiller à la protection des données a effectivement besoin pour accomplir ses tâches. Si le conseiller à la protection des données examine par exemple de manière générale les prescriptions internes en matière de protection des données ou les processus de traitement des données, il n'aura en général pas besoin de consulter les données personnelles. 44

3. l'octroi du droit d'informer l'organe supérieur de direction ou d'administration dans les cas importants (let. c).

45 L'art. 23 let. c OLPD a introduit la possibilité pour les conseillers à la protection des données d'informer, dans les cas importants, l'organe supérieur de direction ou d'administration, c'est-à-dire l'organe qui assume également la responsabilité du respect des prescriptions de protection des données dans l'entreprise. En effet, le conseiller à la protection des données n'a pas de pouvoir de décision propre, mais dépend du niveau de gestion le plus élevé de l'entreprise concernée.

46 La disposition établit un droit d'escalade pour le conseiller à la protection des données. Cela permet au conseiller à la protection des données de ne pas devoir se fier uniquement aux documents dont il dispose lors des contrôles internes de l'entreprise concernant le respect des dispositions légales en matière de protection des données, mais de pouvoir imposer l'obtention d'informations et de documents supplémentaires. En outre, cela garantit que le conseiller à la protection des données puisse, en cas de situations complexes et de violations particulièrement graves, faire rapport aux organes supérieurs du responsable ou du sous-traitant et obtenir une décision. Dans la pratique, l'information de l'organe supérieur de direction ou d'administration devrait également se faire par l'établissement de rapports trimestriels et annuels sur les activités du conseiller à la protection des données.

III. CONSEILLER À LA PROTECTION DES DONNÉES AUPRÈS DES ORGANES FÉDÉRAUX (ART. 10 AL. 4 LPD)

A. Nomination (art. 25 OLPD)

47 Dans le domaine Schengen, les organes fédéraux sont tenus, en vertu de l'article 32 de la directive (UE) 2016/680, de désigner un conseiller à la protection des données. Les règles relatives à la désignation du conseiller à la protection des données par les organes fédéraux ne se trouvent toutefois pas dans la LPD, mais ont été laissées au Conseil fédéral (art. 10 al. 4 LPD).

48 Selon l'art. 25 OLPD, plusieurs organes fédéraux peuvent désigner ensemble un conseiller à la protection des données. Cette réglementation doit avant tout permettre aux petits organes fédéraux ou aux départements disposant d'une structure organisationnelle centralisée d'exploiter des synergies utiles et

permettant d'économiser des ressources. On peut en revanche attendre des offices fédéraux plus importants qu'ils désignent un conseiller à la protection des données pour eux seuls. Les organes fédéraux sont également libres de désigner plusieurs conseillers à la protection des données.

B. Exigences et tâches (art. 26 OLPD)

L'art. 26 al. 1 OLPD contient les exigences auxquelles doit satisfaire le conseiller à la protection des données : il doit disposer des connaissances spécialisées nécessaires et exercer sa fonction à l'égard de l'organe fédéral de manière professionnellement indépendante et en étant lié par des instructions. Cette réglementation est analogue à celle prévue à l'art. 10 al. 3 LPD pour les responsables privés, raison pour laquelle il peut y être fait référence. 49

Le rôle du conseiller à la protection des données auprès des organes fédéraux, qui sont habituellement hiérarchisés, a été renforcé et institutionnalisé par la révision afin qu'il puisse exercer efficacement ses fonctions. L'indépendance s'exprime par le fait que le conseiller à la protection des données peut, dans des cas importants - comme le prévoit l'art. 23 let. c OLPD pour les particuliers - s'adresser à la direction suprême de l'organe fédéral. L'indépendance du conseiller à la protection des données doit être garantie en premier lieu par des mesures organisationnelles : il s'agit avant tout d'éviter que l'activité de conseiller à la protection des données n'ait des répercussions négatives sur l'entretien d'évaluation. 50

L'art. 26 al. 2 OLPD contient les tâches du conseiller à la protection des données d'un organe fédéral. Elles ont été harmonisées, sur le plan terminologique, avec la disposition applicable aux responsables privés (art. 10, al. 2, LPD), raison pour laquelle on peut également renvoyer aux explications qui y sont données. Il participe à l'application des prescriptions en matière de protection des données, notamment en examinant le traitement des données personnelles et en recommandant des mesures correctives (let. a). Si une violation des prescriptions de protection des données est constatée, il ou elle conseille le responsable et vérifie leur exécution (let. b). En outre, elle ou il forme et conseille les collaborateurs de l'organe fédéral sur les questions de protection des données (let. c). Enfin, elle ou il sert de point de contact pour les personnes concernées (let. d). 51

C. Obligations de l'organe fédéral (art. 27 OLPD)

52 L'organe fédéral donne au conseiller à la protection des données accès à tous les renseignements, documents, registres des activités de traitement et données personnelles dont il a besoin pour accomplir ses tâches (art. 27 al. 1 let. a OLPD) et veille à ce qu'il soit informé d'une violation de la sécurité des données (art. 27 al. 1 let. b OLPD).

53 L'art. 27 al. 1 let. a OLPD est donc identique à la réglementation concernant les responsables privés à l'art. 23 let. b OLPD. On peut se référer par analogie aux explications qui y sont données. Cette obligation s'applique par ailleurs à toutes les violations de la sécurité des données, et pas seulement à celles qui doivent être notifiées au PFPDT conformément à l'art. 24 LPD. L'information sur la violation de la sécurité des données selon l'art. 27 al. 1 let. b OLPD peut par exemple être assurée par le fait que l'organe fédéral oblige les collaborateurs, par le biais de directives, à informer le conseiller à la protection des données en cas de violation de la sécurité des données. Le conseiller à la protection des données conseille le responsable sur la question de savoir si la violation est soumise à une obligation de notification au sens de l'article 24 LPD. L'organe fédéral veille à ce qu'il ou elle soit informé(e) d'une violation de la sécurité des données. La notification elle-même incombe toutefois à l'organe fédéral. C'est lui qui décide si et quelles violations doivent être notifiées au PFPDT.

54 Enfin, l'organe fédéral publie sur Internet les coordonnées du conseiller à la protection des données et les communique au PFPDT (art. 27, al. 2, OLPD). Comme pour le responsable privé, il n'est pas nécessaire que l'entreprise publie le nom du conseiller à la protection des données. Il suffit par exemple d'indiquer l'adresse électronique du service compétent sur le plan technique. Le service compétent peut également être une équipe entière ou une entreprise.

D. Point de contact du PFPDT (art. 28 OLPD)

55 Le conseiller à la protection des données sert de point de contact au PFPDT pour les questions liées au traitement de données personnelles par l'organe fédéral concerné. Il est donc, puisqu'il dispose des connaissances techniques et internes nécessaires, l'interlocuteur technique direct du PFPDT.

BIBLIOGRAPHIE

Frey Marco, Kommentierung zu Art. 11a DSG (altes DSG), in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023 (zit. SHK DSG-Bearbeiter:in).

Rosenthal David, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020 (zit. Rosenthal, Jusletter 2020).

Rosenthal, David/Jöhri, Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. HK-Rosenthal/Jöhri).

Ehrensberger Jennifer/Bersler Urs, Kommentierung zu Art. 11a DSG (altes DSG), In: von Maurer-Lambrou, Urs/Blechta, Gabor-Paul (HrsG.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014 (zit. BK-Bearbeiter:in).

MATÉRIAUX

Leitlinien in Bezug auf Datenschutzbeauftragte («DSB») der Datenschutzgruppe nach Art. 29 der Richtlinie 95/46/EG, angenommen am 13. Dezember 2016, zuletzt überarbeitet und angenommen am 5.4.2017.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 11 LPD

Un commentaire de Ursula Sury / Jael Inauen

PROPOSITION DE CITATION

Ursula Sury/Jael Inauen, Kommentierung zu Art. 11 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Sury/Inauen, N. XXX zu Art. 11 DSG.

Art. 11 Codes de conduite

[1] Les associations professionnelles, sectorielles et économiques, lorsqu'elles sont autorisées de par leurs statuts à défendre les intérêts économiques de leurs membres, de même que les organes fédéraux, peuvent soumettre leur code de conduite au PFPDT.

[2] Le PFPDT prend position sur les codes de conduite et publie ses prises de position.

TABLE DES MATIÈRES

En bref 189
I. Généralités 190
A. Historique 190
1. Codes de conduite dans l'entreprise 190
2. Les meilleures pratiques 190
B. Objectif de la norme 191
1. Promotion de la conformité à la protection des données 191
2. L'autorégulation réglementée 192
II. Contenu 193
A. Code de conduite 193
1. Un code de conduite en général 193
2. Codes de conduite en matière de protection des données 194
3. Concrétisation et autorégulation 195
B. Délimitation par rapport à la certification 196
III. Avis du PFPDT 197
A. Portée juridique d'une saisine 197
B. Conséquences de l'avis 198
IV. Autorégulation selon l'article 40 du RGPD 200
Bibliographie 201
Matériaux 202

EN BREF

Les codes de conduite sont des règles de comportement, établies par des associations professionnelles, sectorielles ou économiques. Ils se sont établis dans l'économie en tant que code de conduite dans le cadre de la "bonne gouvernance d'entreprise" et doivent maintenant être étendus à la protection des données. Les directives et dispositions relatives à la protection des données sont concrétisées par des codes de conduite spécifiques à chaque secteur. Les organes fédéraux et les associations privées sont libres d'élaborer leur propre code de conduite.

Les codes de conduite peuvent être soumis au PFPDT. Le PFPDT examine la compatibilité des codes avec la LPD. La présentation n'est obligatoire que si le code doit être utilisé pour justifier une exportation de données conformément à l'art. 12 OLPD. Elle est toutefois recommandée en principe pour des raisons de diligence et de responsabilité.

L'article 11 peut être comparé à l'article 40 du RGPD, où les exigences et les conséquences juridiques des codes de conduite ou des "règles de conduite" (article 40 du RGPD) sont similaires. Les codes établis conformément à l'article 40 du RGPD constituent donc un bon point de repère pour une éventuelle mise en œuvre en Suisse. Si une approbation du code est souhaitée pour l'Union européenne, ses exigences sont déterminantes.

Par ailleurs, l'établissement de codes de conduite favorise l'internationalisation des entreprises et l'uniformisation de la protection des données au sein de certaines branches. Les codes de conduite ont été introduits depuis longtemps au niveau économique international et soutiennent une gestion d'entreprise transnationale, uniforme et efficace. Un code de conduite peut donc permettre à une entreprise de répondre à des exigences internationales, juridiques et sectorielles.

I. GÉNÉRALITÉS

A. Historique

1. Codes de conduite dans l'entreprise

1 L'un des objectifs déterminants de la révision totale de la LPD était de développer et d'encourager certains aspects de l'autorégulation. Alors que l'art. 11 aLPD ne prévoyait qu'une procédure de certification (n. 22 s.), la nLPD la complète par l'instrument des codes de conduite. Ceux-ci doivent permettre aux associations de concrétiser la législation sur la protection des données de manière autonome, en fonction de leurs besoins. Le code de conduite introduit une notion d'économie et d'entreprise ("code of conduct") dans le droit de la protection des données. En tant que partie intégrante de la culture de conformité et de la "gouvernance d'entreprise", les codes de conduite sont déjà répandus depuis longtemps dans les entreprises. Désormais, ils sont prévus et définis par la loi pour soutenir, concrétiser et guider les systèmes de gestion de la protection des données.

2. Les meilleures pratiques

2 Pour la mise en œuvre de la protection des données, la FF 2017 mentionne ce que l'on appelle les "meilleures pratiques" pour la mise en œuvre de la protection des données au sein de l'entreprise. Les "meilleures pratiques" sont courantes depuis longtemps dans le domaine de la gouvernance d'entreprise et décrivent divers modèles ou méthodes permettant d'optimiser systématiquement les procédures, processus ou pratiques au sein même de l'entreprise. Un processus est standardisé afin de parvenir à un déroulement optimal des affaires. La notion de "bonne pratique" est en outre expressément mentionnée à l'art. 58, al. 1, let. g LPD, selon lequel le PFPDT doit lui-même élaborer des instruments de travail pour la respecter.

3 Les bonnes pratiques sont également représentées au niveau international ; l'art. 4, al. 3, de l'ordonnance sur les certifications en matière de protection des données (OCPD) renvoie aux normes internationales existantes, qui servent de référence pour les systèmes de gestion de la protection des données qui fonctionnent. Indirectement, il est également fait référence aux bonnes pratiques et aux codes de conduite. La Nouvelle-Zélande et l'Argentine qualifient en outre les codes de conduite de bonnes pratiques.

En Suisse également, la question de savoir si le PFPDT devait lui-même édicter des "bonnes pratiques" en matière de protection des données a été discutée lors de la procédure de consultation, étant donné que le PFPDT a pour mission de conseiller les organes fédéraux et les particuliers et, dans ce cadre, de mettre à leur disposition des guides et des instruments de travail. Ces directives au sens de "best practices" auraient donc également influencé des codes de conduite. L'art. 58, al. 1, let. g LPD peut également être compris comme une compétence pour élaborer des guides similaires à des codes de conduite. 4

Lors de la consultation, les milieux économiques ont notamment critiqué le fait que le PFPDT outrepasserait ses compétences exécutives, car de telles directives ont indirectement un effet similaire à celui d'une loi. C'est pourquoi on a finalement renoncé à accorder ces compétences supplémentaires au PFPDT. En lieu et place, on mise sur les mesures autorégulatrices et individualisées des codes de conduite, qui ont été largement plébiscitées lors de la consultation. Les "meilleures pratiques" peuvent ensuite être inscrites dans le code de conduite lui-même. 5

B. Objectif de la norme

Le but de la norme et l'objectif du législateur sont de créer un cadre d'orientation ainsi qu'une sécurité juridique pour les parties prenantes et les associations économiques. Par une mesure d'autorégulation, une association peut concrétiser des directives de protection des données et les adapter de manière flexible aux nouveaux développements en matière de protection des données. 6

1. Promotion de la conformité à la protection des données

Les codes de conduite doivent promouvoir la conformité en matière de protection des données à deux niveaux : au premier niveau, ils constituent un cadre qui offre une sécurité juridique aux différents groupements et associations économiques. Les mesures relevant du droit de la protection des données peuvent désormais être réglementées de manière uniforme. Une concrétisation autonome offre également des possibilités d'adaptations spécifiques aux professions et de flexibilité par rapport aux évolutions de la protection des données. Cette dernière devrait notamment s'avérer particulièrement importante, étant donné que les progrès technologiques 7

s'installent à une vitesse fulgurante. Bien entendu, ces libertés doivent toujours tenir compte des dispositions de la LPD elle-même et être respectées. Ainsi, la nouvelle loi sur la protection des données pourra être mieux appliquée à long terme. Les destinataires doivent être incités à adopter un comportement conforme à la loi.

8 Au deuxième niveau, la loi représente un allègement pour le PFPDT. Il apparaît ainsi que l'adoption de codes par les responsables entraînera une uniformisation des directives de protection des données dans les différentes branches. Lors d'un éventuel contrôle d'un responsable, le PFPDT pourra se baser sur le code déjà approuvé et n'aura plus qu'à vérifier si celui-ci est respecté. Il n'est désormais plus nécessaire de chercher et de rassembler des règles de protection des données éparpillées dans les règlements et les statuts, ce qui peut prendre beaucoup de temps. Les contrôles d'admissibilité de la conformité à la protection des données ne sont plus ponctuels et axés sur des cas particuliers, mais s'appuient sur un ensemble uniforme de règles définies par un code de conduite.

2. L'autorégulation réglementée

9 Dans le cadre de la numérisation et de l'interconnexion mondiale, les prestataires de services intermédiaires et les exploitants de réseaux acquièrent une influence toujours plus grande sur la collecte et le traitement des données personnelles. De plus, le législateur ne peut généralement réagir qu'après qu'une technologie donnée a acquis une importance sociale et juridique.

10 L'"autorégulation réglementée" jette un pont entre les normes juridiques de l'État ("hard law") et les guides de droit privé spécifiques au secteur. Les codes de conduite en sont un exemple parfait. D'une part, les codes de conduite sont prévus par la loi et leur présentation a certaines conséquences juridiques (n. 30 s.), d'autre part, le législateur laisse aux associations une marge de manœuvre considérable quant à la manière dont elles souhaitent les élaborer en fonction de leur propre environnement. L'exemple du code de protection des données du Gesamtverband der Deutschen Versicherungswirtschaft, qui repose sur la réglementation analogue du RGPD, illustre la manière dont cela est organisé concrètement dans la pratique. Il établit des règles pour le traitement des données personnelles dans les activités typiques de l'assurance telles que les statistiques, le calcul des tarifs et des primes. Les règles relatives

à la transmission de données à différentes catégories de personnes spécifiques au secteur, telles que les réassureurs, les intermédiaires, les concurrents, etc. sont également définies plus précisément. En revanche, pour le traitement des données de solvabilité, il est renvoyé à la loi sans édicter de règles plus détaillées.

A l'intérieur du cadre fixé par la loi, les associations et les organes fédéraux peuvent s'orienter eux-mêmes et réglementer de manière spécifique à chaque branche. Les connaissances et la conscience de la protection des données augmentent au sein de l'entreprise. Des codifications de comportement contextualisées et précises conduisent à une plus grande sécurité juridique. Les normes spécifiques devraient également être mieux comprises et acceptées dans le secteur concerné. Offrir aux entreprises de telles mesures axées sur la pratique est indispensable pour un droit de la protection des données moderne, dynamique et surtout conforme. 11

II. CONTENU

A. Code de conduite

1. Un code de conduite en général

Un code de conduite est un document formel contenant un ensemble de normes. Il doit définir concrètement le comportement souhaité dans l'entreprise. Il jouit d'une bonne réputation dans la culture d'entreprise et est considéré comme un pilier important de la bonne gouvernance d'entreprise et est devenu un élément indispensable de la culture d'entreprise. 12

Un code de conduite ne fait toutefois pas partie d'un ordre juridique contraignant. Les entreprises décident elles-mêmes si elles souhaitent ou non adhérer à un code de l'association. Il s'agit d'un engagement volontaire. Une fois que l'entreprise s'est engagée, le code est en principe contraignant. C'est à l'association de décider comment et si elle veut imposer le respect de son code. L'objectif d'un tel code est de guider le comportement des collaborateurs et des cadres, tant au sein de l'entreprise que vis-à-vis de tiers extérieurs. Pour ce faire, il uniformise et systématise les actions quotidiennes et les normes de comportement à l'intérieur et à l'extérieur de l'entreprise. 13

14 Ainsi, un code de conduite protège l'entreprise de l'intérieur et de l'extérieur. A l'extérieur, les collaborateurs sont confortés dans leurs décisions et l'entreprise peut mieux se protéger contre les attaques externes en démontrant la conformité juridique, la compliance et la diligence par le biais du code de conduite. En interne, un code de conduite contribue à une culture d'entreprise saine et favorable en définissant des normes, par exemple dans le domaine de la communication, auxquelles les collaborateurs doivent se conformer. Cela renforce la confiance entre les collaborateurs.

15 Pour élaborer un code de conduite en général, il est utile de s'orienter sur des questions directrices. Il convient notamment de clarifier les points suivants :

- Comment dois-je me comporter ?
- Qu'est-ce que je peux faire et qu'est-ce qui est interdit ?
- Quand dois-je intervenir face au comportement d'un tiers ?
- Qui est mon interlocuteur si j'ai des questions, des doutes ou des incertitudes ?
- Que se passe-t-il si je ne respecte pas le code de conduite ?

16 Les points réglementés représentent pour les collaborateurs eux-mêmes une information importante sur les comportements souhaités. Il est donc important de formuler un code de conduite de manière claire et compréhensible et de l'adapter à l'entreprise. Les directives de comportement correspondantes sont en outre axées sur les risques spécifiques à l'entreprise ou au secteur d'activité de l'entreprise individuelle. Un code de conduite valable est régulièrement mis à jour et confirmé par la direction.

2. Codes de conduite en matière de protection des données

17 Les codes de conduite en matière de protection des données se réfèrent aux normes de la LPD, les développent et les adaptent spécifiquement à la branche concernée. Ils comprennent par exemple des modèles de déclarations de protection des données, des traitements de données à haut risque dans l'entreprise ou des instructions pour une anonymisation correcte des données. Vous trouverez ci-dessous une liste de questions directrices sur les domaines de réglementation possibles. Ces questions ne sont ni

exhaustives ni obligatoires. Elles offrent toutefois un aperçu de ce qui devrait figurer dans un code de conduite spécifique à la protection des données.

- Les données que je traite sont-elles correctes ?
- Qui est concerné par ce traitement de données ?
- Quelles données à caractère personnel sont collectées ?
- Quelles sont les données qui présentent un risque particulier ?
- Le cryptage des données peut-il être garanti de manière adéquate ?
- Les personnes concernées disposent-elles d'un droit d'accès ?
- L'entreprise dispose-t-elle de mesures techniques et organisationnelles de protection des données ?
- Conditions pour une transmission de données personnelles à l'étranger et garantie des garanties suisses en matière de protection des données
- Modalités procédurales en cas de conflit entre les personnes concernées et le responsable du traitement.

De telles questions directrices peuvent servir de point de départ aux associations. Toutefois, pour répondre aux exigences individuelles d'un secteur donné, des explications plus précises sont nécessaires, ainsi qu'une documentation et une réflexion minutieuses sur les données collectées au quotidien dans le secteur en question. Il convient de tenir compte des besoins des entreprises membres de l'association, c'est-à-dire des collaborateurs, des actionnaires, de la clientèle, etc. 18

3. Concrétisation et autorégulation

Le code de conduite selon l'art. 11 LPD applique donc les normes de la loi sur la protection des données à un état de fait concret. Les formulations générales sont concrétisées, précisées et rendues compréhensibles également pour les collaborateurs. 19

Elle doit être au moins aussi stricte que la LPD, avec éventuellement des directives plus strictes, spécifiques à la branche. L'association procède elle-même à des précisions. L'autorégulation et la responsabilité individuelle doivent ainsi être encouragées. Les interventions de l'État doivent être minimisées. De plus, une autonomie autorégulatrice favorise le sens des responsabilités des responsables. 20

21 L'État ne doit pas intervenir activement dans les activités des différentes branches ou autres associations, mais leur laisse le soin de concrétiser les clauses générales de la LPD en fonction de leurs besoins. Il en résulte une clarté de la situation juridique et des formulations précises.

B. Délimitation par rapport à la certification

22 L'article 13 LPD introduit des certifications de protection des données qui attestent de la conformité des systèmes, produits et services d'une entreprise avec la protection des données. Les organismes de certification agissent ici de manière indépendante dans le cadre des directives du PFPDT. Ainsi, contrairement aux codes de conduite, le PFPDT ne contrôle pas lui-même, mais n'exerce qu'une influence indirecte en édictant des réglementations sur la reconnaissance d'une certification (art. 13 LPD). L'OCPD sert de référence en la matière, puisqu'elle détaille et précise les exigences auxquelles doivent répondre les organismes de certification.

23 Les certifications en matière de protection des données servent à évaluer ponctuellement la conformité d'un système ou de certaines opérations de traitement avec la protection des données. Les codes de conduite, en revanche, décrivent toutes ou la plupart des exigences relatives aux activités de traitement d'une entreprise ou la manière dont elles doivent être traitées en fonction du secteur. En d'autres termes, les codes de conduite fournissent un cadre général d'orientation, tandis que les certifications de protection des données confirment la conformité d'une opération individuelle. Les certifications sont essentielles pour la mise en œuvre de la conformité en matière de protection des données dans la pratique. Alors que les codes de conduite définissent le comportement souhaité de manière analogue à la loi en théorie, la certification sert d'instrument dans la mise en œuvre des règles au quotidien.

24 Les certifications et un code de conduite ne s'excluent donc en aucun cas. Il semble ainsi qu'une entreprise puisse atteindre ses objectifs si, en plus d'un code de conduite, elle obtient des certifications ponctuelles en matière de protection des données auprès d'organismes qualifiés. Cela vaut surtout lorsque le traitement concret des données semble atypique, nouveau ou particulièrement risqué pour l'entreprise concernée.

III. AVIS DU PFPDT

Les associations professionnelles, sectorielles et économiques qui sont habilitées par leurs statuts à défendre les intérêts économiques de leurs membres sont légitimées à élaborer un code qui peut être soumis au PFPDT pour examen. 25

Les responsables individuels ou les sous-traitants ne peuvent pas soumettre leurs codes de conduite. Cela se justifie par le fait que l'article 11 LPD vise une certaine uniformisation au sein de certaines branches. 26

En revanche, par analogie avec l'article 89 CPC, les associations et organisations qui ont une certaine importance au niveau national ou au moins régional sont autorisées à déposer une demande. Une association cantonale remplira régulièrement cette condition. 27

La forme juridique de l'association n'est en principe pas déterminante. Toutefois, certaines entreprises, notamment les sociétés anonymes, sont exclues, car elles ne disposent pas de membres. Pour la même raison, les fondations n'ont pas le droit de présenter une demande. Les organisations de consommateurs et les associations de personnes concernées ne remplissent pas les conditions nécessaires pour représenter les intérêts économiques de leurs membres. 28

Les organes fédéraux ont toujours le droit de saisir la justice. Cela s'explique par les nombreuses dispositions légales et les différentes tâches qui incombent aux différents organes. 29

A. Portée juridique d'une saisine

Selon l'article 11 LPD, la présentation d'un code de conduite est en principe facultative pour les associations et les entreprises. Ce principe est relativisé par l'article 12 OLPD. Celui-ci prévoit l'obligation de soumettre le code au PFPDT pour approbation si une exportation de données doit être justifiée par le code (art. 12 OLPD). Le principe du volontariat, qui s'applique tant à l'élaboration des codes de conduite qu'à leur présentation au PFPDT, est désormais rompu par cette constellation de transferts de données à l'étranger. Cela peut se justifier par un standard de sécurité plus élevé, qui découle presque automatiquement de l'échange international de données, beaucoup plus risqué. Il s'agit ainsi de s'assurer que le code de conduite garantit une 30

protection suffisante des données. Cela est souligné par une obligation "contraignante et exécutoire" du responsable du traitement ou du sous-traitant dans l'État tiers de respecter le code de conduite (article 12, paragraphe 3, du RGPD). Elle devient contraignante par des mesures conformes au droit applicable dans l'État tiers concerné, comme par exemple l'inscription des codes dans les statuts du responsable.

31 Un modèle s'avère avantageux du point de vue du devoir de diligence et de la responsabilité civile au sein des entreprises représentées. En effet, seul un avis officiel officiel peut prouver de manière suffisante que le code est conforme à la législation sur la protection des données. Un code de conduite confirmé est une preuve directe que l'entreprise suit des règles claires en matière de protection des données qui satisfont à la LPD.

32 Dans la mesure où les codes de conduite sont des mesures autorégulatrices qui agissent sur les branches et les professions respectives pour lesquelles ils ont été élaborés, ils représentent une concrétisation juridique pour la pratique. Ils offrent donc également la possibilité que des directives de comportement généralement reconnues se forment dans un domaine particulier. Cela simplifie considérablement le respect de la protection des données par les entreprises, qui disposeraient ainsi d'un guide concret et d'un point de repère pour leur propre domaine d'activité.

B. Conséquences de l'avis

33 Le PFPDT est tenu d'émettre un avis. L'avis n'est pas une décision, mais un acte réel et n'est donc en principe pas contraignant. Néanmoins, une confirmation du PFPDT peut avoir différentes conséquences.

34 On peut toujours s'attendre à un avis positif lorsque le code prévoit le respect de toutes les dispositions de la LPD. Le critère de l'avis est donc la loi. Le PFPDT peut assortir l'avis de propositions d'amélioration et de recommandations, notamment en cas d'absence de concrétisation ou d'application incorrecte de la loi. Conformément à l'art. 59 LPD, un émolument est perçu auprès des personnes privées pour une prise de position. Conformément à l'art. 44, al. 1 et 2, OLPD, les émoluments se calculent en principe en fonction du temps consacré, le tarif horaire étant de 150 à 250 CHF, selon la fonction du personnel chargé de l'exécution.

On peut partir du principe, après un avis positif, que le comportement conforme au code n'entraînera pas de sanctions ou de mesures administratives, c'est-à-dire que les traitements de données conformes au code sont conformes à la protection des données. 35

En outre, il est possible de renoncer à une analyse d'impact sur la protection des données (AIPD) si le PFPDT émet un avis positif et si le code de conduite se fonde sur une AIPD encore actuelle qui protège la personnalité et les droits fondamentaux de la personne concernée (art. 22 al. 5 let. a et b LPD). Un code de conduite approuvé constitue une alternative ou une exception à l'obligation d'établir une analyse d'impact. Pour les analyses de risques d'une entreprise, il est judicieux de coupler les DSFA et les codes de conduite afin de minimiser autant que possible un éventuel risque lié à la protection des données. 36

Les conséquences d'une prise de position erronée posent question. Dans ce cas, la personne privée est persuadée que son propre code de conduite est conforme à la protection des données. Les traitements qui s'y fondent n'entraîneront donc pas de mesures administratives ou de sanctions. Si la personne privée viole malgré tout la protection des données en raison de renseignements erronés, elle risque malgré tout des sanctions dans certaines circonstances. En effet, les conditions d'une protection valable de la confiance sont strictes. Pour que celle-ci soit acceptée, il faut notamment que le code contienne des formulations suffisamment concrètes et que les faits survenus soient congruents avec ce qui est prévu. 37

L'article 11 ne prévoit pas de réglementation pour le cas où différentes associations fixent des règles différentes dans leurs codes pour des situations identiques ou qui se recoupent. Dans la mesure où les projets concurrents remplissent en eux-mêmes les conditions susmentionnées, le PFPDT donnera un avis favorable aux codes. Il est toutefois libre de signaler les contradictions dans son avis, étant donné que l'uniformisation des règles de protection des données est incluse dans l'objectif de la norme. 38

Il peut ainsi arriver qu'un responsable de traitement membre de différentes associations s'engage à respecter des codes de conduite contradictoires. Comme le PFPDT n'émettra un avis positif que si les exigences légales de la LPD sont remplies, il n'entrera pas en conflit avec la loi de ce fait. Néanmoins, il est recommandé de n'adhérer qu'à un seul code de conduite afin de 39

maintenir la rigueur des principes de protection des données internes à l'entreprise.

IV. AUTORÉGULATION SELON L'ARTICLE 40 DU RGPD

40 Le RGPD connaît également une norme d'autorégulation et de concrétisation de la protection des données. L'article 40 du RGPD parle de "l'élaboration de règles de conduite" par des fédérations ou des associations similaires. Ici aussi, on mise sur des mesures autorégulatrices des entreprises. Les règles doivent être considérées comme un complément et non comme un substitut aux dispositions légales.

41 Les exigences et les conséquences juridiques des codes de conduite et celles des règles de conduite sont similaires. Ainsi, les codes de conduite sont également soumis à une autorité de surveillance pour avis, qui est également publié. Le responsable doit respecter les principes de la protection des données conformément à l'obligation générale de rendre compte visée à l'article 5 al. 2 du RGPD et être en mesure de le prouver. La rédaction de règles de conduite facilite cette démarche. L'article 40 du RGPD précise les exigences relatives aux codes de conduite (al. 2 let. a à k) et prévoit différentes procédures pour assurer une protection sûre des données dans tous les États membres, notamment par le biais d'actes d'exécution de la Commission.

42 Le RGPD promet également aux entreprises des avantages et des facilités de preuve si elles se soumettent volontairement à des codes de conduite approuvés.

43 Contrairement à la Suisse, une règle de conduite qui a été soumise au Comité européen de la protection des données par l'autorité de surveillance nationale (article 63 du RGPD) et confirmée par ces dernières peut également avoir des effets au niveau de l'Union. Par le biais d'une déclaration de validité générale, les règles de conduite peuvent être déclarées valables dans toute l'Union (art. 40, al. 9 RGPD). Un code de conduite qui s'inspire uniquement de la LPD et qui n'a été soumis qu'au PFPDT n'a aucune garantie de conformité à la protection des données au niveau transnational. Il semble préférable que les associations (suisses) actives dans l'Union soumettent également leurs codes aux organes compétents de l'UE ou que les responsables reprennent des codes de conduite déjà approuvés. Cela facilite l'accès au marché et entraîne en même temps une augmentation de l'efficacité, car moins de temps et de

ressources doivent être consacrés aux processus bureaucratiques et réglementaires. En outre, il en résulte une harmonisation des normes, ce qui profite notamment aux entreprises actives à la fois en Suisse et dans l'UE.

BIBLIOGRAPHIE

Amacher Michel/Hajdini Lorian, Straf- und Strafprozessrecht/Geheime Überwachungsmassnahmen im digitalen Zeitalter, in: Alexandra Dal Molin-Kränzlin/Anne Mirjam Schneuwly/Jasna Stojanovic (Hrsg.), Digitalisierung - Gesellschaft - Recht, Zürich/St. Gallen 2019, S. 386.

Baeriswyl Bruno, Geschichten aus dem Wilden Westen - Der Datenschutz im privatrechtlichen Bereich geht seine eigenen Wege: Der Grundrechtsschutz bleibt auf der Strecke., digma 2011, S. 140 ff.

Drittenbass Joel, Regulierung von autonomen Robotern, Zürich 2021, S. 309 ff.

Gasser Dominik/Rickli Brigitte, Schweizerische Zivilprozessordnung (ZPO), Kurzkommentar, Zürich et al. 2014.

Kasper Gabriel, People Analytics in privatrechtlichen Arbeitsverhältnissen, Zürich 2021, S. 315 ff.

Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutzgrundverordnung BDSG, München 2020.

Kunz Laura, Kommentierung zu Art. 11 DSG in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Aufl., Zürich/Basel, 2023.

Lepperhoff Niels, Kommentierung zu Art. 40 DS-GVO in: Gola/Heckmann (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl., Königswinter et al. 2022.

Paal Boris P./Pauly Daniel A., Datenschutzgrundverordnung, Beck'sche Kompakt-Kommentare, 3. Auf., München 2021.

Portmann Wolfgang/Meier Anne (Hrsg.), Jahrbuch des Schweizerischen Arbeitsrechts 2021, Bern 2021, S. 57 ff. (zit. JAR 2021).

Richter Julia, Soft Law als Brückenbauer zwischen Wirtschaft und dem Schutz der Gesundheit?, Archiv des Völkerrechts 2014/52, S. 545 ff.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16.11.2020; Stirnimann Sonja, Der Verhaltenskodex aus praxistauglicher Perspektive, EF 10/22 2022, S. 460 ff.

Rothkegel Tobias, Verhaltensregeln und Zertifizierungen, in: Moos Flemming/Schefzig Jens/Arning Marian Alexander (Hrsg.), Praxishandbuch DSGVO, Frankfurt am Main 2021, S. 879 ff.

Wind Christian, Leitfaden Compliance, Zürich et al. 2018, S. 111 ff.

MATÉRIAUX

Botschaft vom 15.9.2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941 ff.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 12 LPD

Un commentaire de Ursula Sury / Jael Inauen

PROPOSITION DE CITATION

Ursula Sury/Jael Inauen, Commentaire de l'art. 12 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Sury/Inauen, art. 12 LPD N. XXX.

Art. 12 Registre des activités de traitement

[1] Les responsables du traitement et les sous-traitants tiennent chacun un registre de leurs activités de traitement.

[2] Le registre du responsable du traitement contient au moins les indications suivantes:

a. l'identité du responsable du traitement;

b. la finalité du traitement;

c. une description des catégories de personnes concernées et des catégories de données personnelles traitées;

d. les catégories de destinataires;

e. dans la mesure du possible, le délai de conservation des données personnelles ou les critères pour déterminer la durée de conservation;

f. dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données selon l'art. 8;

g. en cas de communication de données personnelles à l'étranger, le nom de l'État concerné et les garanties prévues à l'art. 16, al. 2.

[3] Le registre du sous-traitant contient des indications concernant l'identité du sous-traitant et du responsable du traitement, les catégories de traitements effectués pour le compte du responsable du traitement ainsi que les indications prévues à l'al. 2, let. f et g.

[4] Les organes fédéraux déclarent leur registre d'activités de traitement au PFPDT.

[5] Le Conseil fédéral prévoit des exceptions pour les entreprises qui emploient moins de 250 collaborateurs et dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées.

TABLE DES MATIÈRES

En bref ... 206
I. Généralités ... 207
A. Aperçu ... 207
B. Historique ... 207
C. Objectif de la norme ... 209
II. Contenu ... 210
A. Contenu d'un registre des traitements ... 210
B. Forme d'un registre ... 211
C. Obligations des personnes privées ... 212
1. Exigences légales ... 212
2. Le sous-traitant ... 212
3. Exceptions légales : PME ... 213
4. Exigences contractuelles ... 214
D. Obligations des organes fédéraux (art. 12, al. 4, LPD) ... 215
E. Mise en œuvre de la conformité avec la protection des données ... 216
1. Obligations d'information ... 216
2. Le droit d'accès ... 217
F. Données à l'étranger (art. 12, paragraphe 2, point g)) ... 218
III. Comparaison avec le droit de l'UE ... 219
Bibliographie ... 220
Matériaux ... 221

EN BREF

L'art. 12 LPD décrit l'obligation pour les organes fédéraux et les responsables et sous-traitants privés de tenir un registre des activités de traitement. Les données doivent être enregistrées tout au long de leur cycle de vie dans l'entreprise. Un registre comprend au minimum :

- l'identité des responsables
- les catégories de données personnelles traitées
- la finalité du traitement
- si possible, la durée de conservation ou au moins les critères de détermination de cette durée
- les destinataires des données traitées
- les mesures conformes à la protection des données
- les prescriptions relatives à la communication de données à l'étranger

Ne figurent pas dans le répertoire les catégories de données personnelles que l'entreprise ne traite pas du tout et les garanties pour la communication de données à l'étranger lorsqu'il n'y a pas d'exportation de données. De même, les données qui ne pourraient être obtenues en premier lieu qu'au prix d'efforts disproportionnés.

Enfin, les entreprises de moins de 250 collaborateurs (PME) sont légalement dispensées de l'obligation d'établir et de tenir un registre des traitements en raison de l'allégement administratif. Étant donné qu'un registre des activités de traitement sert à l'information interne de l'entreprise sur les données traitées ainsi qu'au respect des obligations de responsabilité et de diligence, il est recommandé à chaque entreprise de tenir un registre.

Le registre des activités de traitement, qui n'est soumis à aucune exigence de forme, est saisi au sein de l'entreprise et offre, entre autres, une possibilité d'autorégulation réglementée, parallèlement aux codes de conduite et aux certifications. D'une part, l'entreprise gagne en clarté sur les données qu'elle traite et, d'autre part, le PFPDT s'orientera lui aussi, dès l'entrée en vigueur de la LPD révisée, vers des registres de traitement des données afin de vérifier la conformité avec la protection des données.

I. GÉNÉRALITÉS

A. Aperçu

Conformément aux dispositions de la loi sur la protection des données (LPD), un registre des activités de traitement est un instrument important pour le respect des prescriptions en matière de protection des données. Il constitue un aperçu systématisé des activités de traitement des données et sert d'obligation aussi bien aux organes fédéraux qu'aux personnes privées. Il fournit des informations sur l'origine et la finalité des données, les aspects de conservation, ainsi que les mesures de sécurité appliquées et le transfert de données, éventuellement à l'étranger. La norme remplace l'art. 11a aLPD en relation avec l'art. 11 OPD. Art. 11 OLPD et précise et étend l'obligation de tenir un registre des fichiers. Les responsables doivent déterminer de manière autonome les données collectées en interne et les documenter de manière systématique. Le registre met ainsi davantage l'accent sur l'obligation de documentation et sur les processus de traitement des données. Un registre des activités de traitement doit toutefois être distingué d'un registre des fichiers et présente des exigences supplémentaires en termes de contenu (cf. N 6). 1

Grâce au registre des activités de traitement, les organisations disposent d'informations importantes sur leurs données numériques, elles ont une vue d'ensemble claire et actuelle. Ainsi, tant le PFPDT, dont le contrôle de la conformité d'une entreprise avec la protection des données est simplifié, que l'entreprise elle-même en profitent. 2

B. Historique

Conformément à l'art. 11a aLPD, le "préposé", c'est-à-dire le PFPDT, tenait un registre des fichiers ("registre") accessible au public. Alors que les organes fédéraux devaient déclarer tous leurs fichiers au PFPDT pour enregistrement (art. 11a, al. 1, aLPD), les particuliers n'étaient tenus de déclarer leurs fichiers que s'ils transmettaient régulièrement des données personnelles à des tiers (art. 11a, al. 3, let. b, aLPD) ou s'ils traitaient des profils de la personnalité ou des données sensibles (art. 11a, al. 3, let. aLPD). L'art. 11a al. 5 aLPD exemptait plusieurs maîtres de fichiers d'une obligation de déclaration au PFPDT, dont les titulaires d'une certification de protection des données ou les entreprises disposant d'un responsable de la protection des données. 3

4 L'art. 11a LPD ne précisait pas lui-même les exigences posées à un registre des fichiers, mais l'art. 11 OLPD les concrétisait. Selon cet article, le registre devait contenir des descriptions des structures organisationnelles internes et des procédures de traitement et de contrôle des données. Des justificatifs concernant la planification, la mise en œuvre et l'exploitation du fichier ainsi que les moyens informatiques utilisés devaient également y figurer. Ces précisions ne s'appliquaient qu'aux traitements de données soumis à déclaration.

5 La notion de "liste des activités de traitement" va cependant au-delà d'un bref aperçu des données collectées. Il comprend en outre les informations sur ce qui est fait avec les données, comment elles sont collectées et où elles sont transmises. Le contenu des registres se recoupe certes avec celui d'un registre des activités de traitement, mais il se concentre davantage sur la structure, la planification et la gestion internes (de l'entreprise). La notion de registre des fichiers ne figure plus dans la LPD actuelle, car elle a été remplacée par la liste des activités de traitement.

6 L'article 12 LPD est plus complet et exige des informations supplémentaires telles que l'identité du responsable, le but du traitement, une catégorisation des données personnelles traitées et des destinataires prévus, la durée de conservation et des mesures concrètes pour garantir la sécurité des données. Bien que de nombreux points se recoupent avec l'article 11 OLPD, les exigences sont beaucoup plus détaillées, ce qui devrait également simplifier l'établissement d'un registre. L'ancienne obligation générale de documentation, c'est-à-dire l'obligation de déclarer les fichiers, est également remplacée par le registre des traitements de données.

7 Avec l'entrée en vigueur de la nouvelle LPD, les personnes privées et les organes fédéraux doivent établir un registre des activités de traitement conformément à l'article 12 LPD. Toutefois, seuls les organes fédéraux doivent soumettre leur registre des traitements au PFPDT (art. 12, al. 4, LPD). L'obligation de tenir un registre s'applique en revanche également aux personnes privées. Le registre des activités de traitement permet de mieux contrôler ses propres données. Le registre des activités de traitement est désormais classé parmi les dispositions générales de protection des données.

C. Objectif de la norme

L'article 12 LPD est considéré comme une norme d'obligation pour les responsables du traitement et les sous-traitants. L'objectif de la norme est d'accroître la transparence lors du traitement des données. Cela est garanti par les exigences plus strictes posées au registre (art. 12 LPD) qu'à son ancien pendant, le registre des fichiers (art. 11a aLPD). Avec des indications minimales précises, les responsables disposent d'un cadre d'orientation clair pour savoir quelles données doivent figurer dans un registre. Les traitements de données sont ainsi enregistrés de manière uniforme. Il est plus facile pour le responsable interne de l'entreprise de garder une vue d'ensemble des données collectées. D'une part, il peut remplir de manière adéquate son devoir d'information et, d'autre part, satisfaire à son droit d'accès. 8

Une saisie systématique des données et des informations est généralement avantageuse pour les entreprises, et pas seulement dans le domaine des données personnelles. Un registre des matériaux ou une saisie des informations soumises à une obligation de confidentialité permettent à l'entreprise d'avoir un aperçu toujours actuel, correct et simplifié du flux d'informations interne. Ici aussi, le principe selon lequel la collecte et le relevé systématiques des données constituent une installation numérique importante s'applique. 9

Pour le PFPDT, la norme représente également une simplification. Il profite de l'uniformisation du répertoire, car il dispose désormais directement de toutes les catégorisations ou de tous les traitements pertinents. A l'avenir, le PFPDT demandera en premier lieu le répertoire lors d'une enquête. Néanmoins, le fait de ne pas tenir un registre n'entraîne pas de sanction immédiate. Le fait de fournir de faux renseignements ou de refuser son aide dans le cadre d'une enquête du PFPDT reste toutefois punissable, comme c'est déjà le cas dans le droit en vigueur. 10

II. CONTENU

A. Contenu d'un registre des traitements

11 L'art. 12 prévoit pour ce répertoire quelques exigences minimales en matière de contenu, qui sont les suivantes :

- Qui est responsable ?, art. 12, al. 2, let. a LPD.
  Le responsable est la personne qui décide de la finalité et des moyens d'un traitement de données. S'il y a plusieurs responsables, ils doivent tous être mentionnés.
- Quelle est la finalité du traitement, art. 12 al. 2 let. b LPD.
  La finalité peut varier ; ce qui est déterminant, c'est l'objectif poursuivi par un traitement de données. En règle générale, c'est la personne à l'origine du traitement qui décide également de sa finalité.
- Quelles personnes et quels types de données personnelles sont traités (catégorisations), art. 12 al. 2 let. c LPD.
  Les catégories de personnes concernées sont des groupes typiques tels que les "consommateurs" ou les "employés". Les catégories de "données personnelles traitées" désignent les types de données traitées, par exemple les données personnelles particulièrement sensibles.
- Qui est le destinataire des données traitées, art. 12 al. 2 let. d LPD.
  Les destinataires des données personnelles traitées sont également catégorisés, par exemple les autorités de surveillance.
- Combien de temps les données personnelles sont-elles conservées ou comment cette durée peut-elle être déterminée, art. 12 al. 2 let. e LPD ?
  Il s'agit notamment des délais d'archivage des données collectées. S'il n'existe plus de base légale ou de but défini pour la conservation des données personnelles collectées, celles-ci doivent être effacées ou rendues anonymes (art. 6 al. 4 LPD).
- Quelles sont les mesures prises pour garantir la sécurité des données conformément à l'art. 8, art. 12 al. 2 let. f LPD ?
  Il est fait référence aux principes fondamentaux de la protection et de la sécurité des données. Il s'agit notamment de l'intégrité des données collectées, de mesures techniques et organisationnelles appropriées et de "privacy by default" et "privacy by design".

- Quelles mesures doivent être prises pour communiquer des données à l'étranger ?, art. 12, al. 2, let. g LPD.
  Outre les mesures légales (cf. art. 16 ss LPD), ces mesures comprennent également des clauses contractuelles standard dans les contrats et des normes sectorielles fixées au niveau international (cf. à ce sujet l'art. 11 LPD en relation avec l'art. 12 OLPD).

L'article 12 est rédigé de manière très précise et détaillée, tout en permettant une certaine marge de manœuvre. La liste ne doit par exemple contenir que des informations dont le contenu est suffisamment certain. Une description ne doit être faite que si les activités peuvent être décrites de manière suffisamment concrète. Parfois, il n'est pas possible de déterminer la durée exacte de conservation. Ainsi, seuls les critères relatifs à la durée de conservation doivent être définis. En raison de cette conception large, il serait souhaitable d'élaborer des guides sectoriels qui pourraient être appliqués de manière uniforme dans les différentes branches. Tant le travail des entreprises que celui du PFPDT s'en trouveraient facilités. L'élaboration de guides sectoriels, qui pourraient être appliqués de manière uniforme dans les différentes branches, permettrait de concrétiser cette conception large. Cela aiderait tant les responsables que le PFPDT à faciliter leur travail. Les guides donneraient des instructions claires aux responsables et les aideraient à mieux comprendre et à mettre en œuvre les exigences en matière de protection des données dans leur secteur. Parallèlement, il permettrait au PFPDT de procéder à un examen et à une mise en œuvre plus uniformes de la protection des données dans différents secteurs. 12

B. Forme d'un registre

L'article 12 LPD ne règle pas dans le détail la manière exacte dont les traitements de données sont systématisés dans le registre des activités de traitement. Il n'y a pas non plus de prescriptions de forme. Un registre peut prendre la forme d'un simple document Word ou Excel, mais aussi d'une solution informatique complexe. Le registre peut être tenu de manière décentralisée et sa tenue peut même être déléguée. 13

C. Obligations des personnes privées

1. Exigences légales

14 En principe, toutes les entreprises et autres responsables privés sont tenus de tenir un registre des activités de traitement. Cela découle du fait que presque toutes les personnes privées collectent et traitent également des données personnelles dans le cadre de leur activité économique ou d'utilité publique.

2. Le sous-traitant

15 La liste des activités de traitement doit être tenue par le responsable du traitement et le sous-traitant (art. 12, al. 1, LPD). Par sous-traitant, on entend une personne qui traite des données pour le compte du responsable (art. 5 let. k LPD). Un exemple est le prestataire de services informatiques qui héberge un site web ou un employé qui prend les coordonnées des clients. Un responsable est en revanche la personne qui décide de la finalité et des moyens du traitement des données (art. 5 al. j LPD).

16 Chaque entreprise est exclusivement responsable des données qu'elle traite en interne. Un sous-traitant (processor), n'est pas tenu de tenir un registre de traitement pour les responsables. Les données du responsable, également appelé "contrôleur", ne doivent pas y figurer. Cela incombe uniquement au responsable lui-même, qui est responsable des données qu'il a collectées - par exemple les données des clients. Dans le cas contraire, cela entraînerait une saisie excessive de données personnelles. Cette exigence serait quasiment impossible à mettre en œuvre pour les entreprises. Il faudrait saisir l'ensemble des données personnelles du client pour chaque prestation. Il faudrait s'attendre à une prolifération des répertoires et à une perte de vue d'ensemble des données saisies. Le registre du sous-traitant contient donc moins d'informations que celui du responsable du traitement. En revanche, ce registre assure la transparence de la relation contractuelle entre le responsable du traitement et le sous-traitant, en exigeant que les deux parties soient clairement identifiables. Les conditions-cadres déterminantes sont fixées à l'article 9 LPD, qui clarifie le traitement des données par un sous-traitant.

3. Exceptions légales : PME

L'article 12 al. 5, prévoit une exception pour les entreprises qui emploient moins de 250 personnes et ne traitent pas de données à risque. Celles-ci sont exemptées de l'obligation de tenir un registre des activités de traitement. Les traitements de données à risque sont ceux qui ont une probabilité plus élevée d'entraîner une atteinte à la personnalité (atteinte à la sphère intime, données médicales, orientation sexuelle, confession et bien d'autres). Cette exception est également mentionnée à l'article 24 de l'ordonnance sur la protection des données (OPD). L'article 24 ne contient toutefois pas de dispositions plus détaillées sur l'exception légale. Il se contente de répéter que les PME sont exemptées de l'obligation de tenir un registre, sauf si elles traitent à grande échelle des données personnelles sensibles (let. a) ou si elles pratiquent un profilage à haut risque (let. b). La notion de risque élevé est utilisée de manière analogue à celle de l'art. 22, al. 2 LPD. 17

L'objectif de cette exception est d'alléger la charge administrative des petites entreprises. Il n'est pas seulement tenu compte de la taille de l'entreprise, mais aussi des données qui sont traitées et des risques qui y sont liés. Les PME sont également concernées par les sanctions prévues par la LPD et le respect des principes de protection des données est exigé des PME. Il en résulte pour les entreprises, bien qu'elles ne soient pas légalement tenues d'établir un registre des traitements, une obligation indirecte de documentation. En effet, qu'il existe ou non un registre des activités de traitement, le PFPDT s'occupera des mesures de protection des données au sein d'une PME. La PME doit donc de toute façon présenter les données traitées. Un registre permet de mieux protéger l'entreprise en termes de responsabilité civile et de devoir de diligence. 18

Si la moitié de toutes les données traitées sont à risque, elles tombent sous le coup des exigences des obligations de documentation renforcées, mais il se peut que la loi ne les oblige pas à figurer dans un registre des activités de traitement. La responsabilité et le risque d'éventuelles infractions à la législation sur la protection des données incombent toujours au responsable. Il est donc recommandé d'établir un registre des traitements lorsque des traitements de données à haut risque sont effectués, quelle que soit leur ampleur. 19

4. Exigences contractuelles

20 Il est également possible de prévoir contractuellement la tenue d'un registre. Bien qu'une telle obligation soit dispositive, elle pourrait prendre de l'importance selon le secteur. En effet, la tenue d'un registre des traitements permet à une entreprise de se prémunir non seulement contre le PFPDT et les exigences légales, mais aussi contre d'autres entreprises qui peuvent être aussi bien des partenaires que des clients. Si un responsable sait comment le sous-traitant traite et conserve les données et avec quels moyens, cela favorise la confiance et la collaboration entre les deux parties. En outre, la mise en œuvre d'une pratique de contractualisation des répertoires permet d'élaborer de manière autonome des répertoires adaptés aux secteurs économiques concernés et répondant aux enjeux spécifiques de la protection des données dans les domaines d'activité concernés.

21 Lors de la contractualisation des annuaires, certains aspects doivent être pris en compte et différents obstacles peuvent survenir. La mise en œuvre d'une telle pratique permet aux entreprises de créer de manière autonome des annuaires qui répondent aux exigences et aux défis spécifiques en matière de protection des données de leurs secteurs économiques respectifs.

22 L'un des obstacles consiste à rédiger les contrats de manière à ce qu'ils répondent aux exigences précises de la législation sur la protection des données. Des accords clairs doivent être conclus sur le type de données collectées, la finalité du traitement des données, la durée de conservation, les mesures de sécurité et d'autres aspects pertinents de la protection des données. Il est important de s'assurer que les accords contractuels sont conformes aux dispositions légales et que les droits des personnes concernées sont protégés de manière adéquate.

23 En outre, l'élaboration de répertoires spécifiques au secteur peut s'avérer difficile. Différents secteurs économiques ont des exigences différentes en matière de protection des données et des domaines d'activité spécifiques qui peuvent poser des défis particuliers en matière de protection des données. Les entreprises doivent être en mesure d'identifier ces exigences spécifiques et de les intégrer dans leurs répertoires afin de se conformer aux règles de protection des données.

24 La coopération entre les parties concernées, telles que les entreprises, les experts en protection des données et, le cas échéant, les autorités de contrôle,

peut être utile pour mettre en œuvre avec succès les accords contractuels et l'élaboration d'inventaires spécifiques au secteur.

D. Obligations des organes fédéraux (art. 12, al. 4, LPD)

Selon l'article 5 lettre i LPD, sont considérés comme organes fédéraux non seulement les autorités ou les services administratifs centraux, mais aussi toute autorité ou service de la Confédération, ainsi que les personnes qui accomplissent des tâches publiques de la Confédération. 25

Les organes fédéraux ont l'obligation, en vertu de l'art. 12, al. 4, LPD, de déclarer leurs listes d'activités de traitement au PFPDT. Conformément à l'art. 56 LPD, le PFPDT tient lui-même un registre des activités de traitement des organes fédéraux, qui est publié. 26

Déjà avant la révision de la loi sur la protection des données, les organes fédéraux étaient tenus de consigner les structures organisationnelles et les procédures de traitement des données dans un registre des fichiers. Cela impliquait implicitement d'indiquer le nom et l'adresse de l'organe fédéral responsable, une désignation du fichier, l'organe compétent pour le droit d'accès ainsi que la base juridique et le but. Les catégories de données personnelles traitées, les destinataires et les personnes participant au fichier devaient être saisies (art. 11a de l'ancienne LPD). Les registres de fichiers devaient également être déclarés au PFPDT pour enregistrement, conformément à l'art. 11a de l'ancienne LPD. D'une manière générale, les organes fédéraux étaient soumis à des exigences plus strictes. Le Conseil fédéral avait en outre la compétence de définir des règles particulières pour la protection des données (art. 16, al. 2, aLPD). 27

Il n'y a donc pas de modification importante des obligations des organes fédéraux. L'art. 12 LPD agit plutôt comme une extension aux personnes privées des obligations qui ne s'appliquaient auparavant qu'aux organes fédéraux. Un registre des activités de traitement doit donc être tenu sans exception par les organes fédéraux. Un registre déjà existant, correctement tenu à jour, répond déjà à de nombreuses exigences d'un registre, raison pour laquelle la mise en œuvre de la loi actuelle sur la protection des données ne nécessite souvent que peu ou pas de modifications. Le changement le plus important est qu'au lieu de distinguer les fichiers, on distingue désormais les traitements de données. 28

E. Mise en œuvre de la conformité avec la protection des données

29 En principe, un registre des activités de traitement n'est pas destiné aux personnes concernées, mais sert principalement au contrôle interne d'une entreprise ainsi qu'à l'examen par le PFPDT. L'établissement d'un registre des activités de traitement permet aux responsables d'être au clair sur leurs propres activités de traitement des données. La tenue d'un registre simplifie la mise en œuvre de certaines obligations et le respect des droits des personnes concernées, comme le droit d'accès (art. 25 LPD).

1. Obligations d'information

30 L'art. 19 LPD prévoit une obligation d'information pour le responsable du traitement et le sous-traitant lors de la collecte de données personnelles. L'identité et le contact du responsable, le but du traitement et, le cas échéant, les destinataires des données personnelles collectées doivent au moins être communiqués. Avec la révision de la protection des données, l'obligation d'informer a été étendue de manière générale. Avant la révision, elle ne s'appliquait qu'à la collecte de données sensibles ou de profils de la personnalité, alors qu'elle existe désormais pour toute collecte de données personnelles.

31 Un registre des activités de traitement permet d'informer la personne concernée de manière efficace et uniforme sur la collecte de ses propres données. En outre, la finalité, les moyens et, dans certaines circonstances, la durée de conservation peuvent être communiqués avec précision, puisque ces informations sont déjà contenues dans le registre. En ce sens, le répertoire représente un allègement administratif pour les entreprises, grâce auquel les processus d'information externes vis-à-vis des personnes concernées ou du PFPDT peuvent être organisés de manière plus simple et plus efficace. Plusieurs avantages découlent de cette conception plus efficace. Premièrement, le responsable réduit la charge administrative, car il ne doit plus établir et envoyer une notification séparée pour chaque traitement de données. Au lieu de cela, il peut faire référence au registre qui contient déjà toutes les informations nécessaires. Deuxièmement, la communication avec les personnes concernées est uniformisée. Comme toutes les informations sont contenues dans l'annuaire, toutes les personnes concernées reçoivent les mêmes informations sur la finalité, les moyens et la durée de conservation, ce

qui permet une communication plus cohérente et plus transparente. Troisièmement, le registre facilite également la collaboration avec des parties externes, comme le Préposé fédéral à la protection des données et à la transparence (PFPDT). Lorsque le PFPDT demande des informations sur le traitement des données, l'entreprise peut simplement fournir le registre au lieu de devoir établir des rapports séparés pour chaque traitement de données.

2. Le droit d'accès

Le droit d'accès prévu à l'article 25 LPD est un droit de la personne concernée qu'un particulier peut faire valoir dans le cadre de la législation sur la protection des données. Le droit d'accès permet de vérifier la légalité d'un traitement de données et la personne concernée a le droit d'exiger l'autorisation ou la suppression des données. Conformément à l'article 25 de la LPD, la personne concernée reçoit toutes les informations sur ses propres données personnelles afin de pouvoir faire valoir ses droits, notamment l'identité du responsable du traitement, la finalité du traitement et les données personnelles traitées elles-mêmes. Les droits qui peuvent ensuite être exercés sont par exemple le droit à la rectification des données personnelles collectées de manière erronée ou à la suppression de ces dernières (art. 32 LPD). 32

Un registre des activités de traitement garantit et soutient le droit d'accès, car il comprend l'ensemble des informations qui doivent être communiquées à la personne concernée conformément à l'article 25 LPD. Un registre bien tenu permet à la personne concernée d'obtenir des informations complètes, uniformes et correctes sur les données collectées. Une information adéquate est garantie et la sécurité est accrue pour les deux parties, car l'entreprise a déjà en principe une meilleure vue d'ensemble des données collectées et court moins de risques d'enfreindre les dispositions légales en matière de protection des données. Si le registre n'est pas correct, cela peut conduire le responsable à ne pas collecter correctement les informations sur le traitement des données ou à prendre des mesures de sécurité insuffisantes. Cela comporte un risque de violation de la protection des données et peut entraîner des conséquences juridiques. 33

F. Données à l'étranger (art. 12, paragraphe 2, point g))

34 Selon l'art. 12, al. 1, let. g LPD, le pays concerné doit être indiqué en cas de communication de données à l'étranger, ainsi que les garanties prévues à l'art. 16, al. 2 LPD. Ces dispositions garantissent que la personne concernée est informée de la transmission de ses données personnelles à l'étranger et que des mesures de protection appropriées sont prises pour la protection des données. Le registre des activités de traitement peut inclure ces exigences en indiquant le but précis du transfert de données à l'étranger et en désignant le pays de destination. En outre, la liste devrait également contenir des informations sur les garanties mises en place conformément à l'article 16, paragraphe 2, LPD, afin de rassurer la personne concernée sur l'existence de mesures de protection adéquates. Il est important que la personne concernée soit informée de manière claire et compréhensible du fait que ses données sont transférées à l'étranger et des mesures de protection qui ont été prises à cet égard. Cela permet de garantir le droit d'accès de la personne concernée et de protéger sa vie privée. Elles renforcent les exigences en matière de protection des données lors d'un traitement et d'une communication transfrontaliers de données. En principe, les données personnelles ne peuvent être communiquées à l'étranger que si le Conseil fédéral a décidé que ce pays garantit lui-même une protection adéquate des données. Le Conseil fédéral détermine quels pays présentent un niveau de protection des données adéquat et le publie dans l'annexe 1 de l'ordonnance sur la protection des données. La Russie, une grande partie des pays africains et sud-américains ainsi que toute l'Asie (à l'exception d'Israël), entre autres, offrent une protection insuffisante.

35 L'art. 16 al. 2 LPD exige soit un traité international, soit des clauses contractuelles de protection des données, soit des garanties spécifiques approuvées par le PFPDT, soit des clauses de protection standard, soit des directives internes contraignantes en matière de protection des données, également approuvées par le PFPDT (art. 16 let. a-e LPD). Celles-ci s'appliquent désormais lors d'une communication de données non seulement lorsque le pays lui-même ne garantit pas une protection suffisante, mais aussi lors de toute communication à l'étranger.

III. COMPARAISON AVEC LE DROIT DE L'UE

L'art. 12 LPD, comme d'autres articles après la révision totale, présente quelques parallèles avec les conditions du RGPD. Ainsi, l'article 12 a été conçu de manière analogue à l'article 30 du RGPD. Tant l'article 30 du RGPD que l'article 12 de la LPD imposent aux organes publics et aux personnes privées de tenir un registre. L'identité du responsable du traitement et du sous-traitant doit y être indiquée. Les deux dispositions exigent des informations sur le but du traitement, les catégories de données personnelles traitées et les destinataires, les garanties de transfert à l'étranger, la durée de conservation et les mesures techniques et organisationnelles relatives à la mise en œuvre de la sécurité des données. L'exception à l'établissement d'un registre de traitement des données est également conservée tant à l'article 30 RGPD qu'à l'article 12 LPD. L'expression "si possible" (al. 1, let. f et g) permet, comme dans la loi suisse sur la protection des données, une certaine flexibilité. Le contenu d'un registre n'est pas fixé de manière stricte et identique pour chaque entreprise, mais s'oriente en fonction de la précision avec laquelle les données traitées peuvent être décrites. Ainsi, il n'est pas toujours possible de dire avec certitude quand les données seront effacées, et toutes les entreprises suivent des mesures techniques et organisationnelles analogues et généralement reconnues. Ici aussi, un registre de données doit pouvoir s'adapter à l'activité concernée. 36

Des différences entre les dispositions apparaissent sporadiquement dans les formulations et les explications. Comme le PFPDT en Suisse, l'autorité de surveillance de la protection des données dans l'UE assume des fonctions similaires de contrôle du respect du RGPD ou de la LPD. L'art. 30 du RGPD exige en outre que l'identité du délégué à la protection des données soit indiquée dans le registre, s'il en existe un dans l'entreprise. Le transfert à l'étranger doit être spécifiquement indiqué selon le RGPD et la forme d'un répertoire doit être écrite. Les institutions publiques ou les personnes privées ont également l'obligation, en vertu du droit de l'Union, de mettre le registre des activités de traitement à la disposition de l'autorité de contrôle, à sa demande. Une coopération de bonne foi avec les autorités publiques est en principe requise. 37

Outre l'article 30 du RGPD, l'article 24 de la directive 2016/680 précise le contenu d'un registre des activités de traitement. Il convient seulement de mentionner ici que l'article 24 de la directive prévoit également l'utilisation du 38

profilage (article 24 al. 1 let. e)) et l'indication de la base juridique des transferts de données à caractère personnel (article 24 al.1 let. g) dans un registre de traitement. Cela n'est pas prévu dans la réglementation suisse, mais peut être couvert par des indications complémentaires dans la finalité du traitement ou des catégorisations de données personnelles traitées.

BIBLIOGRAPHIE

Baeriswil Bruno, Kommentierung zu Art. 12 DSG in: Baeriswil Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpfli Handkommentar zum DSG, 2. Aufl., Zürich/Basel, 2023.

Bucheli Bernadette, Datenschutz im Mietverhältnis: Ausgangslage und Revision des DSG, mp 2020, S. 383 ff.

Pärli Kurt/Eggmann Jonas, Das Auskunftsrecht im Privatrecht, digma 2020, S. 140 ff.

Rosenthal David, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, Jusletter 17.6.2019 (zit. Rosenthal, Controller oder Processor)

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16.11.2020 (zit. Rosenthal, Datenschutzgesetz)

Rosenthal David/Gubler Seraina, Die Strafbestimmungen des neuen DSG, SZW 2021, S. 52 ff. Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. Rosenthal/Jöhri), S. 304 ff.-

Steiner Thomas, Neues DSG: Umsetzung und Anwendung in Anwaltskanzleien, Anwaltsrevue 2022, S. 417 ff.

Sury Ursula, Neues Datenschutzgesetz und Dokumentation von Unternehmen, SJZ 2021, S. 458 ff.

Trüeb Hans Rudolf/Zobl Martin, Steuerdaten in der Cloud?, digma 2016, S. 102 ff.

Vasella David, Das neue Datenschutzgesetz und seine Umsetzung, TREX 2021, S. 272 ff.

MATÉRIAUX

Botschaft vom 15.9.2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941 ff.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 14 LPD

Un commentaire de Martin Steiger

PROPOSITION DE CITATION

Martin Steiger, Kommentierung zu Art. 14 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Steiger, N. XXX zu Art. 14 DSG.

Section 2
Traitements de données personnelles par des responsables du traitement privés ayant leur siège ou leur domicile à l'étranger

Art. 14 Représentant

[1] Le responsable du traitement privé qui a son siège ou son domicile à l'étranger désigne un représentant en Suisse lorsqu'il traite des données personnelles concernant des personnes en Suisse et que ce traitement remplit les conditions suivantes:

a. le traitement est en rapport avec l'offre de biens ou de services ou le suivi du comportement de personnes en Suisse;

b. il s'agit d'un traitement à grande échelle;

c. il s'agit d'un traitement régulier;d.le traitement présente un risque élevé pour la personnalité des personnes concernées.

[2] Le représentant est le point de contact pour les personnes concernées et le PFPDT.

[3] Le responsable du traitement publie le nom et l'adresse de son représentant.

TABLE DES MATIÈRES

En bref ... 226
I. Généralités ... 226
A. Objectif ... 226
B. Historique ... 226
II. obligation de désigner un délégué à la protection des données (al. 1) ... 227
A. champ d'application personnel ... 227
B. champ d'application matériel ... 228
1. en relation avec l'offre de biens ou de services ou avec l'observation du comportement de personnes en Suisse (let.) ... 228
2. traitement global (let. b) ... 229
3. traitement régulier (let. c) ... 229
4. risque élevé pour la personnalité des personnes concernées (let. d) ... 229
III. fonction du délégué à la protection des données (al. 2) ... 230
IV. désignation volontaire d'un délégué à la protection des données ... 231
V. Communication du nom et de l'adresse (al. 3) ... 231
Bibliographie ... 232

EN BREF

L'art. 14 LPD régit l'obligation de désigner un délégué à la protection des données en Suisse par les responsables privés ayant leur siège à l'étranger. Cette obligation n'existe que sous certaines conditions cumulatives et ne devrait s'appliquer en pratique qu'à un petit nombre de responsables. Cette représentation doit servir de point de contact pour les personnes concernées et le PFPDT afin de faciliter l'application de la LPD à l'égard de certains responsables du traitement à l'étranger. Les responsables du traitement doivent publier le nom et l'adresse de leur représentant, par exemple dans le cadre de la déclaration de confidentialité sur leur site web.

I. GÉNÉRALITÉS

A. Objectif

1 Les responsables de traitement qui n'ont pas leur siège en Suisse doivent désigner un représentant en Suisse sous certaines conditions, qui sont rarement remplies. La formulation de ces conditions entraîne une insécurité juridique quant au moment où elles sont remplies.

2 L'obligation peut être justifiée par le vaste champ d'application territorial de la LPD, car la LPD s'applique à toutes les affaires ayant des répercussions en Suisse, même si elles sont engagées à l'étranger (art. 3 al. 1 LPD). L'obligation de désigner un représentant vise à améliorer l'applicabilité pratique de la LPD, à l'instar de la représentation en matière de protection des données de l'UE prévue à l'art. 27 LPD.

B. Historique

3 La LPD a été complétée au cours des débats parlementaires par la représentation en matière de protection des données conformément aux articles 14 et 15 LPD. Ces deux articles forment, avec les "Dispositions générales", la section 2 "Traitement de données par des titulaires privés ayant leur siège ou leur domicile à l'étranger". La structure s'inspire de la représentation de l'UE en matière de protection des données selon l'art. 27 du DSGVO. Selon ce texte, le délégué à la protection des données peut être une

personne morale ou une personne physique. Le règlement sur la protection des données (RGPD) ne mentionne pas la représentation.

La représentation en matière de protection des données touche aux revendications politiques concernant une juridiction obligatoire pour les grandes plateformes Internet étrangères, comme notamment les plateformes de médias sociaux, en matière de droit pénal et civil, mais ne les met pas en œuvre. Un projet de consultation du Conseil fédéral annoncé pour 2024 sur la réglementation des grandes plateformes de communication, selon lequel de telles plateformes doivent désigner un point de contact et un représentant juridique en Suisse, pourrait apporter une concrétisation possible de ces demandes d'élection de domicile obligatoire. 4

II. OBLIGATION DE DÉSIGNER UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES (AL. 1)

L'art. 14 al. 1 LPD définit les conditions dans lesquelles les responsables du traitement des données doivent exceptionnellement désigner un délégué à la protection des données en Suisse. Contrairement au représentant de la protection des données de l'UE selon l'art. 27 al. 1 et 2 RGPD, il n'existe pas d'obligation générale assortie d'exceptions. En conséquence, le nombre de responsables de données concernés devrait être faible. 5

Le PFPDT peut ordonner ou disposer de la désignation d'un représentant en tant que mesure administrative (art. 51 al. 4 LPD). 6

Le non-respect de l'obligation de désigner un représentant ne tombe pas sous le coup des dispositions pénales des articles 60 et suivants LPD. LPD. Le non-respect d'une injonction du PFPDT de désigner un représentant peut être sanctionné par une amende (art. 63 LPD). 7

A. champ d'application personnel

L'obligation de désigner un représentant s'applique aux responsables privés de données (art. 5 let. j LPD) ayant leur siège ou leur domicile à l'étranger s'ils traitent des données de personnes en Suisse (art. 5 let. a et b LPD) et si le traitement remplit les conditions cumulatives de l'art. 14 al. 1 let. a-d LPD. Contrairement à la représentation de la protection des données de l'UE, 8

l'obligation en Suisse ne s'applique qu'aux responsables du traitement des données et non pas également aux personnes traitant les données.

B. champ d'application matériel

1. en relation avec l'offre de biens ou de services ou avec l'observation du comportement de personnes en Suisse (let.)

9 L'article 14 al. 1 let. a LPD se fonde sur les conditions alternatives pour le champ d'application territorial de la LPD par l'offre ou l'observation d'un comportement (article 3 al. 2 LPD), plutôt que sur le principe de l'effet selon l'article 3 al. 1 LPD. Selon ce principe, l'exigence ne s'applique que si une offre ou une observation de comportement a un effet sur un état de fait en Suisse. Un simple lien avec une offre ou une observation du comportement n'est pas suffisant.

10 La première exigence cumulative de l'art. 14 al. 1 let. a LPD est remplie, d'une part, si le traitement de données personnelles est en rapport avec l'offre de biens et de services à des personnes en Suisse. Selon le considérant 80 relatif à l'art. 27 al. 3 RGPD, une offre gratuite ou non est suffisante.

11 La seule accessibilité des offres, par exemple dans une application sur une plateforme de médias sociaux ou via un site web, n'est pas suffisante. Il faut des indices concrets montrant qu'une offre s'adresse effectivement à des personnes en Suisse. Les indices possibles sont par exemple des contenus dans les langues nationales suisses, des possibilités de livraison en Suisse, des indications de prix en francs suisses, des prix avec indication de la TVA suisse, la publication d'un numéro de téléphone suisse ou l'utilisation d'un domaine de premier niveau suisse (.ch ou .swiss).

12 En revanche, la première exigence cumulative de l'art. 14 al. 1 let. a LPD est remplie si le traitement est effectué dans le cadre de l'observation du comportement de personnes en Suisse en tant qu'alternative à l'offre ou en même temps que l'offre. Le terme "observation du comportement" est utilisé au sens de l'art. 3 al. 2 du DSGVO. Le simple enregistrement de l'accès à un service en ligne ou à un site web ne suffit donc pas. Il faut qu'il y ait un ciblage effectif de personnes en Suisse ou que l'observation conduise à un profilage par rapport aux personnes concernées en Suisse. Ainsi, la disposition devrait s'appliquer aux fournisseurs de plateformes Internet comme ByteDance,

Google et Meta, mais pas, par exemple, aux exploitants de boutiques en ligne, tant que leur modèle commercial n'est pas centré sur les données et que le profilage des utilisateurs n'est effectué que dans une mesure habituelle à des fins de marketing propres.

2. traitement global (let. b)

La deuxième condition cumulative selon l'art. 14 al. 1 let. b LPD est remplie lorsque le traitement de données personnelles est de grande ampleur. La loi n'explique pas ce qu'il faut entendre par "traitement à grande échelle". 13

L'art. 22 al. 2 let. a LPD cite comme exemple de traitement de données à risque le traitement à grande échelle de données personnelles sensibles, mais n'explique pas non plus ce qu'est un "traitement à grande échelle". Des critères possibles seraient un grand nombre de personnes concernées en Suisse ou une grande quantité de données sur des personnes en Suisse. 14

3. traitement régulier (let. c)

La troisième exigence cumulative de l'article 14 al. 1 let. c LPD est remplie s'il y a un traitement régulier de données personnelles. La loi n'explique pas ce qu'il faut entendre par "traitement régulier". 15

Il est évident qu'il n'y a pas de régularité lorsque les responsables du traitement ne traitent les données à caractère personnel qu'occasionnellement ou pendant une période limitée. En revanche, il devrait y avoir régularité lorsqu'un responsable du traitement traite régulièrement des données à caractère personnel afin d'exercer son activité (exemple : offre par le biais d'une boutique en ligne) ou poursuit un modèle commercial centré sur les données (exemple : surveillance par le biais d'une plateforme de médias sociaux). 16

4. risque élevé pour la personnalité des personnes concernées (let. d).

La quatrième condition cumulative selon l'art. 14 al. 1 let. d LPD est remplie lorsque le traitement comporte un risque élevé pour la personnalité des personnes concernées. Cette exigence correspond à l'approche basée sur les risques de la LPD, mais sans mention des droits fondamentaux des personnes concernées (voir p. ex. aussi l'art. 5 let. g LPD : profilage à haut risque ; art. 22 al. 1 et al. 2 LPD : analyse d'impact relative à la protection des données ; art. 17

24 al. 1 LPD : notification des violations de la sécurité des données). L'absence de mention des droits fondamentaux des personnes concernées est probablement un oubli législatif, compte tenu des autres mentions de la LPD.

18 Le traitement de données présentant un risque élevé pour la personnalité des personnes concernées devrait être rare dans la pratique. Il est donc rare que les analyses d'impact relatives à la protection des données révèlent un risque élevé ou qu'un tel risque soit éliminé par des mesures appropriées.

III. FONCTION DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES (AL. 2)

19 Le préposé à la protection des données sert de point de contact pour les personnes concernées et le PFPDT. Les personnes concernées et le PFPDT peuvent s'adresser à la représentation, mais ne sont pas tenus de le faire. La représentation est juridiquement considérée comme ayant le droit de notifier.

20 La représentation est donc un point de contact alternatif pour les personnes concernées et le PFPDT en tant qu'autorité particulière à côté de l'entité responsable. Si l'entité responsable a désigné un délégué à la protection des données, il existe au total trois points de contact alternatifs différents (art. 10 al. 1 et 2 LPD).

21 Le délégué à la protection des données d'un responsable du traitement des données ne peut pas agir en même temps comme délégué à la protection des données du même responsable du traitement des données. La représentation serait incompatible avec l'indépendance du conseiller à la protection des données (art. 10 al. 3 let. a et b LPD).

22 Pour les personnes concernées, la représentation en tant que point de contact présente l'avantage particulier de leur permettre de s'adresser directement au service responsable en Suisse pour les questions relevant de la protection des données, notamment dans le cadre de leurs droits au sens des art. 25 ss. LPD. Dans le cas des maîtres de fichiers sans représentation en Suisse, les personnes concernées doivent par exemple adresser leurs demandes de renseignements aux maîtres de fichiers respectifs ou à leurs délégués à la protection des données à leur siège ou domicile à l'étranger.

23 Pour le PFPDT, la représentation en tant que point de contact présente notamment l'avantage de ne pas devoir atteindre les responsables du

traitement des données à l'étranger par le biais de l'entraide judiciaire internationale.

La loi ne précise pas dans quelles langues les personnes concernées peuvent contacter la représentation. Dans le cas d'une représentation liée à l'offre, les personnes concernées devraient au moins pouvoir s'adresser à la représentation dans la langue de l'offre ou dans l'une des langues de l'offre. La limitation aux langues nationales ne semble pas appropriée. Le PFPDT devrait pouvoir contacter la représentation dans l'une des quatre langues officielles suisses (art. 33a LPO par analogie). 24

IV. DÉSIGNATION VOLONTAIRE D'UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Le responsable du traitement des données peut également désigner un délégué à la protection des données en Suisse sans y être obligé par l'article 14 al. 1 LPD. Le responsable du traitement des données peut également confier au représentant volontaire et au représentant obligatoire des tâches qui dépassent les obligations prévues aux art. 14 s. LPD. 25

V. COMMUNICATION DU NOM ET DE L'ADRESSE (AL. 3)

Le maître du traitement des données doit communiquer le nom et l'adresse de son délégué à la protection des données. Dans le cas d'une personne morale en tant que préposé, la raison sociale correspond au nom. La publication d'une adresse électronique ou d'un numéro de téléphone n'est pas expressément requise. Toutefois, en cas de publication dans l'espace numérique, il est évident de proposer un moyen de contact numérique, notamment une adresse électronique. En comparaison, l'art. 13 al. 1 let. a du DSGVO prévoit non seulement l'"adresse", mais aussi les "données de contact". 26

Pour remplir sa fonction de point de contact (article 14 al. 2 du DSGVO), le nom et l'adresse du représentant doivent être publiés sous une forme facilement repérable et accessible. Il est logique de publier ces informations dans le cadre de la déclaration générale de protection des données sur le site web du responsable ou, le cas échéant, dans les mentions légales. 27

28 Contrairement aux obligations d'information selon l'art. 13 f. RGPD, le nom et l'adresse de la représentation en Suisse ne relèvent pas de l'obligation d'information selon l'art. 19 f. LPD.

29 Contrairement au préposé à la protection des données (art. 10 al. 3 let. d LPD), il n'existe pas d'obligation de notification au PFPDT pour la représentation. Le PFPDT doit déduire des informations publiées si un responsable des données a désigné un représentant ou se renseigner directement auprès de ce dernier.

BIBLIOGRAPHIE

Husi-Stämpfli Sandra, Kommentierung zu Art. 14 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023. (zit. SHK-Husi-Stämpfli, Art. 14 DSG).

Rosenthal David, Das neue Datenschutzgesetz, in: Jusletter vom 16.11.2020 (zit. Rosenthal, Jusletter).

Lang Markus, Kommentierung zu Art. 27 DSGVO, in: Taeger Jürgen/Gabel Detlev, DSGVO – BDSG – TTDSG, 4. Aufl., Bremen 2022 (zit. Taeger/Gabel, Bearbeiter/-in).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 15 LPD

Un commentaire de Martin Steiger

PROPOSITION DE CITATION

Martin Steiger, Kommentierung zu Art. 15 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Steiger, N. XXX zu Art. 15 DSG.

Art. 15 Obligations du représentant

[1] Le représentant tient un registre des activités de traitement du responsable du traitement qui contient les indications mentionnées à l'art. 12 al. 2.

[2] Il fournit sur demande au PFPDT les indications contenues dans ce registre.

[3] Il fournit sur demande à la personne concernée des renseignements concernant l'exercice de ses droits.

TABLE DES MATIÈRES

En bref 235
I. généralités 235
II. obligations du délégué à la protection des données 235
A. liste des activités de traitement (al. 1) 235
B. obligation de communiquer au PFPDT (al. 2) 236
C. information des personnes concernées (al. 3) 236
Bibliographie 237

EN BREF

L'art. 15 LPD mentionne certaines autres obligations pour une représentation en matière de protection des données conformément à l'art. 14 LPD. La représentation doit tenir un registre des activités de traitement pour le compte du ou des responsables et communiquer les données correspondantes au PFPDT sur demande. En outre, la représentation doit fournir aux personnes concernées, sur demande, des informations sur l'exercice de leurs droits.

I. GÉNÉRALITÉS

L'art. 15 LPD énumère certaines autres obligations du représentant à la protection des données en complément des obligations prévues à l'art. 14 al. 2 et 3 LPD (fonction de point de contact, art. 14 al. 2 LPD, et publication des coordonnées, art. 14 al. 3 LPD). L'énumération de l'art. 15 LPD n'est pas exhaustive en raison de la définition large du rôle de la représentation en tant que point de contact. 1

II. OBLIGATIONS DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES

A. liste des activités de traitement (al. 1)

Selon le texte, le délégué à la protection des données doit tenir un registre des activités de traitement du responsable du traitement (al. 1). Cette obligation va plus loin que celle prévue à l'art. 30 al. 1 RGPD, selon laquelle le représentant de l'UE pour la protection des données ne doit tenir un registre que pour les activités de traitement qui relèvent de sa compétence. Cette obligation excessive, en tout cas nettement plus étendue que celle du RGPD, constitue probablement un oubli législatif. 2

L'exception prévue pour les entreprises de moins de 250 collaborateurs, conformément à l'art. 12 al. 5 LPD en relation avec l'art. L'art. 24 OCPD ne s'applique pas à la représentation de la protection des données. Conformément à l'art. 14 al. 1 let. a LPD, le représentant chargé de la protection des données ne doit être désigné que si le traitement effectué par 3

le responsable présente un risque élevé, notamment pour la personnalité des personnes concernées. Cela correspond à l'approche générale de la LPD basée sur les risques, telle qu'elle est exprimée notamment à l'art. 24 OLPD.

4 Les informations contenues dans le registre doivent être conformes à l'art. 12 al. 2 LPD. Dans la pratique, le ou la responsable tiendra un registre partiel des activités de traitement qui ont un impact sur la Suisse et en fournira une copie à la représentation.

B. obligation de communiquer au PFPDT (al. 2)

5 La représentation doit communiquer au PFPDT, sur demande, les informations contenues dans l'inventaire (al. 2), même en l'absence de procédure administrative. Dans la pratique, il est probable que la représentation communique l'annuaire au PFPDT plutôt que de fournir uniquement les informations qu'il contient.

6 Cette obligation s'applique donc indépendamment de l'obligation du ou des responsables de fournir au PFPDT tous les documents nécessaires dans le cadre d'une enquête (art. 49 al. 3 LPD) et également indépendamment du pouvoir du PFPDT d'ordonner l'accès à tous les registres nécessaires des activités de traitement dans le cadre d'une enquête (art. 50 al. 1 let. a LPD).

7 Avec la représentation comme point de contact, le PFPDT n'a pas besoin de passer par la voie de l'entraide judiciaire internationale pour obtenir les données du répertoire. La représentation en Suisse ne peut communiquer que les données dont elle dispose déjà.

8 Une représentation désignée volontairement ne doit pas tenir un registre en tant que telle.

C. information des personnes concernées (al. 3)

9 En tant que point de contact (art. 14 al. 2 LPD), la représentation doit informer les personnes concernées qui en font la demande de l'exercice de leurs droits conformément aux art. 25 ss. LPD.

10 La représentation doit permettre aux personnes concernées qui en font la demande d'exercer leurs droits. La représentation doit par exemple informer les personnes concernées des coordonnées et des voies par lesquelles elles peuvent exercer leur droit d'accès (art. 25 ss LPD) auprès du responsable et

leur indiquer si le ou la responsable a désigné un conseiller ou une conseillère à la protection des données (art. 10 LPD) qui peut être consulté (art. 10 al. 2 LPD).

Le devoir d'information du ou de la responsable concerné(e) (art. 19 ss. LPD) n'est pas affecté par l'obligation d'information de la représentation. Le ou la responsable peut en outre charger la représentation de fournir d'autres renseignements aux personnes concernées. 11

BIBLIOGRAPHIE

Husi-Stämpfli Sandra, Kommentierung zu Art. 15 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023. (zit. SHK-Husi-Stämpfli, Art. 15 DSG).

Eidgenössisches Justiz- und Polizeidepartement, EU-Datenschutzgrundverordnung DSGVO: Erläuterungen betreffend die Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DSGVO, 4.9.2018 (zit. EJPD, Erläuterungen).

Gogniat Yves, Die Datenschutzgrundverordnung im Kontext von Art. 271 StGB, in: Jusletter vom 19.11.2018 (zit. Gogniat, Art. 271 StGB).

Rosenthal David, Das neue Datenschutzgesetz, in: Jusletter vom 16.11.2020 (zit. Rosenthal, Jusletter).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 19 LPD

Un commentaire de Matthias Glatthaar / Annika Schröder

PROPOSITION DE CITATION

Matthias Glatthaar/Annika Schröder, Kommentierung zu Art. 19 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Glatthaar/Schröder, N. XXX zu Art. 19 DSG.

Chapitre 3
Obligations du responsable du traitement et du sous-traitant

Art. 19 Devoir d'informer lors de la collecte de données personnelles

[1] Le responsable du traitement informe la personne concernée de manière adéquate de la collecte de données personnelles, que celle-ci soit effectuée auprès d'elle ou non.

[2] Lors de la collecte, il communique à la personne concernée les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la présente loi et pour que la transparence des traitements soit garantie; il lui communique au moins:

a. l'identité et les coordonnées du responsable du traitement;

b. la finalité du traitement;

c. le cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises.

[3] Si les données personnelles ne sont pas collectées auprès de la personne concernée, il communique en outre les catégories de données traitées à cette personne.

[4] Lorsque des données personnelles sont communiquées à l'étranger, il communique également à la personne concernée le nom de l'État ou de l'organisme international auquel elles sont communiquées et, le cas échéant, les garanties prévues à l'art. 16, al. 2, ou l'application d'une des exceptions prévues à l'art. 17.

[5] Si les données personnelles ne sont pas collectées auprès de la personne concernée, il communique à cette personne les informations mentionnées aux al. 2 à 4 au plus tard un mois après qu'il a obtenu les données personnelles. S'il communique les données personnelles avant l'échéance de ce délai, il en informe la personne concernée au plus tard lors de la communication.

TABLE DES MATIÈRES

En bref ... 242
I. Généralités ... 242
A. But de la norme ... 242
B. Historique ... 243
C. Classification et délimitation ... 244
D. Notes d'interprétation ... 245
II. Personne soumise à l'obligation et point de rattachement (al. 1) ... 245
A. Personne obligée ... 245
B. Point de rattachement ... 246
III. Contenu de l'information (al. 2-4) ... 247
A. Informations obligatoires ... 247
1. Généralités ... 247
2. Données de contact ... 247
3. Finalités du traitement ... 248
4. Destinataires des données ... 248
5. Données personnelles traitées ... 249
6. États destinataires ... 250
7. Décisions individuelles automatisées ... 251
B. Autres informations ... 251
IV. Modalités de l'information (al. 5 ; art. 13 OLPD) ... 252
A. Moment ... 252
B. Forme ... 253
C. Mise à disposition ... 255
D. Communication ... 256
V. Conseils pratiques ... 258
A. Procédure et outils ... 258
B. Préparation et conception ... 259
VI. Application et conséquences juridiques ... 261
A. Droit administratif ... 261
B. Droit pénal ... 261
C. Droit civil ... 262
D. DSGVO ... 262
VII. Critique de la norme ... 263
Bibliographie ... 264
Matériaux ... 265

EN BREF

Le devoir d'information selon l'art. 19 LPD concerne les déclarations de protection des données importantes dans la pratique et doit concrètement augmenter la transparence des traitements de données. Elle complète le principe général de transparence et exige que les personnes concernées soient informées des points essentiels du traitement des données lors de chaque collecte de données personnelles. Le catalogue des informations minimales à communiquer est plus court que celui du RGPD et comprend les coordonnées, les finalités du traitement, les catégories de données traitées, les catégories de destinataires des données, des informations sur les transferts à l'étranger ainsi que des indications sur les décisions individuelles automatisées. Toutefois, l'art. 19 LPD va plus loin que le RGPD sur un point et exige en outre l'indication des pays destinataires, l'indication de groupes de pays ou de régions étant suffisante. Dans la plupart des cas, les informations ne doivent pas être communiquées activement aux personnes concernées et il suffit qu'elles soient mises à disposition de manière facilement accessible sur Internet. L'obligation d'information fait partie des faits punissables de la loi révisée sur la protection des données : Quiconque omet intentionnellement de fournir des informations ou fournit intentionnellement des informations fausses ou incomplètes peut être sanctionné par une amende. Compte tenu du fait que, dans la pratique, les déclarations de protection des données ne sont pratiquement jamais lues ou comprises dans le détail, il semble douteux que l'obligation d'informer permette réellement d'atteindre l'objectif poursuivi, à savoir accroître la transparence des traitements de données.

I. GÉNÉRALITÉS

A. But de la norme

1 L'art. 19 LPD réglemente le devoir d'information du responsable lors de la collecte de données personnelles. Il s'agit des avis de protection des données, importants dans la pratique, ou des déclarations de protection des données, très répandues dans la vie économique. Le devoir d'information fait partie des dispositions clés du droit de la protection des données, ce qui se traduit parfois par le fait qu'il compte parmi les dispositions de la nouvelle loi sur la protection des données qui sont passibles de sanctions.

L'objectif du devoir d'information est d'accroître la transparence des traitements de données. Un traitement transparent des données personnelles est un principe fondamental du droit de la protection des données et l'augmentation de la transparence était un objectif déclaré de la révision de la LPD. Les personnes concernées doivent savoir que des données les concernant sont traitées et elles doivent avoir la possibilité de connaître les points essentiels du traitement des données. 2

La transparence des traitements de données doit permettre aux personnes concernées de prendre une décision informée sur le recours à des offres et l'utilisation de services, et leur permettre d'exercer les droits que leur confère la législation sur la protection des données. L'obligation d'informer sert donc aussi indirectement à renforcer les droits des personnes concernées, ce qui correspond à un autre objectif de la révision. 3

Enfin, selon le message, l'obligation d'informer doit permettre de sensibiliser davantage la population à la protection des données et donc de promouvoir les questions de protection des données en général. 4

B. Historique

L'art. 19 LPD renforce l'obligation d'informer lors de la collecte de données personnelles qui figurait déjà dans l'ancienne LPD. Sous l'ancien droit, les personnes concernées ne devaient être informées qu'en cas de collecte de données personnelles sensibles ou de profils de la personnalité. Désormais, les responsables doivent en principe informer lors de chaque collecte de données personnelles. La nouvelle LPD élargit également de manière modérée le catalogue des informations obligatoires. La LPD révisée regroupe en outre les dispositions jusqu'ici dispersées dans plusieurs articles et crée une réglementation uniforme pour le traitement par des responsables privés et par des organes fédéraux. 5

L'augmentation de la transparence des traitements de données faisait partie des objectifs principaux de la révision de la LPD. De plus, la Convention 108 sur la protection des données, contraignante pour la Suisse, prescrit un devoir général d'information lors de la collecte de données personnelles, ce qui doit être transposé dans le droit national. La directive (UE) 2016/680, pertinente pour le domaine Schengen, connaît également une obligation d'information. L'extension du devoir d'information n'a donc pas été contestée dans le 6

processus législatif. A quelques modifications près, le texte devenu loi correspond à la version du projet.

C. Classification et délimitation

7 L'art. 19 LPD complète le principe général de transparence de l'art. 6 LPD. Alors que le principe de transparence crée une transparence de base, l'obligation d'information, qui s'appuie sur ce principe, répond à un besoin d'information plus large. Le responsable doit non seulement s'assurer que la collecte de données est reconnaissable en tant que telle, mais aussi fournir aux personnes concernées certaines informations sur les finalités et les modalités du traitement. Illustration avec la comparaison de denrées alimentaires de David Rosenthal : les consommateurs doivent pouvoir reconnaître immédiatement qu'il s'agit d'une confiture de fraises (principe de transparence), tandis que la liste des ingrédients et d'autres détails ressortent de l'étiquette des denrées alimentaires, qui peut être consultée en cas d'intérêt (obligation d'information).

8 Contrairement au principe de transparence, le devoir d'information n'est pas une concrétisation du droit de la personnalité de l'art. 28 CC, mais est de nature publique. La violation du devoir d'information ne constitue donc pas une atteinte à la personnalité. Une violation ne peut donc pas non plus être justifiée en vertu de l'art. 31 LPD. Les exceptions et les limitations du devoir d'information sont définies de manière exhaustive à l'article 20 LPD.

9 L'art. 19 LPD est à son tour complété par l'art. 21 LPD, qui prévoit un devoir d'information particulier en cas d'automatisation complète de décisions importantes, et concrétisé par l'art. 13 OLPD, qui pose des exigences quant à la manière dont l'information doit être fournie.

10 Le devoir d'information doit être distingué du concept de consentement. Une déclaration de protection des données assure la transparence exigée par la loi, mais ne constitue pas un consentement en vertu du droit de la protection des données et ne légitime pas une action en vertu de l'art. 30 s. LPD. LPD qui doit être justifié. Il existe toutefois un lien entre le devoir d'information et les consentements dans la mesure où, d'une part, la déclaration de protection des données permet de créer la base d'information nécessaire à un consentement valable et où, d'autre part, le respect du devoir d'information et l'obtention d'un consentement peuvent coïncider dans un cas particulier (p. ex.

lorsqu'une déclaration de consentement contient toutes les indications obligatoires exigées par l'art. 19 LPD).

D. Notes d'interprétation

L'obligation d'information de la loi révisée sur la protection des données s'inspire de l'obligation d'information contenue dans le RGPD. L'art. 19 LPD ne reprend toutefois pas simplement l'obligation d'information du RGPD, mais établit une réglementation qui s'écarte délibérément du RGPD sur certains points. Par exemple, la LPD prescrit moins d'informations minimales que le RGPD et accorde des exceptions plus larges à l'obligation d'information. Comme l'a montré Thomas Steiner, l'article 19 LPD doit donc être interprété de manière autonome et la pratique du RGPD ne doit être utilisée que pour confirmer et plausibiliser le résultat de l'interprétation suisse. 11

Avec David Vasella, il faut en outre se prononcer en faveur d'une interprétation réservée de l'obligation d'information : D'une part, l'art. 19 LPD est également une norme fondant une infraction pénale et le principe de légalité pénale exige donc une interprétation restrictive. D'autre part, l'exécution de l'obligation d'informer est liée à des dépenses considérables pour les entreprises, ce qui touche à la liberté économique selon l'art. 27 Cst. et n'est admissible que si l'intervention est proportionnée et limitée à la mesure nécessaire. Enfin, une certaine retenue dans l'interprétation s'impose également parce qu'une transparence de base est déjà garantie par le principe de transparence de l'article 6 LPD et que l'obligation d'informer ne protège qu'un besoin d'information allant au-delà. 12

II. PERSONNE SOUMISE À L'OBLIGATION ET POINT DE RATTACHEMENT (AL. 1)

A. Personne obligée

L'obligation d'informer s'adresse au responsable du traitement, c'est-à-dire à la personne privée ou à l'organe fédéral qui décide de la finalité et des moyens du traitement. Les sous-traitants soumis à des instructions ne sont pas soumis à l'obligation d'informer pour les traitements effectués sur mandat du responsable. 13

14 Le responsable n'est pas tenu d'exécuter lui-même l'obligation d'information. Il peut également déléguer l'information à un sous-traitant ou à un autre tiers (p. ex. à une agence web pour l'exploitation d'un site web). Même dans de tels cas, le responsable reste toutefois responsable de l'exécution correcte de l'obligation d'information.

B. Point de rattachement

15 L'obligation d'informer est déclenchée par toute collecte de données personnelles, indépendamment du fait que le responsable collecte les données directement auprès de la personne concernée ou indirectement. Le mode de collecte des données n'a d'importance que pour le moment de l'information. Il n'est pas non plus déterminant de savoir s'il s'agit d'une collecte durable ou répétée ou, comme dans le cas d'un jeu-concours isolé, d'une collecte unique de données. Dans les deux cas, l'information doit être fournie. Le fait d'utiliser des données personnelles déjà existantes dans un but nouveau ou supplémentaire constitue également une (nouvelle) collecte qui déclenche l'obligation d'informer.

16 Il n'est pas nécessaire d'informer le responsable lorsque des données personnelles lui parviennent par hasard ou sans qu'il ait à intervenir. Il s'agit par exemple de demandes de journalistes, de candidatures spontanées, de recommandations de collaborateurs ou de demandes non sollicitées par courrier électronique. L'information doit toutefois être fournie si ces données personnelles reçues involontairement doivent être utilisées à des fins nouvelles ou supplémentaires.

17 Le fait que l'obligation d'informer soit liée à l'événement de la collecte des données signifie, en termes de droit transitoire, que les personnes concernées ne doivent pas être informées, lors de l'entrée en vigueur de la nouvelle LPD, des traitements de données déjà en cours (dans la mesure où l'information n'a pas déjà été faite de toute façon à un moment antérieur). Une information des personnes concernées, par exemple des clients existants, doit cependant avoir lieu au plus tard lorsque de nouvelles données sont collectées, par exemple pour les abonnés à un service en ligne lors de leur prochaine connexion ou pour les participants à un programme de fidélisation de la clientèle lors de leur prochain achat.

III. CONTENU DE L'INFORMATION (AL. 2-4)

A. Informations obligatoires

1. Généralités

L'art. 19 LPD contient aux al. 2 à 4 une liste d'informations obligatoires qui doivent impérativement être communiquées aux personnes concernées : Coordonnées du responsable, finalités du traitement, destinataires des données ou catégories de destinataires, catégories de données traitées ainsi que pays destinataires en cas de transmissions à l'étranger et leur protection. Peu d'informations obligatoires supplémentaires figurent dans d'autres dispositions de la LPD, notamment à l'art. 21 LPD concernant les décisions individuelles automatisées et à l'art. 14 al. 3 LPD concernant la représentation en Suisse. 18

En comparaison avec le RGPD, le catalogue de la LPD est court. Il faut s'en féliciter et cela laisse tout de même la place, en dehors du champ d'application du RGPD, d'informer avec mesure et de lutter contre la "surcharge d'informations" qui sévit aujourd'hui. La réglementation flexible de la LPD permet de limiter l'information aux données pertinentes en fonction des risques et d'omettre les données inutiles. 19

2. Données de contact

Tout d'abord, le nom et les coordonnées du responsable doivent être indiqués. La loi ne précise pas quelles données de contact doivent être communiquées. Il est toutefois évident qu'il faut indiquer au moins une adresse postale et une adresse électronique. L'indication d'un numéro de téléphone est également envisageable, mais inhabituelle et plutôt déconseillée compte tenu de la possibilité de prises de contact importunes par des personnes mal intentionnées. 20

Les responsables domiciliés à l'étranger doivent également publier le nom et les coordonnées d'un représentant en Suisse éventuellement désigné en vertu de l'art. 14 LPD (art. 14 al. 3 LPD). 21

La mention des coordonnées d'un éventuel conseiller à la protection des données désigné est facultative. Ceci à la différence du RGPD, où les coordonnées du conseiller à la protection des données doivent 22

obligatoirement être communiquées. La LPD incite toutefois (un peu) à publier les coordonnées du conseiller à la protection des données en ce sens que les responsables privés ne peuvent se prévaloir de l'exception à la notification du PFPDT qu'en cas de risques résiduels élevés après avoir effectué une analyse d'impact relative à la protection des données. Pour cela, il suffit de publier une boîte aux lettres fonctionnelle (p. ex. datenschutz@unternehmen.ch) ; il n'est pas nécessaire de mentionner le nom du conseiller à la protection des données.

3. Finalités du traitement

23 Le responsable du traitement doit indiquer les finalités pour lesquelles les données personnelles sont traitées. Les personnes concernées doivent donc pouvoir savoir dans quel but leurs données sont traitées.

24 Le degré de détail avec lequel les finalités du traitement sont décrites est laissé à l'appréciation du responsable. Des désignations courtes telles que "communication", "exécution de contrats", "développement de produits" ou "marketing" sont en principe autorisées. Des descriptions plus détaillées ou des exemples explicatifs sont toutefois plus utiles, ce qui est également recommandé au regard du principe de finalité, car des formulations peu claires seraient, en cas de doute, interprétées de manière restrictive au détriment du responsable du traitement, conformément au principe de confiance.

25 Outre les finalités actuelles du traitement, il est également possible de mentionner les éventuelles finalités futures du traitement. Cela est également admissible lorsque les traitements concernés ne sont pas encore concrètement prévus, mais ne constituent qu'une possibilité. Compte tenu du principe de finalité de l'article 6, al. 3, LPD, de nombreuses entreprises seront tentées de rédiger de tels avis de protection des données excessifs afin de se réserver autant que possible de nouvelles utilisations des données, ce qui ne favorise toutefois pas la clarté des avis de protection des données.

4. Destinataires des données

26 Il convient ensuite d'indiquer les catégories de destinataires auxquels les données personnelles sont transmises. La mention "le cas échéant" dans le texte de loi n'a guère d'importance pratique, étant donné que les sous-traitants engagés par le responsable du traitement font également partie des

destinataires et que, de nos jours, rares sont les responsables du traitement qui peuvent se passer entièrement de sous-traitants. Les responsables conjoints sont également considérés comme des destinataires, tout comme les "tiers" proprement dits. Les sociétés du même groupe sont également des destinataires, mais pas les entités appartenant à la même entité juridique, telles que les départements ou les succursales.

Les catégories peuvent être définies par le responsable comme il l'entend, la loi ne donne aucune indication à ce sujet. On pourrait par exemple imaginer des catégories assez étroitement définies comme "prestataire de services informatiques", "entreprise de logistique" ou "prestataire de services de recouvrement", mais des catégories plus sommaires comme "sous-traitant" sont également autorisées. 27

Au lieu de catégories de destinataires, il est également possible de mentionner des destinataires individuels. La mention de destinataires individuels est toutefois facultative, l'indication de catégories suffit. Dans la pratique, on renonce généralement à indiquer des destinataires individuels, car la plupart des entreprises disposent d'un grand nombre de destinataires (surtout des sous-traitants) et la mise à jour d'une liste correspondante serait fastidieuse. L'indication de destinataires concrets s'est quelque peu répandue dans le domaine en ligne, où les outils de tiers utilisés sont parfois mentionnés individuellement en relation avec les cookies et autres technologies similaires. 28

5. Données personnelles traitées

Il convient ensuite d'indiquer les catégories de données personnelles traitées. Ici aussi, le responsable est libre de définir les catégories comme il l'entend et de choisir le degré de détail qui lui semble judicieux et approprié pour une information suffisante des personnes concernées. On pourrait par exemple imaginer des catégories telles que "données de base", "données de comportement" ou "données de préférence". Des catégories telles que "données personnelles sensibles" ou "données relatives à la santé" sont également possibles. En règle générale, il est en outre utile de concrétiser les catégories parfois peu saisissables par des exemples de types de données (p. ex. "nom", "adresse électronique", "lieu de résidence") et de les rendre plus tangibles. Il est également utile, mais pas nécessaire, d'affecter les différentes catégories de données à des fins de traitement concrètes. 29

30 Conformément à l'art. 19 al. 3 LPD, les catégories de données traitées ne doivent être indiquées que si les données ne sont pas collectées directement auprès de la personne concernée. L'idée sous-jacente est que la personne concernée n'a besoin d'être informée que dans ce cas. En revanche, si elle communique elle-même ses données personnelles (p. ex. en remplissant un formulaire en ligne ou un bulletin de participation à un jeu-concours ou en transmettant une candidature à un emploi), elle connaît déjà les données traitées par le responsable du traitement.

31 Suivant cette idée, la limitation doit être interprétée de manière stricte et se limiter aux cas où la personne concernée communique sciemment des données. En revanche, les catégories de données traitées doivent également être indiquées, par exemple, lorsque les données sont certes collectées directement auprès de la personne concernée, mais que cela se fait sans son intervention active et qu'elle n'a donc éventuellement pas conscience que des données la concernant sont traitées. C'est par exemple le cas lors de la collecte automatisée de données de transaction lors d'achats dans des magasins ou dans le commerce en ligne ou lors du webtracking sur Internet. Pour les mêmes raisons, les catégories de données traitées doivent également être indiquées lorsque le responsable du traitement déduit de nouvelles données à partir de celles reçues de la personne concernée, par exemple des informations sur les intérêts et affinités personnels.

6. États destinataires

32 En cas de communication de données personnelles à l'étranger, les États destinataires doivent être indiqués. Selon l'art. 5 let. e LPD, on entend par communication, outre la transmission, tout accès à des données personnelles depuis l'étranger. De telles transmissions à l'étranger sont très fréquentes dans le monde des entreprises, par exemple lors de l'utilisation de services basés sur le cloud.

33 Avec l'obligation d'indiquer les pays destinataires, la LPD est sans nécessité plus stricte que le RGPD, où seules les informations sur la communication à l'étranger elle-même doivent être fournies, mais pas celles sur les pays destinataires. La LPD ne tient pas compte du caractère international des échanges de données. Toujours est-il que la LPD n'impose pas non plus de dresser une liste des différents pays, ce qui serait difficilement praticable dans la pratique. Il suffit d'indiquer des groupes de pays ou des régions, par

exemple "UE/EEE" ou "Europe". Il est également possible d'indiquer "mondial". Pour les personnes concernées, il est évident que leurs données peuvent en principe être traitées dans n'importe quel pays du monde.

Si, parmi les pays destinataires, se trouvent des États ne disposant pas d'un niveau de protection des données adéquat, des indications supplémentaires doivent être fournies : Dans de telles constellations, il faut communiquer les garanties prises conformément à l'art. 16 al. 2 LPD pour assurer une protection des données appropriée ou l'exception revendiquée conformément à l'art. 17 LPD. Dans ce cas, il suffit par exemple de mentionner la conclusion des clauses contractuelles standard reconnues par la Commission européenne et le PFPDT, qui sont de loin l'instrument le plus courant pour garantir les transferts à l'étranger. 34

7. Décisions individuelles automatisées

Dans la mesure où le responsable utilise des décisions individuelles automatisées, il doit en informer les personnes concernées ainsi que de la possibilité de soumettre la décision à un examen humain à la demande de la personne concernée (art. 21 LPD). Sont considérées comme décisions individuelles automatisées les décisions qui sont entièrement automatisées et qui ont des conséquences juridiques pour les personnes concernées ou qui les affectent considérablement d'une autre manière. L'obligation d'informer ne s'applique donc qu'aux décisions entièrement automatisées ; il n'est pas nécessaire d'informer sur les décisions qui ne sont que partiellement automatisées ou qui sont prises par ordinateur. 35

B. Autres informations

Dans la pratique, de nombreuses entreprises iront au-delà des informations obligatoires présentées ci-dessus et s'inspireront généralement du catalogue plus complet du DSGVO. Ce sont surtout les grandes entreprises à vocation internationale (mais pas seulement) qui aspirent à des mentions de protection des données "conformes au RGPD", que ce soit sur une base volontaire ou parce que leurs traitements de données relèvent du champ d'application (extraterritorial) du RGPD. Le catalogue du DSGVO prévoit notamment aussi des indications sur la durée de conservation, la base juridique applicable, les intérêts légitimes poursuivis le cas échéant, les droits des personnes concernées et le droit de recours. 36

37 Toutefois, l'inclusion de telles informations supplémentaires n'est généralement pas prescrite par la LPD. Les informations allant au-delà du catalogue minimal ne doivent être fournies que si elles sont nécessaires dans le cas concret pour garantir un traitement des données suffisamment transparent (art. 19 al. 2 LPD). Cela ne sera que rarement le cas et il est d'autant plus probable que les données traitées sont sensibles, que le traitement est important, que les modalités du traitement sont critiques, que la criticité de la finalité du traitement est grande et que les technologies utilisées pour le traitement sont nouvelles. Conformément à l'art. 19 al. 2 LPD, la ligne directrice est ce que les personnes concernées doivent savoir pour pouvoir faire valoir leurs droits.

38 Le catalogue du DSGVO devrait constituer une sorte de limite supérieure. Il n'est guère possible d'imaginer des cas dans lesquels il serait nécessaire, en vertu de la LPD, d'aller encore plus loin que les informations exigées par le RGPD.

39 La réglementation de la LPD laisse théoriquement la possibilité de concrétiser dans un code de conduite selon l'article 11 LPD l'application de l'obligation d'information pour une branche déterminée. De tels codes de conduite spécifiques à un secteur n'ont toutefois pas encore réussi à s'imposer dans la pratique et ne joueront probablement qu'un rôle secondaire à l'avenir.

IV. MODALITÉS DE L'INFORMATION (AL. 5 ; ART. 13 OLPD)

A. Moment

40 Selon que les données personnelles sont collectées directement auprès de la personne concernée ou indirectement, l'information doit être fournie à des moments différents. Il y a collecte directe lorsque la personne concernée communique de son propre chef ses données au responsable (p. ex. en remplissant un formulaire ou en créant un compte d'utilisateur) ou lorsque le responsable collecte lui-même les données par observation ou de manière automatisée (p. ex. en enregistrant des transactions d'achat ou en collectant des données de mouvement au moyen d'un tracker de fitness). En revanche, il y a collecte indirecte lorsque le responsable recueille des données à partir de sources publiques (p. ex. rapports des médias ou registres publics), les obtient de tiers (p. ex. d'un commerçant d'adresses ou d'une agence de renseignements économiques) ou déduit de nouvelles données à partir de

bases de données existantes (p. ex. déduction de préférences par l'analyse de données de transaction).

En cas d'acquisition directe, l'information doit être fournie en même temps que l'acquisition. Dans la pratique, cela signifie que les informations requises doivent être facilement accessibles au moment de la collecte, par exemple sur le site web du responsable. L'information immédiatement après la première collecte de données, qui était encore autorisée sous l'ancien droit, ne l'est plus sous le nouveau droit. En revanche, une information préalable à la collecte est possible, pour autant que le lien entre l'information et la collecte soit suffisamment reconnaissable pour les personnes concernées. 41

En cas de collecte indirecte, l'information ne doit pas être donnée immédiatement, mais dans un délai d'un mois à compter de la réception des données (art. 19 al. 5 LPD). Le délai de carence d'un mois présuppose toutefois que les données personnelles ne sont pas communiquées à un autre destinataire par le responsable. En revanche, si le responsable communique les données personnelles avant l'expiration du délai, le délai de carence ne s'applique pas et l'information doit avoir lieu au plus tard au moment de la communication. Comme les communications aux sous-traitants sont également concernées (par ex. un stockage dans le cloud), le report de l'information n'a que peu d'importance pratique et il faut généralement informer directement, même en cas d'acquisition indirecte, ce qui nécessite souvent une communication active. Si cela s'avère impossible à mettre en œuvre, le responsable n'a d'autre choix que de recourir à un cas d'exception selon l'article 20 LPD. 42

B. Forme

La LPD ne contient pas de prescriptions de forme pour la communication des informations. Une information orale est également suffisante, par exemple sous la forme d'annonces enregistrées. Dans la pratique, la forme textuelle est toutefois généralement recommandée, ne serait-ce que pour des raisons de preuve. 43

Dans la pratique, le moyen le plus répandu pour remplir l'obligation d'information est la déclaration de protection des données ("Privacy Notice" ou "Privacy Policy"). Il est courant de décrire dans une déclaration générale de protection des données une large palette de traitements de données (des 44

opérations avec les clients à la collaboration avec les partenaires commerciaux en passant par le recrutement de personnel) et de la compléter de manière ciblée par des déclarations de protection des données spécifiques à des produits ou à des services. Dans la pratique, les déclarations de protection des données en ligne ("Cookie Notice" ou "Cookie Policy") sont également très répandues pour les traitements de données liés à la visite d'un site web ou d'une application.

45 Les déclarations de protection des données constituent une information unilatérale du responsable du traitement et peuvent, en tant que telles, être adaptées de manière flexible, notamment pour tenir compte de la nature dynamique de nombreux traitements de données. D'un point de vue pratique, l'information unilatérale signifie en outre qu'aucune confirmation ou acceptation active de la déclaration de protection des données par les personnes concernées n'est nécessaire et qu'il est donc possible, dans la plupart des cas, de renoncer aux cases à cocher que l'on trouve souvent dans les formulaires en ligne ou les processus de commande.

46 Il est également envisageable d'inclure des informations sur la protection des données dans les conditions générales (CG). Toutefois, contrairement aux déclarations de protection des données, les informations relatives à la protection des données contenues dans les conditions générales font partie intégrante du contrat et ne peuvent donc être modifiées que par le biais d'une adaptation du contrat, ce qui s'avère souvent trop lourd dans la pratique. En outre, les conditions générales ne permettent de satisfaire à l'obligation d'information qu'à l'égard des partenaires contractuels (et non des autres personnes concernées). Il n'est donc pas recommandé d'intégrer des informations sur la protection des données dans les CGV et il convient d'inclure dans les CGV uniquement un renvoi à la déclaration de protection des données. Des dispositions supplémentaires en matière de protection des données dans les CG se justifient tout au plus si des consentements en matière de protection des données doivent être obtenus, même si les consentements obtenus par le biais de CG sont parfois considérés de manière critique.

47 Les mentions relatives à la protection des données sont interprétées selon la règle de l'inhabituel et de l'ambiguïté, c'est-à-dire qu'il convient d'attirer l'attention sur les éléments inhabituels et que les formulations peu claires sont interprétées au détriment de leur auteur. Il en va de même lorsque les

mentions relatives à la protection des données sont conçues comme une déclaration de protection des données ou comme une information unilatérale, du moins dans la mesure où elles ne sont pas purement informatives et où elles peuvent également avoir des effets juridiques, par exemple en définissant les finalités du traitement ou en servant de base d'information pour d'éventuels consentements. Les informations sur la protection des données intégrées dans les conditions générales sont en outre soumises au contrôle des abus conformément à l'article 8 de la LCD.

C. Mise à disposition

Les informations obligatoires doivent être facilement accessibles aux personnes concernées (article 13 RGPD). Il n'est pas nécessaire que les personnes concernées prennent effectivement connaissance des informations. Ce n'est pas le principe d'accès qui s'applique, mais il suffit que les personnes concernées aient la possibilité d'accéder aux informations sans grand effort. L'accès à l'information peut donc supposer une participation de la personne concernée, notamment parce qu'une transparence de base est déjà garantie par le principe de transparence et que l'obligation d'information ne sert qu'un besoin d'information plus large. 48

Les démarches à entreprendre par la personne concernée pour prendre connaissance doivent cependant être raisonnables. La simple désignation d'une personne de contact ou l'envoi de la déclaration de protection des données uniquement sur demande ne seraient par exemple plus facilement accessibles et donc insuffisants. En revanche, la mise à disposition d'informations sur la protection des données sur un site web est très répandue. L'information sur Internet est suffisante tant qu'il est garanti que les indications relatives à la protection des données sont facilement trouvables sur le site web et accessibles en quelques clics. Dans la pratique, une sous-page spécifique pour la déclaration de protection des données et son lien permanent dans ce que l'on appelle le pied de page, c'est-à-dire dans la zone située en bas d'une page web, ont fait leurs preuves. 49

Une information sur Internet est en principe suffisante, même si le traitement des données a lieu hors ligne. Les personnes concernées sont aujourd'hui habituées à trouver des informations sur la protection des données sur le site web de l'entreprise, et elles le supposent même. Les informations sur la protection des données mises à disposition sur Internet offrent en outre 50

divers avantages, tels qu'une navigation simplifiée et des possibilités étendues de présentation conviviale. Le changement de support vers Internet est donc acceptable dans la plupart des cas. Ce n'est que dans des cas particuliers, par exemple lorsqu'il s'agit d'un traitement délicat de données personnelles sensibles, que l'on s'adresse de manière ciblée à des groupes de personnes plus âgées ou que la consultation d'une page Internet n'est pas raisonnablement exigible en termes de temps en raison de la situation, qu'il peut être nécessaire, à titre exceptionnel, que les personnes concernées puissent accéder à toutes les informations obligatoires selon l'art. 19 LPD sans devoir changer de média.

51 Un moyen utile pour faciliter le changement de support est la présentation de codes QR qui peuvent être scannés avec un téléphone portable et qui mènent à la déclaration de protection des données sur Internet. Ces codes QR sont de plus en plus fréquents dans la pratique (par exemple pour la signalisation de la vidéosurveillance), mais ils ne sont pas juridiquement nécessaires.

52 Une information à plusieurs niveaux est non seulement admissible, mais aussi généralement adaptée aux besoins des personnes concernées : dans un premier temps, seul un aperçu initial du traitement des données est donné, l'information complète n'intervenant qu'à un autre niveau. Le responsable peut en principe définir à sa guise quelles informations doivent être fournies à quel niveau. Il n'existe pas d'"informations de base" qui doivent obligatoirement être fournies au premier niveau.

53 L'établissement d'une version ou d'une date de la déclaration de protection des données peut être utile, mais n'est pas exigé par la loi, pas plus que l'archivage et la mise à disposition de versions antérieures que l'on rencontre parfois dans la pratique.

D. Communication

54 La mise à disposition des informations nécessaires est généralement suffisante et aucune communication active aux personnes concernées n'est nécessaire. De même, les références à la déclaration de protection des données que l'on trouve parfois dans la pratique sur les formulaires, dans les signatures de courriers électroniques, sur le papier à lettres ainsi que dans les conversations téléphoniques et autres communications similaires ne sont pas nécessaires selon le point de vue défendu ici ; même dans les contrats, une référence

explicite à la déclaration de protection des données semble souvent superflue. En cas de vidéosurveillance, un pictogramme bien visible dès l'entrée dans la surface de vente suffit généralement à établir la transparence de base nécessaire, dans la mesure où l'exploitant est reconnaissable au vu des circonstances. Dans de tels cas, on peut raisonnablement attendre des personnes intéressées qu'elles consultent le site web si elles souhaitent s'informer plus en détail sur les traitements de données effectués par l'entreprise concernée. Ils le feront intuitivement et considéreront comme allant de soi que les informations relatives à la protection des données sont disponibles sur le site web.

Une communication active aux personnes concernées n'est nécessaire que si la personne concernée ne sait pas (et ne doit pas savoir) que l'entreprise en question traite des données la concernant. C'est souvent le cas lorsque les données personnelles ne sont pas collectées directement auprès de la personne concernée, mais aussi dans les cas de collecte directe lorsque les données sont collectées à l'insu des personnes concernées (par exemple lorsque les personnes qui pénètrent dans un lieu public sont enregistrées de manière automatisée et que les parcours sont tracés). Dans de tels cas, les personnes concernées doivent être activement informées de la déclaration de protection des données (ce qui peut être fait par exemple en indiquant l'URL ou en mettant à disposition un code QR), sinon elles n'auront même pas l'idée d'aller sur le site web de l'entreprise pour s'informer sur le traitement des données. 55

Pour les mêmes raisons, les modifications apportées à la déclaration de protection des données dans les contrats de longue durée doivent être communiquées aux clients existants, en tout cas lorsque les finalités du traitement sont élargies et que la modification équivaut donc à une nouvelle acquisition. Sinon, les personnes concernées n'auraient aucun indice que la déclaration de protection des données a pu être modifiée et qu'il pourrait donc être indiqué de consulter le site web. Dans la pratique, une telle information est généralement envoyée par e-mail ou par l'affichage de bannières pop-up dans une boutique en ligne ou lors de la connexion à un compte client. Une indication dans un envoi de facture est également envisageable. 56

V. CONSEILS PRATIQUES

A. Procédure et outils

57 L'élaboration de notes d'information sur la protection des données devrait se faire en étroite collaboration avec les responsables commerciaux et techniques des secteurs qui effectuent les traitements de données, car ces fonctions sont les mieux placées pour savoir quelles données sont utilisées, comment et à quelles fins. Souvent, les détenteurs des connaissances pertinentes se trouvent dans les départements de l'entreprise responsables des traitements intensifs de données, comme par exemple les départements marketing, data analytics et RH. Dans la pratique, une procédure participative basée sur des ateliers et impliquant ces détenteurs de connaissances a fait ses preuves. La collecte d'informations par le biais de questionnaires structurés ou d'entretiens est également possible.

58 Le registre des traitements conformément à l'article 12 LPD ou à l'article 30 DSGVO donne également un premier aperçu des processus de traitement et constitue souvent une bonne base pour identifier les traitements de données pertinents. En outre, le registre des traitements contient dans la plupart des cas des informations qui peuvent être utilisées pour préparer les données obligatoires, comme par exemple des indications sur les types de données traitées, le but du traitement et les (catégories de) destinataires.

59 Dans la pratique, il existe différents outils qui aident les entreprises à rédiger des avis de protection des données, notamment des modèles de déclarations de protection des données qui peuvent être utilisés comme point de départ et adaptés à leurs propres besoins. On peut citer par exemple les offres suivantes, largement utilisées :

- Modèle de déclaration générale de protection des données, qui couvre de nombreuses activités de traitement standard et s'aligne aussi bien sur la LPD suisse que sur le DSGVO, élaboré par deux cabinets d'avocats suisses renommés et disponible sur https://dsat.ch/download/ (gratuit) ;
- Générateur de protection des données de Datenschutzpartner pour l'élaboration d'une déclaration de protection des données pour les sites web avec des formulations types pour de nombreux outils web courants,

disponible sur https://www.datenschutzpartner.ch/angebot-datenschutz-generator/ (payant) ;

- Modèle de déclaration de protection des données du professeur d'université allemand Thomas Hoeren pour les exploitants de sites web, disponible sur https://www.itm.nrw/wp-content/uploads/Musterdatenschutzerkaerung-nach-der-DSGVO_Stand_September_2022-1.docx (gratuit).

Selon la conception courante de la gouvernance, la validation du contenu de la déclaration de protection des données devrait être effectuée par les organes de direction responsables des traitements de données, par exemple la direction. Le rôle du délégué à la protection des données ou du conseiller à la protection des données, ainsi que d'autres fonctions juridiques et de conformité, devrait se limiter à une fonction de coordination et de conseil, notamment au regard du régime des sanctions. 60

B. Préparation et conception

L'ordonnance d'exécution de la loi sur la protection des données exige une information précise et compréhensible (art. 13 OLPD). Il ne s'agit toutefois guère de critères justiciables (ni même punissables) et, dans la pratique, ce sont toujours les textes coulants d'apparence juridique qui dominent. De nombreuses entreprises sont manifestement d'avis qu'il est difficile d'obtenir un positionnement positif avec la protection des données et qu'il ne vaut donc pas la peine d'investir des ressources importantes dans une préparation conviviale des informations sur la protection des données. 61

Le fait que le droit de la protection des données incite à considérer les informations relatives à la protection des données en premier lieu comme un instrument défensif et non comme une communication centrée sur le client n'aide pas non plus : d'une part, les entreprises s'efforcent, compte tenu du renforcement des moyens et des sanctions en matière de droit de surveillance, d'intégrer des formulations ouvertes et des clauses générales et de se protéger ainsi contre le reproche d'informations inexactes ou incomplètes sur la protection des données. D'autre part, les entreprises ne veulent pas se priver d'une marge de manœuvre eu égard au principe de finalité et ne mentionner dans les avis de protection des données que les futures finalités possibles du traitement. 62

63 Malgré cette structure d'incitation malheureuse, il existe dans la pratique différentes approches prometteuses pour rendre les informations sur la protection des données plus faciles à lire et mieux adaptées aux besoins des destinataires :

- Une information à plusieurs niveaux ("layered approach"), dans laquelle les principaux aspects pertinents du traitement des données sont d'abord présentés de manière claire et les informations détaillées ne sont fournies qu'à un niveau ultérieur. Une information à plusieurs niveaux comprend également des textes dépliants et des exemples tangibles pour illustrer les explications parfois plutôt abstraites.
- Utilisation de pictogrammes de protection des données qui permettent aux personnes concernées de se faire rapidement une première idée de la manière dont leurs données sont traitées. Les pictogrammes standardisés publiés par l'association Privacy Icons, qui permettent de reconnaître en un coup d'œil certains aspects typiquement pertinents pour les personnes concernées et qui sont déjà utilisés par différentes entreprises suisses de premier plan, en sont un exemple.
- Tableaux de bord de protection des données, qui offrent un accès facile et permettent aux personnes concernées de définir elles-mêmes des priorités et d'obtenir des informations ciblées sur les points essentiels.
- Des vidéos explicatives qui introduisent les personnes concernées au sujet et leur présentent les contenus les plus importants de manière facilement compréhensible.
- Des éléments de gamification qui permettent aux personnes concernées de comprendre les aspects centraux du traitement des données de manière ludique.

64 De telles approches de "Legal Design" peuvent considérablement améliorer l'accessibilité et la lisibilité des informations sur la protection des données et doivent donc être saluées dans le sens d'un traitement transparent des données. Il n'existe toutefois pas d'obligation légale de recourir à de telles approches conviviales, même sous le régime du RGPD.

VI. APPLICATION ET CONSÉQUENCES JURIDIQUES

A. Droit administratif

Si les personnes concernées n'ont pas été informées correctement du traitement des données, le PFPDT peut ouvrir une enquête et ordonner la mise en place d'une information conforme à la loi en tant que mesure administrative (art. 51 al. 3 let. c LPD). Le PFPDT peut agir d'office ou sur dénonciation. 65

L'interdiction du traitement des données ou l'ordre d'une adaptation par le PFPDT est également envisageable en principe (art. 51 al. 1 LPD). Dans la plupart des cas, une mesure aussi radicale ne devrait toutefois pas être proportionnelle au seul fait que l'information n'a pas été effectuée dans les règles. 66

B. Droit pénal

L'obligation d'informer fait partie des obligations de la LPD qui sont assorties de sanctions pénales. Quiconque omet de fournir l'information prévue à l'art. 19 LPD ou fournit des informations fausses ou incomplètes peut être puni d'une amende pouvant atteindre 250 000 CHF (art. 60 al. 1 LPD). L'obligation d'informer est une obligation à fort impact externe et la menace de sanction a donc le potentiel d'être utilisée de manière ciblée comme moyen de pression contre une entreprise, les employés ou les décideurs responsables. 67

Certains se demandent si l'art. 19 LPD satisfait au principe de précision du droit pénal de l'art. 1 CP et si une violation de l'obligation d'informer peut donc être sanctionnée par le droit pénal. En tout état de cause, il faut exiger qu'en ce qui concerne l'exhaustivité, on se base exclusivement sur les informations obligatoires selon l'art. 19 al. 2-4 LPD. Les éventuelles informations supplémentaires à fournir en vertu de la clause générale de l'art. 19 al. 2 ne doivent pas être prises en compte. 68

En principe, ce n'est pas l'entreprise qui est punissable, mais la ou les personnes physiques responsables de la violation (art. 64 al. 1 LPD en relation avec l'art. 6 DPA). Il peut s'agir de dirigeants qui ont l'obligation légale d'assurer la conformité en matière de protection des données ou de personnes qui ont la responsabilité opérationnelle des processus au sein de l'entreprise et qui sont habilitées à prendre des décisions sur les questions 69

relatives à l'obligation d'informer. En revanche, celui qui se contente d'apporter son soutien est un complice et, en tant que tel, reste impuni. Dans certains cas, il est également possible de ne pas punir la personne physique et d'infliger une amende à l'entreprise. C'est le cas lorsque l'identification de la personne fautive nécessiterait des mesures d'enquête disproportionnées et qu'une amende de 50 000 CHF au maximum peut être envisagée (art. 64 al. 2 LPD en relation avec l'art. 7 DPA).

70 Seuls les actes intentionnels sont punis. Le dol éventuel, c'est-à-dire l'acceptation de l'acte, en fait également partie. En revanche, la commission par négligence n'est pas punissable. Celui qui oublie une indication, formule quelque chose de manière imprécise ou omet délibérément quelque chose parce qu'il estime que cela ne fait pas partie des indications obligatoires, n'agit pas intentionnellement et reste impuni. Afin d'exclure autant que possible tout acte intentionnel, les décisions prises dans le cadre de l'obligation d'information devraient être documentées de manière compréhensible, par exemple en indiquant les raisons pour lesquelles on a renoncé à une information ou omis une donnée.

71 L'art. 60 al. 1 LPD est un délit poursuivi sur plainte. Une violation de l'obligation d'informer n'est donc poursuivie que sur plainte, et non d'office. Toute personne concernée peut déposer une plainte pénale, mais pas le PFPDT.

C. Droit civil

72 La violation de l'art. 19 LPD, en tant que disposition de droit public, n'entraîne pas en soi d'atteinte à la personnalité et ne peut donc pas être invoquée par les personnes concernées par voie d'action.

73 Les personnes concernées peuvent toutefois, le cas échéant, faire valoir une violation du principe général de transparence en tant que principe de traitement et porter plainte sur cette base auprès du tribunal civil compétent.

D. DSGVO

74 Dans le champ d'application du RGPD, les violations de l'obligation d'information peuvent être sanctionnées par des amendes allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial total (art. 83 al. 5 RGPD). Il s'agit du cadre d'amende le plus élevé des deux prévus par le RGPD.

Contrairement à ce qui se passe sous la LPD, l'amende du RGPD est dirigée en premier lieu contre l'entreprise et non contre les personnes physiques agissant pour le compte de l'entreprise.

Sous le RGPD, une violation de l'obligation d'information peut également, le cas échéant, faire disparaître la base juridique nécessaire au traitement et rendre ainsi le traitement des données illégal. 75

VII. CRITIQUE DE LA NORME

L'obligation d'information est l'expression d'une conception fondamentale du droit de la protection des données basée sur l'autodétermination en matière d'information. L'idée de base est que les personnes concernées s'informent sur un traitement de données et prennent sur cette base une décision informée, à savoir si elles sont d'accord avec le traitement correspondant de leurs données et si elles souhaitent exercer l'un des droits de protection des données qui leur sont accordés. 76

Dans le monde numérisé et basé sur les données d'aujourd'hui, les limites de cette compréhension de base sont de plus en plus visibles. Le traitement des données personnelles concerne aujourd'hui tous les domaines de la vie et les personnes concernées sont sans cesse confrontées à des informations complètes sur la protection des données, pour lesquelles elles n'ont souvent pas le temps ni les connaissances techniques nécessaires. Il en résulte une surcharge d'informations ("information overload") et un surmenage constant. Pour de nombreuses personnes, il est économiquement rationnel de s'épargner cet effort et de rester non informées. 77

La question se pose donc de savoir si l'obligation d'informer atteint encore l'objectif qui lui est assigné et si elle justifie les dépenses qui lui sont liées. Son fondement conceptuel remonte aux débuts de la protection des données, lorsque le traitement des données était encore plus simple. Depuis lors, notre monde a considérablement évolué sur le plan technologique et les traitements de données modernes sont souvent complexes. C'est un peu comme si l'on exigeait d'une compagnie aérienne qu'elle publie des informations techniques complètes et qu'elle attende des passagers potentiels qu'ils se fassent ainsi une idée de l'aptitude de l'avion à voler. Ici comme ailleurs, ce n'est ni réaliste ni efficace. Il vaudrait la peine de développer de nouvelles approches de la 78

protection des données qui ne soient pas fondées sur une transparence de façade.

BIBLIOGRAPHIE

Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01, adopted on 29 November 2017, as last revised and adopted on 11 April 2018, abrufbar unter https://ec.europa.eu/newsroom/article29/items/622227/en, besucht am 25.5.2023.

Bäcker Matthias, Kommentierung zu Art. 13 und 14 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung, 3. Aufl., München 2020.

Bergt Matthias, Kommentierung zu Art. 83 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung, 3. Aufl., München 2020.

Bieri Adrian/Powell Julian, Informationspflicht nach dem totalrevidierten Datenschutzgesetz, AJP 2020, S. 1533 ff.

Bühlmann Lukas/Lagler Marion, Informationspflichten und Auskunftsrecht nach dem neuen Datenschutzrecht, SZW 2021, S. 16 ff.

Bühlmann Lukas/Schüepp Michael, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, in: Jusletter 15. März 2021.

Ettlinger Claudius, Die Informationspflicht gemäss neuem Datenschutzgesetz, in Jusletter IT 16. Dezember 2021.

Franck Lorenz, Kommentierung zu Art. 13 DSGVO, in: Gola Peter/Heckmann Dirk (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl., München 2022.

Kohlmeier Astrid/Klemola Meera, Das Legal Design Buch, Hürth 2021.

Maric Antonio, Legal Design im Kontext von Datenschutzerklärungen, in: Jusletter IT 20. Juli 2023.

Paal Boris/Hennemann Moritz, Kommentierung zu Art. 13 DSGVO, in: Paal Boris/Pauly Daniel (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl., München 2021.

Pärli Kurt/Flück Nathalie, Kommentierung zu Art. 19 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Aufl., Bern 2023.

Rampini Corrado/Fuchs Philippe, Kommentierung zu Art. 14 DSG, in: Maurer-Lambrou Urs/Blechta Gabor P. (Hrsg.), Basler Kommentar zum Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014.

Rosenthal David, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020.

Rosenthal David/Gubler Seraina, Die Strafbestimmungen des neuen DSG, SZW 2021, S. 52 ff.

Schweikard Christine/Vasella David, Datenschutzerklärungen und AGB, digma 2020, S. 88 ff.

Steiner Thomas, Zwischen Autonomie und Angleichung: Eine Analyse zur Anwendung des neuen DSG im Lichte der DSGVO, in: Widmer Michael (Hrsg.), Datenschutz: Rechtliche Schnittstellen, Zürich 2023, S. 51 ff.

Thouvenin Florent, Datenschutz auf der Intensivstation, digma 2019, S. 206 ff. (zit. Intensivstation).

Thouvenin Florent, Informationelle Selbstbestimmung: Intuition, Illusion, Implosion (noch nicht erschienen) (zit. Informationelle Selbstbestimmung).

Thouvenin Florent/Glatthaar Matthias/Hotz Juliette/Ettlinger Claudius/Tschudin Michael, Privacy Icons: Transparenz auf einen Blick, in: Jusletter 30. November 2020.

Vasella David, Zu den Anforderungen an die Erfüllung der Informationspflicht nach dem revDSG, datenrecht.ch, 28. Oktober 2022, abrufbar unter https://datenrecht.ch/zu-den-anforderungen-an-die-erfuellung-der-informationspflicht-nach-dem-revdsg, besucht am 25.5.2023 (zit. Informationspflicht).

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom

15.7.2017, BBl 2017 S. 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 25.5.2023 (zit. Botschaft DSG).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 18 LPD

Un commentaire de Apollo Dauag

PROPOSITION DE CITATION

Apollo Dauag, Commentaire de l'art. 18 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Dauag, art. 18 LPD N. XXX.

Art. 18 Publication de données personnelles sous forme électronique

La publication de données personnelles au moyen de services d'information et de communication automatisés afin d'informer le public n'est pas assimilée à une communication à l'étranger, même si ces données peuvent être consultées depuis l'étranger.

TABLE DES MATIÈRES

En bref 269
I. Définition et systématique 269
II. Intention du législateur 270
III. Conditions 270
A. Objectif : informer le public par un accès général 270
B. Moyens : services d'information et de communication automatisés 271
IV. Conséquences juridiques 272
V. Importance dans la pratique 272
Bibliographie 273
Matériaux 273

EN BREF

Quiconque rend légalement accessibles sur Internet des données personnelles à des fins d'information du public (et donc à un cercle indéterminé de personnes) n'est pas tenu de satisfaire aux exigences relatives à la communication à l'étranger.

I. DÉFINITION ET SYSTÉMATIQUE

L'art. 18 définit les conditions dans lesquelles la **mise à disposition générale** de données personnelles sur Internet n'est pas considérée comme une communication à l'étranger. 1

La publication de données personnelles sous forme électronique conformément à l'art. 18 conclut la troisième section « Communication de données personnelles à l'étranger ». Outre le principe énoncé à l'art. 16 et les exceptions prévues à l'art. 17, l'art. 18 décrit les conditions dans lesquelles les dispositions susmentionnées relatives à la communication à l'étranger ne sont pas applicables. Si ces conditions sont remplies, l'**inapplicabilité des art. 16 et 17 entre en vigueur en tant que conséquence juridique**. 2

Il s'agit d'une **présomption légale**, qui est irréfutable : si la communication remplit les conditions énoncées à l'art. 18 (base de la fiction), elle est considérée comme ne remplissant pas les conditions requises pour la communication à l'étranger selon les art. 16 et 17 (conséquence de la fiction). 3

Cette présomption n'affecte pas le fait qu'il s'agit d'une communication. Il s'agit donc d'un traitement. Les principes généraux **(de traitement)** énoncés aux art. 6 ss doivent être respectés en tout temps. 4

Dans le cadre de la **révision totale** de la LPD, la disposition relative à la « communication transfrontalière » (art. 6 aLPD) a été transférée dans une section distincte intitulée « Communication de données personnelles à l'étranger ». La licéité de la communication dans les conditions qui y sont énoncées (anciennement art. 6, al. 1 et al. 2, let. a, aLPD) est désormais régie par le principe énoncé à l'art. 16, et les exceptions (anciennement art. 6, al. 2, let. b à g, aLPD) sont désormais énumérées à l'art. 17. 5

6 La « publication sous forme électronique » (anciennement art. 5 OPD) a été transférée à l'art. 18 avec trois précisions rédactionnelles. Dans le projet et dans le message, elle était référencée à l'art. 15, mais elle ne figurait pas encore dans l'avant-projet. Par ailleurs, cette disposition n'a pas retenu l'attention au cours du **processus législatif**.

7 La conséquence juridique de l'art. 18 est exclusive, raison pour laquelle la publication sur Internet ne constitue **pas une exception** au sens de l'art. 17, al. 1, let. a à f, et n'y figure donc pas.

II. INTENTION DU LÉGISLATEUR

8 Internet ne connaît pas de frontières nationales. La publication de données personnelles sur Internet a inévitablement pour conséquence leur **accessibilité mondiale, y** compris dans les pays ne disposant pas d'une protection adéquate des données. Le cercle des destinataires étant mondial et indéterminé, la personne responsable en Suisse ne peut remplir les conditions requises pour une communication licite à l'étranger. Le législateur accepte le risque d'atteinte à la personnalité qui en découle, le considérant comme une « concession à la numérisation croissante ».

9 L'accès dans les pays ne disposant pas d'une protection adéquate des données peut être rendu plus difficile par des **blocages nationaux** (blocages IP, appelés « géoblocage »), mais il ne peut être empêché de manière définitive.

III. CONDITIONS

10 Deux conditions doivent être remplies **de manière cumulative**, sinon la mise à disposition générale est considérée comme une communication à l'étranger.

A. Objectif : informer le public par un accès général

11 La **publication** doit (déjà par définition) avoir pour objectif d'informer le public en créant un accès général.

12 Aucune exigence supplémentaire ne peut être imposée au **besoin d'information** : celui-ci est couvert si le traitement des données personnelles en vue de leur publication sur Internet est licite, en particulier proportionné et conforme à l'objectif poursuivi.

Seul un cercle de destinataires dont le lieu de séjour ne peut être déterminé peut être considéré comme **le public** : si le lieu de séjour à l'étranger peut être déterminé ou si l'accès peut être contrôlé (par exemple par des blocages par pays, voir ci-dessus N. 9), il serait raisonnable d'exiger de la personne responsable qu'elle remplisse les conditions pour une communication licite à l'étranger. Une restriction géographique est toutefois en contradiction avec l'accès général. 13

Un **accès général** signifie que l'information est en principe accessible sans restriction. L'accès ne doit toutefois pas être gratuit ou accordé sans inscription. Une inscription ne change rien au risque : en raison de l'accessibilité mondiale, même les destinataires inscrits provenant d'un pays offrant une protection adéquate des données peuvent se rendre dans un pays ne disposant pas d'une protection adéquate et consulter les données personnelles publiées à partir de là. 14

B. Moyens : services d'information et de communication automatisés

L'art. 18 mentionne, dans une formulation neutre sur le plan technologique, les « services d'information et de communication automatisés ». Les commentaires font référence à « Internet ou aux services basés sur Internet » et aux « sites web, blogs ou services d'information tels que Twitter, etc. ». La « publication via des applications, des services de streaming, des portails de vidéo à la demande et des services comparables » en fait également partie. Sont concernées **toutes les formes de publication sous forme électronique** qui permettent un accès mondial. Cela vaut également pour les newsletters électroniques. 15

Selon l'avis présent, l'**emplacement du serveur** n'est pas pertinent : premièrement, le risque d'accessibilité depuis des pays ne disposant pas d'une protection adéquate des données (sans blocage par pays, voir ci-dessus N. 9) existe indépendamment de l'emplacement du serveur. Deuxièmement, même en cas de stockage initial en Suisse, la reproduction sur des serveurs situés à l'étranger ne peut être empêchée. Troisièmement, la LPD s'applique également aux situations qui ont des répercussions en Suisse, même si elles sont initiées à l'étranger. La distinction entre les serveurs situés en Suisse et les serveurs situés à l'étranger ne semble pas pertinente dans ce cas. 16

IV. CONSÉQUENCES JURIDIQUES

17 Si les **conditions sont remplies**, la publication sous forme électronique n'est pas considérée comme une communication à l'étranger au sens de l'art. 16 LPD. Les exceptions prévues à l'art. 17 LPD ne doivent pas être examinées.

18 Si les **conditions ne sont pas remplies**, la publication sous forme électronique est considérée comme une communication à l'étranger au sens de l'art. 16 LPD. Des exceptions au sens de l'art. 17 LPD peuvent s'appliquer. Une violation de l'art. 16 LPD (communication sans protection adéquate) est considérée comme un manquement aux obligations de diligence et peut entraîner les conséquences pénales prévues à l'art. 61, let. a, LPD.

V. IMPORTANCE DANS LA PRATIQUE

19 Dans les faits, la présomption légale de l'art. 18 constitue la **base de la publication de données personnelles sur Internet** et permet ainsi la participation à la communication médiatique moderne : les obstacles applicables à la communication à l'étranger ne peuvent généralement pas être surmontés par les personnes responsables sans efforts déraisonnables.

20 Sur le plan juridique, la suppression des conditions requises pour une communication autorisée à l'étranger ne constitue qu'un **privilège spécifique accordé à la personne responsable en Suisse** : la publication de données personnelles sur Internet doit à tout moment remplir les conditions requises pour le traitement et la communication. Les publications qui sont contraires à leur finalité ou qui enfreignent de toute autre manière les principes de traitement ne peuvent pas bénéficier d'un privilège.

21 Conformément à l'art. 3, les dispositions de la LPD s'appliquent en principe également au traitement effectué à l'étranger (des données personnelles publiées sur Internet). Même si le législateur accepte le risque d'atteintes à la personnalité lié à l'accessibilité mondiale, le libellé de l'art. 18 ne contient **aucun privilège général pour la personne responsable à l'étranger**. Les autres communications (suivant la publication sur Internet) ne sont donc pas soumises aux conditions relatives à la communication à l'étranger, mais doivent également remplir les conditions relatives au traitement et à la communication.

Des **conditions supplémentaires** s'appliquent aux organes fédéraux : outre l'exigence d'une base légale pour la publication de ces données (par exemple la loi sur la transparence), l'art. 36, al. 5, prévoit l'obligation de supprimer les données concernées du « service automatisé d'information et de communication » dès qu'il n'y a plus d'intérêt public à leur accès public. 22

Pour autant que l'on sache, cette disposition (ni sous la forme de l'art. 5a OPD ni sous celle de l'art. 18) n'a encore fait l'objet d'aucun arrêt publié. 23

BIBLIOGRAPHIE

Jungo Alexandra, Zürcher Kommentar zum Zivilgesetzbuch, Art. 8 ZGB, 3. Aufl., Zürich 2018.

Dal Molin Luca, Kommentierung zu Art. 18 DSG, in: Blechta Gabor P./Vasella David (Hrsg.), Datenschutzgesetz / Öffentlichkeitsgesetz, Basler Kommentar, 4. Aufl., Basel 2024.

Kunz Christian, Kommentierung zu Art. 18 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023.

Husi-Stämpfli Sandra, Kommentierung zu Art. 18 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Auflage, Bern 2023.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 S. 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 23.12.2025.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 20 LPD

Un commentaire de Matthias Glatthaar / Annika Schröder

PROPOSITION DE CITATION

Matthias Glatthaar/Annika Schröder, Kommentierung zu Art. 20 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Glatthaar/Schröder, N. XXX zu Art. 20 DSG.

Art. 20 Exceptions au devoir d'informer et restrictions

[1] Le responsable du traitement est délié du devoir d'information au sens de l'art. 19 si l'une des conditions suivantes est remplie:

a. la personne concernée dispose déjà des informations correspondantes;

b. le traitement des données personnelles est prévu par la loi;

c. le responsable du traitement est une personne privée et il est lié par une obligation légale de garder le secret;d.les conditions de l'art. 27 sont remplies.

[2] Lorsque les données personnelles ne sont pas collectées auprès de la personne concernée, le devoir d'information ne s'applique pas non plus dans les cas suivants:

a. l'information est impossible à donner;

b. elle nécessite des efforts disproportionnés.

[3] Le responsable du traitement peut restreindre ou différer la communication des informations, ou y renoncer, si l'une des conditions suivantes est remplie:

a. les intérêts prépondérants d'un tiers l'exigent;

b. l'information empêche le traitement d'atteindre son but;

c. lorsque le responsable du traitement est une personne privée et que les conditions suivantes sont remplies:

ses intérêts prépondérants l'exigent,
il ne communique pas les données à un tiers;

d. lorsque le responsable du traitement est un organe fédéral:

si un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Suisse, l'exige, ou
si la communication des informations est susceptible de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative.

[4] Les entreprises appartenant au même groupe ne sont pas considérées comme des tiers au sens de l'al. 3, let. c, ch. 2.

TABLE DES MATIÈRES

En bref ... 278
I. Généralités ... 278
A. But de la norme ... 278
B. Historique ... 278
C. Systématique ... 279
D. Notes d'interprétation ... 279
II. Exceptions (al. 1 et 2) ... 279
A. Généralités ... 279
B. Connaissance préalable des informations (al. 1 let. a) ... 280
C. Traitements prescrits par la loi (al. 1 let. b) ... 281
D. Obligations légales de garder le secret (al. 1 let. c) ... 283
E. Privilège des médias (al. 1 let. d) ... 284
F. Impossibilité d'informer (al. 2 let. a) ... 284
G. Effort disproportionné (al. 2 let. b) ... 285
III. Restrictions ... 286
A. Généralités ... 286
B. Intérêts prépondérants de tiers (al. 3 let. a) ... 287
C. Détournement de la finalité (al. 3 let. b) ... 287
D. Intérêts prépondérants du responsable du traitement (al. 3 let. c) ... 288
E. Intérêts publics prépondérants (al. 3 let. d ch. 1) ... 289
F. Mise en danger de la procédure (al. 3 let. d ch. 2) ... 290
Bibliographie ... 290
Matériaux ... 291

EN BREF

L'art. 20 LPD contient une série d'allègements de l'obligation d'informer : d'une part, des exceptions pour lesquelles l'obligation d'informer est entièrement supprimée, par exemple lorsque la personne concernée dispose déjà des informations correspondantes ou que le traitement est effectué en exécution d'une obligation légale. D'autre part, la disposition contient des restrictions dans lesquelles l'obligation d'informer subsiste, mais où l'information peut être limitée, différée ou suspendue dans un cas particulier, par exemple lorsqu'une information ferait échouer le but du traitement ou lorsque des intérêts prépondérants s'opposent à une information. L'article 20 LPD sert de correctif à une obligation d'information globale et veille à ce que l'obligation d'information ne devienne pas une charge excessive pour les responsables et reste limitée aux cas où elle est nécessaire pour la protection des personnes concernées.

I. GÉNÉRALITÉS

A. But de la norme

1 L'article 20 LPD prévoit une série d'allègements de l'obligation d'information. Cette disposition vise à garantir que l'obligation d'informer s'applique là où elle est nécessaire pour un traitement transparent des données et pour la protection des personnes concernées, et qu'elle ne s'applique pas dans les cas où elle serait superflue ou disproportionnée. Elle est l'expression de la volonté du législateur de trouver un équilibre entre les intérêts en présence et de créer des allègements ciblés. En comparaison avec le RGPD, la liste des exceptions de l'article 20 LPD est assez vaste.

B. Historique

2 L'art. 20 LPD regroupe les exceptions et restrictions réparties dans différents articles de l'ancien droit (art. 9, art. 14 al. 4 et 5, art. 18a et art. 18b aDSG) et les complète de manière modérée. L'art. 20 LPD n'a pas été contesté dans son principe lors des débats parlementaires, une partie du Parlement estimant toutefois que l'exception en cas de charges disproportionnées allait trop loin.

Le privilège de groupe selon l'art. 20 al. 4 LPD a été ajouté lors des débats parlementaires.

C. Systématique

La disposition distingue d'une part les exceptions, dans lesquelles l'obligation d'informer est totalement supprimée, et d'autre part les restrictions, dans lesquelles l'obligation d'informer subsiste en principe, mais où le responsable peut limiter, différer ou suspendre l'information dans un cas particulier. L'art. 20 LPD s'applique aussi bien aux responsables privés qu'aux organes fédéraux, mais fait parfois la distinction entre les particuliers et les organes fédéraux en ce qui concerne les différentes exceptions et restrictions. 3

Les exceptions et restrictions contenues dans l'article 20 LPD sont exhaustives. Une violation du devoir d'information ne peut pas non plus être justifiée en vertu de l'article 31 LPD, car le devoir d'information de l'article 19 LPD est de nature publique et non une concrétisation des principes de traitement selon l'article 6 LPD. 4

D. Notes d'interprétation

Les exceptions prévues à l'art. 20 LPD vont parfois assez loin et comprennent également des cas dans lesquels le traitement des données est certes reconnaissable (base légale, al. 1 let. b) ou la confidentialité des données personnelles traitées est garantie (obligation légale de garder le secret, al. 1 let. c), mais où le besoin d'information de la personne concernée, protégé par le devoir d'information, n'est pas satisfait. Il convient donc d'interpréter les faits constitutifs de manière plutôt restrictive et de les mettre en conformité avec l'objectif du devoir d'information. 5

II. EXCEPTIONS (AL. 1 ET 2)

A. Généralités

L'art. 20 LPD définit aux al. 1 et 2 un total de six situations dans lesquelles le responsable est totalement dispensé de l'obligation d'informer les personnes concernées. Dans ces situations, la personne concernée ne doit pas non plus être informée de l'applicabilité de l'exception elle-même. Il ne lui reste qu'à exercer son droit d'accès, sachant que la personne concernée n'a souvent 6

aucune raison de demander des informations sur ses données si elle n'est pas au courant de leur traitement et que le droit d'accès est lui-même soumis à des restrictions similaires (article 26 LPD).

B. Connaissance préalable des informations (al. 1 let. a)

7 L'obligation d'informer ne s'applique pas si la personne concernée dispose déjà des informations en question. Les personnes concernées ne doivent pas être informées de choses qu'elles connaissent déjà, ce qui est évident. Une exception comparable à l'obligation d'information se trouve également dans le DSGVO. Dans l'ancienne LPD, l'exception était encore un peu plus restreinte et se référait au processus d'information et non à l'existence de l'information en soi (art. 14, al. 4, et art. 18a, al. 3, aDSG : "si la personne concernée a déjà été informée").

8 Cette exception signifie tout d'abord que les personnes concernées ne doivent pas être informées à nouveau lors de collectes de données ultérieures si elles ont déjà été informées à l'occasion d'une collecte précédente. La condition est que les collectes soient matériellement liées et qu'elles ne soient pas trop éloignées dans le temps. On peut penser par exemple à des commandes individuelles dans une boutique en ligne, si l'information a déjà été donnée lors de la création du compte, ou à des traitements médicaux ultérieurs, si une information a déjà été donnée dans le cadre du premier traitement.

9 Un autre cas d'application de l'exception est celui où la personne concernée a consenti à un traitement de données, car un consentement valable selon l'art. 6 al. 6 LPD présuppose par définition une information suffisante. Les informations exigées par l'art. 19 LPD peuvent donc également être communiquées au moyen d'une déclaration de consentement.

10 Selon le message, les situations dans lesquelles la personne concernée transmet ses données personnelles au responsable du traitement sans l'intervention de ce dernier doivent également tomber sous le coup de l'exception. Cela va assez loin, car la connaissance de la personne concernée se limite ici au fait de la collecte. Il existe cependant un intérêt légitime à être informé sur d'autres circonstances du traitement des données, par exemple, dans l'exemple cité par le message d'une candidature à un emploi, si (et pendant combien de temps) les documents de candidature sont également

conservés pour de futurs emplois, à qui ils sont éventuellement transmis et où ils sont stockés.

Enfin, les cas dans lesquels il est établi que la personne concernée a renoncé aux informations visées à l'art. 19 LPD ou qu'elle n'a pas d'intérêt à être informée relèvent également de l'exception. Cela doit toutefois se limiter à des cas clairs et ne peut en tout cas pas être supposé dès lors que la personne concernée a rendu ses données personnelles accessibles au public (p. ex. sur un profil de média social). 11

C. Traitements prescrits par la loi (al. 1 let. b)

L'obligation d'informer ne s'applique pas non plus lorsque le traitement des données est prévu par la loi. La réflexion est que dans ces cas, le législateur a déjà défini les points clés du traitement des données en mettant en balance les différents intérêts en jeu et que l'information des personnes concernées n'offrirait donc pas de protection supplémentaire importante. Le RGPD contient une exception similaire, mais limitée au cas d'une collecte indirecte et liée à la condition que la norme légale régisse expressément le traitement des données et prévoie des mesures appropriées pour protéger les intérêts légitimes des personnes concernées. 12

Pour bénéficier de l'exception, soit le traitement des données lui-même doit être prescrit par la loi, soit le traitement des données doit être indispensable à l'exécution d'une obligation légale. En ce qui concerne les responsables privés, une base suffisamment précise dans une loi au sens matériel suffit. Pour les organes fédéraux, le critère de l'article 34 LPD s'applique et une loi au sens formel est nécessaire lorsqu'il s'agit du traitement de données personnelles sensibles, du profilage ou d'une atteinte grave aux droits fondamentaux. 13

Les traitements de données exigés par la loi sont nombreux dans l'ordre juridique et l'exception a donc une grande importance pratique. On peut citer comme exemple : La tenue du registre des actions ainsi que la convocation et la tenue de l'assemblée générale dans le cas des sociétés anonymes ; les obligations d'identification et la détermination de l'ayant droit économique dans le cadre de la lutte contre le blanchiment d'argent ; les obligations de déclaration en matière de santé publique en rapport avec les maladies transmissibles ; le paiement du salaire et l'établissement de certificats par 14

l'employeur dans le cadre des rapports de travail ; les obligations de décompte en matière de fiscalité et d'assurances sociales.

15 L'exception peut également être invoquée lorsque le responsable a lui-même provoqué l'obligation légale, par exemple les obligations d'identification prévues par le droit du blanchiment d'argent en initiant la relation commerciale ou les traitements indiqués par le droit du travail en concluant le contrat de travail.

16 Si le traitement des données va au-delà de l'obligation légale (par exemple, si les données collectées dans le cadre de la lutte contre une pandémie doivent également être utilisées à des fins de marketing), l'exception ne s'applique pas et il convient d'informer. De même, les traitements de données qui ne se déroulent qu'à un niveau général dans un cadre défini par la loi, mais qui sont effectués volontairement, ne sont pas exemptés de l'obligation d'informer. Dans le domaine des collaborateurs, une information est donc régulièrement nécessaire, par exemple sous la forme d'une déclaration de protection des données des collaborateurs. Même si le cadre fixé par l'article 328b CO n'est pas dépassé, les traitements de données dans le domaine des collaborateurs vont généralement au-delà de ce qui est effectivement prescrit par la loi.

17 Dans le cas des organes fédéraux, le traitement de données personnelles en vertu de l'article 34 LPD repose dans la plupart des cas sur une base légale. Les dispositions légales correspondantes sont toutefois souvent formulées de manière assez générale et ne peuvent souvent pas garantir à elles seules la transparence visée par l'obligation d'informer. De l'avis correct, l'al. 1 let. b ne dispense donc les organes fédéraux de l'obligation d'informer que si le traitement des données est expressément prévu par la loi et décrit de manière suffisamment précise. Les art. 69f et 69g LRTV en relation avec l'art. 6 de la loi sur la radio et la télévision peuvent servir d'exemple de traitement de données décrit de manière précise dans la loi. Les art. 67 et 67a ORTV peuvent être cités. En revanche, exempter les organes fédéraux de l'obligation d'informer sur la base de l'al. 1 let. b pour chaque traitement fondé sur la loi mettrait excessivement à mal la transparence des traitements de données effectués par l'Etat fédéral et rendrait largement obsolète l'applicabilité de l'art. 19 LPD aux organes fédéraux en tant que tels ainsi que les restrictions prévues à l'art. 20 al. 3 LPD spécialement pour les organes fédéraux.

D. Obligations légales de garder le secret (al. 1 let. c)

Les personnes physiques soumises à une obligation légale de garder le secret sont exemptées de l'obligation d'informer. On pense notamment aux groupes professionnels mentionnés à l'art. 321 CP, comme les ecclésiastiques, les avocats, les pharmaciens et les médecins. L'exception ne vaut que (mais tout de même) pour le domaine d'activité protégé par le secret, mais pas pour d'autres activités éventuelles d'une personne appartenant à ces groupes professionnels. Ainsi, si l'avocate ou le médecin de famille traite par exemple des données personnelles pour l'acquisition de clients (invitation à des manifestations ou envoi d'informations à la clientèle) ou pour la mise à disposition de son site web, elle est soumise à l'obligation d'informer pour ces activités. 18

La personne morale qui emploie éventuellement la personne tenue au secret ou pour laquelle elle travaille n'est pas concernée par l'exception. Une corporation d'avocats ou un centre médical doit donc également informer sur les traitements de données effectués dans le domaine d'activité protégé par le secret (p. ex. sur les prestations d'avocats dans le domaine du monopole ou sur les prestations de santé). L'exception ne s'applique pas non plus aux organes fédéraux. 19

Selon le message, l'exception prévue à l'al. 1 let. c permet de régler un éventuel conflit de normes entre l'obligation de garder le secret et l'obligation d'informer, ce qui n'est toutefois pas convaincant : même dans le domaine d'activité protégé par le secret, la mise à disposition des informations exigées à l'art. 19 LPD ne révélerait aucune donnée personnelle et donc aucun secret. Un avocat pourrait par exemple sans autre informer de manière générale que les données personnelles contenues dans un acte juridique seront transmises à la partie adverse et au tribunal compétent. De la même manière, un médecin pourrait informer de la transmission de données personnelles à l'assurance-maladie à des fins de facturation. Le secret professionnel ne serait pas touché dans de tels cas. Si un conflit devait néanmoins exister dans un cas particulier, il pourrait être résolu par l'une des restrictions prévues à l'al. 3 (par ex. en cas d'intérêts prépondérants). 20

L'exception générale au devoir d'information pour les personnes soumises à l'obligation de garder le secret est également surprenante parce que la confidentialité des données personnelles traitées est certes garantie en cas 21

d'obligation légale de garder le secret, mais le besoin d'information protégé par le devoir d'information ne disparaît pas pour autant sans autre. Par exemple, la question de savoir à quelles fins le détenteur du secret traite les données personnelles reste ouverte, p. ex. si le médecin ou l'avocat pratique également le profilage et utilise les données collectées à des fins de marketing.

22 Le RGPD contient une exception comparable pour le cas où les données personnelles collectées sont soumises à un secret professionnel. Elle est à la fois plus large et plus étroite que l'exception de la LPD : l'exception du RGPD n'est pas limitée aux personnes privées, mais ne s'applique qu'en cas de collecte indirecte.

E. Privilège des médias (al. 1 let. d)

23 Une autre exception concerne l'activité de recherche des médias en vue de la publication d'un travail journalistique et de la protection des sources. Dans les mêmes conditions que celles selon lesquelles un renseignement peut être refusé, il est également possible de renoncer à une information : L'art. 20 al. 1 let. d LPD renvoie à l'art. 27 LPD. Cette exception protège la fonction d'information et de contrôle des médias. Si les personnes qui font l'objet d'une recherche d'investigation devaient en être informées et les sources d'information divulguées, le travail journalistique serait rendu impossible et les médias ne pourraient pas remplir la fonction démocratique qui leur est dévolue.

24 L'exception de l'al. 1 let. d n'est disponible que pour les traitements de données personnelles en vue d'une publication dans la partie rédactionnelle d'un média à parution périodique (p. ex. un journal ou un magazine en ligne). L'exception ne peut pas être invoquée pour les "publireportages" et autres publications à caractère essentiellement publicitaire, ni pour les activités de recherche en vue d'un film documentaire ou d'un autre média non périodique. Le cas échéant, il est toutefois possible de recourir à un autre motif d'exception ou de restriction pour de telles activités de recherche, par exemple à l'art. 20 al. 3 let. b LPD (entrave à la finalité).

F. Impossibilité d'informer (al. 2 let. a)

25 Si les données personnelles ne sont pas collectées directement auprès de la personne concernée, c'est-à-dire indirectement, l'obligation d'informer tombe

également si l'information n'est pas possible. En cas de collecte directe, l'exception n'est pas disponible, ce qui est logique. Logiquement, la collecte directe de données auprès de la personne concernée ne peut pas être possible, mais son information impossible.

L'impossibilité de procéder à l'information existe par exemple lorsque la personne concernée ne peut pas du tout être identifiée. Dans l'exemple de la photo d'une personne inconnue cité dans le message, cela ne peut pas être supposé sans autre au vu des possibilités technologiques actuelles. L'exception n'a pas non plus de pertinence pratique : En cas d'impossibilité d'identification, le lien avec la personne des données concernées fait généralement défaut et la question du devoir d'information ne se pose même pas. 26

G. Effort disproportionné (al. 2 let. b)

Enfin, l'obligation d'informer ne s'applique pas lorsque les données personnelles sont collectées indirectement et que l'information des personnes concernées exigerait un effort disproportionné. Là encore, l'exception ne peut pas être invoquée en cas de collecte directe. On peut raisonnablement attendre de celui qui collecte des données personnelles directement auprès de la personne concernée qu'il l'informe de la collecte. 27

Il convient de déterminer au cas par cas quel effort est encore proportionné et se base sur l'effort du responsable par rapport à l'intérêt des personnes concernées à être informées. Ce qui est déterminant à cet égard, ce n'est pas l'intérêt concret à être informé de certaines personnes, mais un intérêt général à être informé. Plus les données traitées sont sensibles, plus le traitement est important, plus les modalités du traitement sont critiques, plus la criticité du but du traitement est grande et plus les technologies utilisées pour le traitement sont nouvelles, plus on peut exiger des efforts importants du responsable. 28

Le message cite comme exemple de charge disproportionnée le traitement de données personnelles à des fins d'archivage. Dans le cas d'un grand nombre de personnes, l'information serait liée à une charge de travail élevée, alors que l'intérêt des personnes concernées à être informées devrait régulièrement rester limité dans de tels cas. La disposition d'exception analogue du RGPD cite comme autres exemples le traitement à des fins de recherche scientifique 29

ou historique ainsi qu'à des fins statistiques. L'information des personnes concernées peut également être disproportionnée lorsque de très grandes quantités de données sont utilisées pour l'entraînement de Large Language Models et de modèles d'IA similaires, par exemple lorsque l'intelligence artificielle est entraînée avec "l'ensemble de l'Internet". Dans la pratique, il est recommandé de documenter à chaque fois les considérations pour lesquelles une information de la personne concernée n'est plus jugée proportionnée.

30 L'état de fait de l'al. 2 let. b est conçu comme une exception, mais une limitation aurait été plus appropriée. Si une information est disproportionnée, par exemple en raison du grand nombre de personnes concernées, une omission totale de l'information ne semble pas appropriée. Un moyen plus doux (et évident) dans de tels cas serait de mettre à disposition une déclaration de protection des données sur le site web de l'entreprise concernée en renonçant à une notification individuelle.

III. RESTRICTIONS

A. Généralités

31 L'article 20 LPD contient à l'al. 3 un total de cinq constellations dans lesquelles l'information peut être limitée, différée ou suspendue. Contrairement aux exceptions visées aux al. 1 et 2, l'obligation d'informer ne disparaît pas complètement dans ces cas et l'information ne peut être limitée que dans la mesure où le motif correspondant l'exige dans le cas particulier. Si le motif de la restriction disparaît ultérieurement, l'information doit être complétée. Comme pour les exceptions, la personne concernée ne doit pas être informée de l'application et de l'étendue de la restriction conformément à l'al. 3 et il ne lui reste plus qu'à faire valoir son droit d'accès.

32 Les possibilités de restriction de l'information se basent en grande partie sur une pesée des intérêts, lors de laquelle le motif concret d'une restriction doit être mis en relation avec le besoin d'information des personnes concernées. En revanche, dans le cas des exceptions, c'est le plus souvent l'existence d'un fait précis (par exemple le fait que la personne concernée dispose déjà de l'information) qui permet de déterminer s'il peut être fait usage de l'exception ou non.

B. Intérêts prépondérants de tiers (al. 3 let. a)

Il existe une possibilité de limiter l'information si celle-ci est nécessaire en raison d'intérêts prépondérants de tiers. La formulation "tiers" à l'al. 3 let. a ne doit pas être comprise exclusivement au pluriel et l'intérêt prépondérant d'un seul tiers suffit également pour pouvoir restreindre l'information. Cette possibilité de limitation existe aussi bien pour les responsables privés que pour les organes fédéraux. 33

La limitation peut être utilisée dans les cas où des tiers ont un intérêt à ce que l'information ne soit pas transmise à la personne concernée et que cet intérêt l'emporte sur le besoin d'information de la personne concernée. Cela est surtout envisageable dans des constellations où la personne concernée obtiendrait également des informations sur des tiers par le biais de l'information et où leurs intérêts au maintien du secret seraient ainsi lésés. Dans la pratique, de tels cas de figure ne devraient toutefois que rarement se présenter, car l'information en tant que telle ne révèle généralement pas de données à caractère personnel. 34

C. Détournement de la finalité (al. 3 let. b)

La limitation de l'information pour les responsables privés et les organes fédéraux est également possible si l'information fait échouer le but poursuivi par le traitement des données. L'art. 20 al. 3 let. b LPD ne précise pas si une simple atteinte à la finalité du traitement suffit à limiter l'information ou s'il doit y avoir un empêchement complet. Selon le message, les dispositions de l'art. 20 al. 3 LPD doivent être interprétées de manière restrictive, raison pour laquelle il faut partir du principe que l'empêchement doit être total. 35

Dans le cas de plusieurs finalités poursuivies par un traitement de données, l'information à la personne concernée doit faire échouer la finalité principale proprement dite, qui doit en outre revêtir une importance considérable selon le message. La possibilité de restreindre l'information est également limitée par le fait que les intérêts purement économiques n'entrent généralement pas dans le champ d'application de la restriction selon l'al. 3 let. b. Dans la pratique, il n'y aura donc que peu de cas où les responsables privés pourront faire usage de cette restriction. Les possibilités d'application sont plus larges pour les organes fédéraux, surtout dans le domaine de la poursuite pénale, 36

mais dans ce cas, la possibilité de restriction de l'al. 3 let. d ch. 2 devrait également s'appliquer.

37 Les activités de recherche en rapport avec le journalisme d'investigation, qui ne tombent pas sous le coup de l'exception de l'art. 20 al. 1 let. d LPD, par exemple parce que la recherche est effectuée pour un documentaire et non pour un média à parution périodique, constituent un exemple d'application de la restriction. Un ajournement de l'information sur la base de l'al. 3 let. b peut également se justifier lorsque des données personnelles sont traitées dans le cadre d'une conservation de preuves pour un procès ultérieur et que l'information de la personne concernée rendrait impossible la collecte de ces preuves. Il est tout aussi envisageable de différer l'information lors de la réalisation d'études comportementales dans lesquelles les personnes concernées doivent adopter un comportement aussi naturel que possible et où une information avant la réalisation de l'étude fausserait les résultats. De même, dans le cas d'une filature justifiée d'une personne par un détective privé, l'information à la personne observée ferait échouer son objectif.

D. Intérêts prépondérants du responsable du traitement (al. 3 let. c)

38 La possibilité de limiter l'information en raison des intérêts prépondérants du responsable n'est ouverte qu'aux responsables privés. Les organes fédéraux ne peuvent pas se prévaloir de cette possibilité.

39 Contrairement à l'al. 3 let. b, les intérêts économiques tels que la promotion des ventes ou le développement de produits entrent également en ligne de compte. Comme la possibilité de restriction ne s'adresse qu'aux responsables privés, il s'agira dans de nombreux cas précisément de tels intérêts économiques. La limitation effective de l'information doit toutefois être précédée d'une mise en balance entre les intérêts du responsable et le besoin d'information des personnes concernées. Il s'agit d'un critère assez ouvert et il est donc conseillé aux responsables de documenter les raisons pour lesquelles leurs propres intérêts prévalent.

40 La condition préalable à une limitation de l'information selon l'al. 3 let. c est en outre qu'aucune communication de données ne soit faite à des tiers. On entend par là les communications à des responsables indépendants, par exemple à des partenaires de coopération ou à des réseaux publicitaires, mais

les autorités sont également concernées. En revanche, les communications à des sous-traitants, qui effectuent le traitement des données sur ordre du responsable, ainsi qu'à des responsables conjoints, sont inoffensives. Si les communications aux sous-traitants et aux responsables conjoints doivent également être couvertes, la LPD parle généralement de "destinataires" plutôt que de "tiers".

De même, selon l'al. 4, les communications de données à des sociétés du groupe sont généralement inoffensives, et ce même si le destinataire interne au groupe est lui-même un responsable. En cas de communication de données personnelles au sein du propre groupe, par exemple dans le domaine des RH, les conditions de la possibilité de restriction restent donc remplies. Ce privilège de groupe n'était pas prévu à l'origine dans le projet de loi et a été ajouté au cours des débats parlementaires. L'exclusion de la possibilité de restriction de l'al. 3 let. c ne concerne donc que les communications à des responsables distincts en dehors du propre groupe de sociétés. 41

L'al. 3 let. c offre une marge de manœuvre considérable pour l'application pratique d'une limitation de l'information, car un intérêt prépondérant du responsable peut être invoqué pour un grand nombre de traitements de données. En règle générale, on peut supposer qu'il existe des intérêts prépondérants, par exemple dans le cas de traitements de données à bas seuil tels que de simples mesures de fidélisation de la clientèle, pour lesquels les circonstances ainsi que la manière dont les données sont traitées sont évidentes et pour lesquels une information complète n'apporterait donc aucune valeur ajoutée aux personnes concernées. 42

E. Intérêts publics prépondérants (al. 3 let. d ch. 1)

Pour les organes fédéraux, il est possible de limiter une information si cela est nécessaire pour protéger des intérêts publics prépondérants. Pour les responsables privés, il n'est pas possible de fonder une limitation de l'information sur l'al. 3 let. d. 43

Ce qu'il faut entendre par intérêt public est défini de manière assez large. La norme cite à titre d'exemple les intérêts de la sécurité intérieure ou extérieure de la Suisse, ce qui peut être pertinent en particulier dans le contexte des activités de renseignement. Mais les intérêts publics sont également concernés lorsqu'il s'agit par exemple de respecter des obligations de droit 44

international public, de poursuivre des objectifs diplomatiques ou d'entretenir des relations avec l'étranger. Un organe fédéral pourrait donc limiter l'information, par exemple, si la communication aux personnes concernées devait nuire aux relations de politique étrangère avec un autre pays.

45 Ici aussi, l'intérêt public doit "prévaloir" et une pesée des intérêts est donc nécessaire pour qu'un organe fédéral puisse faire usage de la possibilité de restriction. Une pesée qui compare le besoin d'information des personnes (individuellement) concernées avec les intérêts nationaux de sécurité devrait toutefois souvent être en faveur de la possibilité de restriction.

F. Mise en danger de la procédure (al. 3 let. d ch. 2)

46 Enfin, l'al. 3 let. d ch. 2 prévoit encore une possibilité de restriction lorsque l'information aurait pour conséquence de mettre en danger une enquête, une instruction ou une procédure administrative ou judiciaire. Cette possibilité n'est également ouverte qu'aux organes fédéraux et ne peut pas être utilisée par des responsables privés. Les responsables privés doivent recourir à un autre motif d'exception ou de restriction dans les cas où la procédure est menacée.

47 Cette possibilité a un contenu proche de la limitation de l'information lorsque celle-ci ferait échouer le but même du traitement des données. Contrairement à l'al. 3 let. b, pour lequel la finalité doit être effectivement mise en échec, une mise en danger suffit toutefois pour la possibilité de restriction selon l'al. 3 let. d. Il n'est donc pas nécessaire que la mise en danger se réalise effectivement ; le risque suffit.

BIBLIOGRAPHIE

Bieri Adrian/Powell Julian, Informationspflicht nach dem totalrevidierten Datenschutzgesetz, AJP 2020, S. 1533 ff.

Bühlmann Lukas/Lagler Marion, Informationspflichten und Auskunftsrecht nach dem neuen Datenschutzrecht, SZW 2021, S. 16 ff.

Cottier Bertil, Transparence des traitements de données personnelles opérés par les organes fédéraux: un pas en avant, deux en arrière, SZW 2021, S. 65 ff.

Ettlinger Claudius, Die Informationspflicht gemäss neuem Datenschutzgesetz, in Jusletter IT 16. Dezember 2021.

Pärli Kurt/Flück Nathalie, Kommentierung zu Art. 19 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Aufl., Bern 2023.

Rosenthal David, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020.

Vasella David, Zu den Anforderungen an die Erfüllung der Informationspflicht nach dem revDSG, datenrecht.ch, 28. Oktober 2022, abrufbar unter https://datenrecht.ch/zu-den-anforderungen-an-die-erfuellung-der-informationspflicht-nach-dem-revdsg, besucht am 25.5.2023 (zit. Informationspflicht).

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.7.2017, BBl 2017 S. 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 18.5.2023 (zit. Botschaft DSG).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 21 LPD

Un commentaire de Liliane Obrecht / Anna Kuhn

PROPOSITION DE CITATION

Liliane Obrecht/Anna Kuhn, Commentaire de l'art. 21 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Obrecht/Kuhn, art. 21 LPD N. XXX.

Art. 21 Devoir d'informer en cas de décision individuelle automatisée

[1] Le responsable du traitement informe la personne concernée de toute décision qui est prise exclusivement sur la base d'un traitement de données personnelles automatisé et qui a des effets juridiques pour elle ou l'affecte de manière significative (décision individuelle automatisée).

[2] Si la personne concernée le demande, le responsable du traitement lui donne la possibilité de faire valoir son point de vue. La personne concernée peut exiger que la décision individuelle automatisée soit revue par une personne physique.

[3] Les al. 1 et 2 ne s'appliquent pas dans les cas suivants:

a. la décision individuelle automatisée est en relation directe avec la conclusion ou l'exécution d'un contrat entre le responsable du

traitement et la personne concernée et la demande de cette dernière est satisfaite;

b. la personne concernée a expressément consenti à ce que la décision soit prise de manière automatisée.

[4] Si la décision individuelle automatisée émane d'un organe fédéral, ce dernier doit la qualifier comme telle. L'al. 2 ne s'applique pas lorsque la personne concernée ne doit pas être entendue avant la décision conformément à l'art. 30, al. 2, de la loi fédérale du 20 décembre 1968 sur la procédure administrative (PA)[6] ou en vertu d'une autre loi fédérale.

TABLE DES MATIÈRES

En bref ... 297
I. Généralités ... 297
A. Aperçu et structure ... 297
B. Objectif de la norme ... 297
C. Genèse ... 298
II. Obligation d'information en cas de décision individuelle automatisée (al. 1) ... 301
A. Contexte technique ... 302
1. Niveaux d'automatisation ... 302
2. Évolution ... 304
B. Décision individuelle automatisée ... 304
1. Automatisation complète ... 304
2. Conséquence juridique ou atteinte significative ... 305
3. Autres conditions ... 307
4. Appréciation ... 307
C. Obligation d'information ... 308
1. Moment, contenu et forme ... 308
2. Appréciation ... 310
III. Droits de la personne concernée (al. 2) ... 310
A. Droit de faire valoir son point de vue ... 310
1. Particuliers ... 311
2. État ... 311
B. Droit à un contrôle par une personne physique ... 312
IV. Exceptions (al. 3) ... 313
V. Décision individuelle automatisée prise par un organe fédéral (al. 4) ... 313
A. Obligation de signalement ... 314
B. Non-applicabilité de l'art. 21, al. 2, LPD ... 315
C. Absence d'intention générale de régularité ... 316
VI. Application ... 316
VII. Remarques de droit comparé ... 318
A. Réglementation européenne (art. 22 de la DSGVO) ... 318
B. Casuistique ... 319
1. Distinction entre décisions partiellement et entièrement automatisées ... 319
a. Autriche : l'algorithme AMAS ... 319
b. Allemagne : l'exemple de la Schufa ... 321
2. Concernant l'atteinte substantielle au sens de l'article 21, al. 2, de la LPD ... 322
a. Pays-Bas : le système SyRI ... 322
b. Tribunal d'arrondissement d'Amsterdam : service de taxi Uber ... 323
c. Tribunal d'arrondissement d'Amsterdam : application Ola ... 323
3. Enseignements pour le droit suisse ... 323
VIII. Perspectives ... 324

Bibliographie 325
Matériaux 331

EN BREF

L'article 21 de la LPD prévoit une obligation d'information en cas de décisions individuelles entièrement automatisées qui portent gravement atteinte à une personne concernée ou qui entraînent des conséquences juridiques pour celle-ci. En outre, cette disposition accorde à la personne concernée divers droits de protection : un droit de faire valoir son point de vue et un droit à une vérification par un être humain. De plus, cette norme oblige les organes fédéraux à signaler expressément les décisions individuelles entièrement automatisées en tant que telles. Une lacune majeure de cette disposition réside dans le fait qu'elle n'inclut pas les décisions partiellement automatisées dans son champ d'application.

I. GÉNÉRALITÉS

A. Aperçu et structure

La révision de la loi sur la protection des données a introduit en septembre 2023 la **notion** de décision individuelle automatisée dans le droit suisse. L'art. 21 LPD régit les obligations du responsable du traitement au sens de l'art. 5, let. j, LPD et les droits de la personne concernée en cas de décision individuelle automatisée. L'al. 1 définit la décision individuelle automatisée et établit une obligation d'information à cet égard. L'al. 2 énonce les droits de la personne concernée, parmi lesquels figurent le droit d'être entendue ainsi que le droit à la vérification de la décision par une personne physique. L'al. 3 prévoit des exceptions aux al. 1 et 2. L'al. 4 établit une disposition particulière pour les organes fédéraux. 1

La LPD est précisée par l'**OPDo**. Celle-ci ne contient pour l'instant aucune autre disposition relative aux décisions individuelles automatisées. 2

B. Objectif de la norme

Selon le message du Conseil fédéral, l'article 21 de la LPD vise à se conformer aux dispositions existantes **du droit international**. Sur le fond, le Conseil fédéral justifie cette nouvelle disposition par le fait que les décisions individuelles automatisées ne cessent de se multiplier en raison des évolutions technologiques. Il n'y a toutefois pas d'analyse détaillée des risques liés aux 3

décisions individuelles automatisées ni du besoin de réglementation qui en découle.

4 Le message cite toutefois des exemples montrant comment des décisions **erronées** peuvent être prises sur la base de jeux de données faux ou incomplets. Cela laisse supposer que la crainte de telles décisions ait également constitué l'un des motifs de l'introduction du nouvel article 21 de la LPD. La protection de la dignité humaine peut donc être considérée comme un objectif réglementaire potentiel, dont le but est notamment de protéger les personnes contre une simple réduction au statut d'objet de décisions automatisées. Un autre objectif réglementaire possible peut être vu dans la protection contre la discrimination par l'État : lorsqu'une décision individuelle automatisée repose sur des procédés d'apprentissage automatique, elle ne suit pas des règles établies par l'homme, mais apprend à partir de vastes quantités de données (appelées « données d'entraînement »), qui peuvent refléter des désavantages sociaux, des schémas ou des stéréotypes dépassés (ce que l'on appelle le *data bias*). De cette manière, une décision individuelle automatisée peut reproduire des désavantages et avoir un effet discriminatoire. La nouvelle disposition accorde aux personnes concernées la possibilité d'exercer une influence lorsqu'elles font l'objet d'une décision individuelle automatisée (« droit à être entendu par un être humain »). Selon le message, cela vise à contrer les décisions erronées et leurs conséquences. Par ailleurs, le législateur considère ainsi implicitement que les décisions humaines sont supérieures, car il estime que les décisions automatisées erronées peuvent être évitées grâce à une intervention humaine. C'est également sur cette hypothèse de base que repose la disposition relative aux décisions individuelles automatisées prévue par la DSGVO (cf. N. 69 et suivants), que le message cite comme justification supplémentaire de l'art. 21 LPD.

C. Genèse

5 Le débat juriste autour des décisions individuelles automatisées n'a certes pris de l'ampleur qu'avec l'introduction expresse de l'art. 21 LPD. Cependant, comme on le verra ci-après, cette notion remonte déjà à plusieurs décennies. L'art. 21 LPD est donc le résultat d'une évolution progressive qui s'appuie sur des tentatives de réforme antérieures et des prescriptions internationales.

6 **1981 :** Les documents relatifs à la directive du 16 mars 1981 sur le traitement des données personnelles au sein de l'administration fédérale mettaient en

garde contre les risques pouvant découler de la création de profils de personnalité et de la prise de décision automatisée qui en découle. Une réglementation explicite de la décision individuelle automatisée n'a toutefois pas été introduite dans le droit suisse à cette époque.

2003 : Dans le cadre de la révision partielle de la LPD en 2003, le Conseil fédéral souhaitait introduire une obligation expresse d'information en cas de décisions individuelles automatisées. Le Parlement a toutefois rejeté cette proposition. 7

2017 – 2020 : La version de l'article 21 de la LPD proposée par le Conseil fédéral dans son message relatif à la révision totale de 2017 a été reprise pour l'essentiel par le Parlement. Alors que la consultation avait donné lieu à des controverses, la disposition en question n'a guère été contestée au cours de la procédure parlementaire. Comme le montre le tableau de concordance ci-dessous, les modifications apportées se sont limitées à des précisions rédactionnelles : 8

	Vorentwurf (Art. 15) Informations- und Anhörungspflicht bei einer automatisierten Einzelentscheidung	**Entwurf (Art. 19)** Informationspflicht bei einer automatisierten Einzelentscheidung	**Endfassung (Art. 21)** Informationspflicht bei einer automatisierten Einzelentscheidung
Abs. 1	Der Verantwortliche informiert die betroffene Person, wenn eine Entscheidung erfolgt, die ausschliesslich auf einer automatisierten Datenbearbeitung beruht, und diese rechtlichen Wirkungen oder erhebliche Auswirkungen auf die betroffene Person hat.	Der Verantwortliche informiert die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung, einschliesslich Profiling, beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt.	Der Verantwortliche informiert die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt (automatisierte Einzelentscheidung).
Abs. 2	Er gibt der betroffenen Person die Möglichkeit, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Personendaten zu äussern.	Er gibt der betroffenen Person auf Antrag die Möglichkeit, ihren Standpunkt darzulegen. Die betroffene Person kann verlangen, dass die Entscheidung von einer natürlichen Person überprüft wird.	Er gibt der betroffenen Person auf Antrag die Möglichkeit, ihren Standpunkt darzulegen. Die betroffene Person kann verlangen, dass die automatisierte Einzelentscheidung von einer natürlichen Person überprüft wird.
Abs. 3	Die Informations- und Anhörungspflicht gilt nicht, wenn ein Gesetz eine automatisierte Einzelentscheidung vorsieht.	Die Absätze 1 und 2 gelten nicht, wenn: a. die Entscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und ihrem Begehren stattgegeben wird; oder b. die betroffene Person ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt.	Die Absätze 1 und 2 gelten nicht, wenn: a. die automatisierte Einzelentscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und ihrem Begehren stattgegeben wird; oder b. die betroffene Person ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt.
Abs. 4	--	Ergeht die automatisierte Einzelentscheidung durch ein Bundesorgan, so muss es die Entscheidung entsprechend kennzeichnen. Absatz 2 gilt nicht, wenn der betroffenen Person gegen die Entscheidung ein Rechtsmittel zur Verfügung steht.	Ergeht die automatisierte Einzelentscheidung durch ein Bundesorgan, so muss es die Entscheidung entsprechend kennzeichnen. Absatz 2 ist nicht anwendbar, wenn die betroffene Person nach Artikel 30 Absatz 2 des Verwaltungsverfahrensgesetzes vom 20. Dezember 19686 (VwVG) oder nach einem anderen Bundesgesetz vor dem Entscheid nicht angehört werden muss.

Tableau 1 : Tableau de concordance sur l'évolution de l'art. 21 LPD (élaboration propre)

2018 : Une nouvelle impulsion a été donnée à la réglementation des décisions individuelles automatisées dans le cadre de la mise en œuvre de la directive (UE) 2016/680, contraignante pour la Suisse, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans le domaine de la coopération judiciaire et policière. À cette fin, une disposition relative aux décisions individuelles automatisées a été introduite dans le cadre de la loi sur la protection des données de Schengen (LPDS ; en vigueur jusqu'au 31 août 2023) (art. 11 LPSC). Celle-ci obligeait les organes fédéraux, dans les domaines concernés, à informer les personnes concernées des décisions individuelles automatisées et leur accordait des droits de participation correspondants. Avec l'entrée en vigueur de la loi révisée sur la protection des données, la LPSC a été abrogée (art. 68 en liaison avec l'annexe 1 LPD). L'article 21 de la LPD a succédé, sur le fond, à l'article 11 de la LPSD. 9

2019 – 2023 : En outre, l'introduction de l'article 21 de la LPD vise à mettre en œuvre les obligations de la Suisse en vertu du droit international. La Convention modernisée du Conseil de l'Europe sur la protection des données (Convention 108+, Conv. 108+ du Conseil de l'Europe), que la Suisse a signée le 21 novembre 2019 et ratifiée le 7 septembre 2023, oblige expressément les États parties à garantir un droit à l'information et à être entendu en cas de décisions individuelles automatisées (art. 8, al. 1, let. e, et art. 9, al. 1, let. a, de la Convention du Conseil de l'Europe 108+). En outre, en introduisant l'art. 21 LPD, le législateur visait à instaurer un niveau de protection des données qui, par rapport à l'Union européenne, continue d'être considéré comme «adéquat» au sens de l'art. 45 de la DSGVO. 10

II. OBLIGATION D'INFORMATION EN CAS DE DÉCISION INDIVIDUELLE AUTOMATISÉE (AL. 1)

La décision individuelle automatisée est définie juridiquement à l'art. 21, al. 1, LPD. Afin de pouvoir situer cette notion (B.), il convient tout d'abord de formuler quelques remarques sur l'automatisation et son évolution technique (A.). Les conditions légales essentielles seront ensuite précisées (C.). 11

A. Contexte technique

1. Niveaux d'automatisation

12 Le terme « automatisation » désigne le transfert de tâches des personnes vers des machines. Une décision individuelle automatisée peut présenter différents niveaux d'automatisation. De manière générale, on peut distinguer l'automatisation partielle de l'automatisation complète.

13 La notion d'automatisation partielle revêt plusieurs significations. D'une part, il peut s'agir d'une **aide à la décision**. Dans ce cas, le système automatisé prépare la décision (collecte, compilation ou évaluation d'informations ; établissement de synthèses). La décision proprement dite est toutefois prise par une personne physique responsable.

- *Ainsi, les systèmes partiellement automatisés peuvent par exemple être utilisés pour établir des diagnostics médicaux en analysant des radiographies, des tomodensitométries ou des IRM.*
- *Les systèmes semi-automatisés peuvent être utilisés pour établir les conditions contractuelles.*
- *La semi-automatisation peut également s'avérer utile pour extraire des données pertinentes à partir de volumes importants de texte. Ainsi, dans l'administration fiscale, un système d'aide à la décision peut mettre à la disposition de l'autorité des données supplémentaires qui ne résultent pas directement de la déclaration d'impôt du contribuable, ou mettre en évidence les clauses contractuelles pertinentes dans des contrats volumineux.*
- *Dans le cadre des procédures pénales, notamment aux États-Unis, on utilise des systèmes semi-automatisés qui calculent la probabilité de récidive des délinquants.*

14 D'autre part, le système semi-automatisé peut servir de **vérification de la décision**, en étant utilisé pour contrôler une décision prise par une personne physique.

15 La **plenaire automatisation**, en revanche, signifie qu'un système exécute lui-même chaque étape du processus décisionnel. Au sens strict, même la

programmation et le déclenchement du processus décisionnel doivent être assurés par le système.

- *Ainsi, dans le secteur privé, les décisions relatives aux demandes de crédit peuvent par exemple être prises de manière entièrement automatisée, en vérifiant automatiquement la solvabilité et la capacité de paiement de la personne concernée. La conclusion des contrats s'effectue alors de manière automatisée.*
- *On peut également envisager l'automatisation du processus de recrutement. On peut penser, par exemple, à la présélection entièrement automatisée des candidatures de travailleurs potentiels. Dans ce cadre, c'est le système qui décide de l'invitation à un entretien d'embauche avec une personne physique.*
- *Les systèmes entièrement automatisés peuvent attribuer une place d'études à des futurs étudiants et, par là même, les affecter à un établissement d'enseignement supérieur.*

Dans le secteur public, l'automatisation complète se prête particulièrement bien, en raison de la standardisation des processus et de la disponibilité de grandes quantités de données, aux **procédures d'administration de masse**. Il s'agit des domaines de l'administration publique dans lesquels un grand nombre de décisions sont prises sur des situations factuelles quasi identiques. 16

- *Ainsi, en raison de la disponibilité de grandes quantités de données, la procédure d'imposition fiscale se prête à être menée de manière partiellement, mais aussi entièrement automatisée.*
- *Dans le domaine de la sécurité sociale, la décision relative au droit à une réduction des cotisations s'avère se prêter à une automatisation complète.*
- *Dans la procédure d'octroi des permis de construire également, l'introduction de décisions individuelles entièrement automatisées est envisagée comme une possibilité.*

Le potentiel des systèmes automatisés est jugé particulièrement élevé dans un avenir proche au sein de l'administration publique pour les systèmes partiellement automatisés. Ainsi, les tâches existantes devraient être exécutées de manière plus efficace, plus précise et donc plus sûre sur le plan juridique. 17

2. Évolution

18 Les origines de la décision individuelle automatisée remontent à ce que l'on appelle les **systèmes experts**. Ceux-ci reposent sur des schémas structurés de type « si... alors » (appelés systèmes basés sur des règles) et, en ce sens, ne vont pas au-delà des processus décisionnels cognitifs des personnes physiques.

19 C'est notamment grâce à l'émergence du **Big Data Analytics** – la possibilité d'analyser de très grands ensembles de données non structurés – et aux avancées techniques qui y sont liées que les méthodes d'apprentissage automatique (souvent désignées de manière quelque peu générique sous le terme d'« intelligence artificielle » [IA]) ont pu s'imposer. Il en résulte en quelque sorte un changement de perspective : au lieu de causalités, ce sont les corrélations ou les probabilités qui entrent en jeu – par exemple lors de l'utilisation de réseaux neuronaux artificiels. Les ensembles de données ne sont plus traités à l'aide de schémas « si... alors », mais les systèmes établissent plutôt leurs propres règles pour parvenir à un résultat. Or, la manière dont les systèmes parviennent à un tel résultat reste souvent obscure. La littérature ne fait pas toujours clairement la distinction entre ce qui relève d'une « simple » automatisation ou d'un « simple » système automatisé et ce qui relève de l'utilisation de méthodes d'apprentissage automatique.

B. Décision individuelle automatisée

1. Automatisation complète

20 Il y a décision individuelle automatisée au sens de l'art. 21 LPD lorsqu'une décision repose **exclusivement sur un traitement automatisé** et qu'elle entraîne une conséquence juridique pour la personne concernée ou la porte gravement atteinte (art. 21, al. 1, LPD) . Il est nécessaire qu'une décision soit prise à l'égard d'une personne déterminée (décision individuelle) et qu'elle repose sur le traitement de données à caractère personnel. Du point de vue du droit public, une décision individuelle automatisée peut également être qualifiée de «décision automatisée».

21 L'élément déterminant est que le traitement s'effectue «sans intervention d'une personne physique». Il s'agit donc d'une **évaluation des faits** ainsi que d'une prise de décision **détachées d'une personne physique**, et donc d'une

automatisation complète au sens de la distinction opérée dans le présent commentaire (cf. N. 15). Toutefois, si la décision ne peut plus être modifiée, le fait qu'elle soit communiquée à la personne concernée par une personne physique ne s'oppose pas à l'automatisation complète, conformément au message. Divers auteurs estiment en revanche qu'il y a toujours décision individuelle automatisée même lorsqu'une personne physique est impliquée dans la programmation. Si l'on suit ce point de vue, une décision individuelle automatisée au sens de l'art. 21, al. 1, LPD ne doit pas nécessairement être prise de manière totalement indépendante de l'intervention humaine.

2. Conséquence juridique ou atteinte significative

Une décision individuelle automatisée implique en outre qu'elle soit liée à une conséquence juridique ou qu'elle porte une atteinte significative à la personne concernée. Selon le message du Conseil fédéral, la décision est liée à une **conséquence juridique** lorsqu'elle entraîne des conséquences directes et prévues par la loi pour la personne concernée. La décision entraîne toujours une conséquence juridique lorsqu'elle affecte la situation juridique de la personne concernée – c'est-à-dire lorsqu'elle crée, modifie ou supprime un droit pour celle-ci. Contrairement à ce qui est le cas pour l'atteinte (cf. N. 24), il n'est pas exigé que la conséquence juridique revête une importance particulière. À titre d'exemple, le Conseil fédéral cite la conclusion et la résiliation de contrats, qui entraînent chacune une conséquence juridique pour la personne concernée en tant que partie contractante. Concrètement, il est fait mention de la conclusion automatisée d'un contrat d'assurance. Dans ce contexte, la couverture d'assurance et l'obligation de payer les primes devraient être considérées comme des conséquences juridiques. En revanche, selon le message, les factures de primes envoyées périodiquement et de manière automatisée sur la base du contrat d'assurance ne sont pas considérées comme une décision individuelle automatisée, d'autant plus que la facturation, en tant que conséquence juridique, découle déjà de la conclusion du contrat. De même, le fait lorsqu'aucun contrat n'est conclu avec une personne. Dans cet exemple, la non-conclusion du contrat peut néanmoins être considérée comme une décision individuelle automatisée et entraîner une obligation d'information si la personne concernée subit de ce fait un préjudice considérable (cf. N. 24).

22

23 Dans le contexte du droit public, il y a essentiellement une conséquence juridique lors de l'adoption de **décisions** au sens de l'art. 5 PA ainsi que lors d'actes réels au sens de l'art. 25a PA. Le message cite à titre d'exemple les taxations automatisées.

24 Une décision individuelle automatisée entraîne en outre une obligation d'information lorsque la personne concernée s'en trouve **considérablement préjudiciée**. C'est ce qu'il convient de supposer lorsque la décision a un effet négatif sur les intérêts économiques ou personnels de la personne concernée. La situation doit toutefois atteindre un certain degré de gravité ; une simple nuisance ne suffit pas. Des aspects tels que l'importance du bien lésé pour la personne concernée, la durée de l'effet de la décision ou la possibilité de se tourner vers des alternatives. Il convient donc de déterminer si la personne concernée subit un préjudice considérable en appréciant l'ensemble des circonstances au cas par cas. Le message cite comme exemple possible l'attribution de prestations médicales ou la non-conclusion d'un contrat sur la base d'une décision individuelle automatisée.

25 Parmi les **exemples** de décisions individuelles automatisées entraînant une conséquence juridique ou une atteinte considérable pour la personne concernée, on peut également citer :

- *la conclusion ou la non-conclusion d'un contrat de crédit-bail, y compris ses modalités (par exemple, taux d'intérêt, délai de paiement), dans la mesure où ces éléments dépendent d'une évaluation automatisée de la situation financière de la personne concernée (conséquence juridique ou atteinte considérable en cas de non-conclusion) ;*
- *le refus d'une assurance maladie de conclure un contrat avec la personne concernée sur la base de l'évaluation automatisée de ses données de santé (préjudice important) ;*
- *l'envoi automatisé d'amendes routières sur la base d'images du conducteur concerné (conséquence juridique) ;*
- *le rejet automatisé d'une demande de crédit en ligne ou d'une candidature en ligne sans intervention humaine (préjudice important) ;*
- *la fixation de conditions contractuelles, par exemple pour une tarification personnalisée (conséquence juridique) ;*

En revanche, ne sont pas considérées comme des décisions individuelles automatisées : 26

- *l'envoi de publicités personnalisées, car il n'y a ni conséquence juridique ni préjudice d'une gravité suffisante.*

3. Autres conditions

Selon le message du Conseil fédéral, il ne faut pas se fonder uniquement sur la caractéristique de «personne physique», mais également tenir compte de la **complexité du système** et de l'**impact particulier** sur la personne concernée. Il y a décision individuelle automatisée lorsque l'automatisation présente une certaine complexité et qu'elle entraîne une conséquence juridique particulièrement préjudiciable pour la personne concernée. Les simples « décisions du type si-alors » ne doivent pas être considérées comme des décisions individuelles automatisées. 27

- *Le Conseil fédéral cite comme exemple le retrait d'argent à un distributeur automatique. Si le solde du compte est suffisant, le retrait est autorisé.*

Hormis cet exemple, le message ne précise pas le niveau de complexité requis pour de telles décisions, qui reste donc pour l'instant indéfini. Le Conseil fédéral précisera toutefois, si nécessaire, dans une ordonnance, dans quels cas une décision repose exclusivement sur un traitement automatisé. 28

Dans le contexte public, certains auteurs se concentrent sur la marge d'appréciation dont disposent les autorités lors de la prise de décision. D'autres voix, en revanche, affirment explicitement qu'une décision individuelle automatisée ne saurait être prise tant qu'une marge d'appréciation est accordée à l'autorité. S'appuyant sur le critère de la complexité, Braun Binder précise que la complexité requise peut être déterminée par un raisonnement a contrario : ne constituent pas des décisions individuelles automatisées celles qui ne nécessitent aucune enquête sur les faits. 29

4. Appréciation

Ni le texte de loi ni le message ne permettent de déterminer précisément quand il y a décision individuelle automatisée. Le critère de la « complexité » du système n'est guère utile. Cela pourrait donner l'impression que la norme ne s'applique qu'aux procédures décisionnelles entièrement automatisées 30

reposant sur des procédés d'apprentissage automatique (ou justement « IA ») , tandis que tout processus fondé sur des schémas « si-alors » n'en relèverait pas. Cela ne saurait guère s'appliquer à l'administration publique, car la plupart des algorithmes qu'elle utilise reposent sur des schémas « si-alors ». La réglementation en matière de protection des données serait donc dépourvue de toute substance. Afin d'éviter que l'article 21 de la LPD ne reste lettre morte, les schémas « si-alors » fondés sur des règles doivent également être pris en compte. L'obstacle lié à l'exigence de complexité ne devrait donc pas être trop élevé dans la pratique.

31 Il est par ailleurs regrettable que les décisions reposant sur une automatisation partielle – sous la forme d'une aide à la décision ou d'une vérification de la décision (cf. N. 13 et suivants) – ne relèvent pas de la notion de « décision individuelle automatisée » au sens de l'art. 21, al. 1, LPD. L'applicabilité de cette disposition se heurtera à de nombreux obstacles dans la pratique. Cela est d'autant plus choquant que l'automatisation partielle, tout comme l'automatisation complète, soulève des questions relatives à la personnalité et aux droits fondamentaux (notamment en matière de discrimination, cf. N. 4). Cela vaut d'autant plus lorsque l'automatisation partielle repose sur des méthodes complexes d'apprentissage automatique.

C. Obligation d'information

32 L'art. 21, al. 1, LPD stipule que le responsable du traitement doit informer la personne concernée d'une décision individuelle automatisée. Compte tenu de la notion de décision individuelle automatisée (cf. N. 20 et suivants), l'obligation d'information ne s'applique donc que si la décision entraîne une conséquence juridique ou une atteinte significative pour la personne concernée (cf. N. 22 et suivants) .

1. Moment, contenu et forme

33 Ni la loi ni le message ne fournissent d'indications détaillées quant au moment, à la forme et au contenu de l'obligation d'information en cas de décision individuelle automatisée.

34 En ce qui concerne le **moment**, le responsable du traitement est libre de choisir s'il informe la personne concernée avant (*ex ante*) ou après (*ex post*) la prise de la décision individuelle automatisée. Même s'il existait de bonnes

raisons de fournir une information préalable – par exemple, la possibilité de se soustraire à une décision individuelle automatisée sans devoir engager une procédure judiciaire –, et qu'une précision légale en ce sens serait nécessaire, cela n'est pas prévu par le libellé de la norme. En ce sens, l'exercice des droits des personnes concernées au titre de l'art. 21, al. 2, de la LPD (exposé du point de vue et réexamen humain a posteriori de la décision, cf. N. 49 et suivants), considéré comme l'un des objectifs de l'obligation d'information, est actuellement suffisamment pris en compte par une information *ex post*.

35 En ce qui concerne la **forme**, on peut se référer à l'article 13 de l'OPDo, qui prescrit une communication sous une forme précise, transparente, compréhensible et facilement accessible. Cette disposition se rapporte en principe à l'obligation d'information lors de la collecte de données à caractère personnel. Une application par analogie à l'article 21, al. 1, de la LPD est possible en raison du libellé identique («informe») justifiée pour l'information relative à une décision individuelle automatisée. Le responsable du traitement peut s'acquitter de cette obligation d'information, par exemple, en publiant ces informations dans une déclaration de confidentialité facilement accessible sur son site web ou en y renvoyant par un lien dans un contrat. L'indication de la décision individuelle automatisée (cf. N. 57 et suivants) n'est obligatoire que pour les organes fédéraux et, *a contrario*, facultative pour les particuliers.

36 L'obligation d'information vise à garantir la transparence et à fournir à la personne concernée toutes les informations nécessaires à l'exercice de ses droits en vertu de l'art. 21, al. 2, de la LPD. Pour ce faire, le responsable du traitement doit impérativement fournir les informations suivantes :

- une indication précisant qu'une décision individuelle automatisée va être prise ou a été prise (selon le moment où l'information est communiquée) ;
- une désignation claire des décisions ou catégories de décisions prises de manière automatisée (seules celles relevant de l'art. 21, al. 1, de la LPD étant concernées) ;
- la possibilité d'exercer le droit de faire valoir son point de vue et de demander la révision de la décision individuelle automatisée, ainsi que des indications sur la mise en œuvre concrète de ces droits (par exemple, les coordonnées du responsable du traitement).

37 Selon l'interprétation défendue ici concernant la logique de la décision individuelle automatisée, il **n'est pas** nécessaire d'en informer la personne

concernée. Pour obtenir les informations correspondantes, celle-ci peut plutôt faire valoir son droit d'accès. En conséquence, le responsable du traitement doit lui communiquer explicitement l'existence de la décision individuelle automatisée ainsi que la logique de décision (cf. art. 25, al. 2, let. f, LPD).

38 L'obligation d'information prévue à l'art. 21, al. 1, LPD doit toujours être mise en œuvre par le responsable du traitement en complément de l'obligation générale d'information lors de la collecte des données prévue à l'art. 19 LPD. Il est toutefois possible que les informations soient fournies au même endroit ou dans le même document (voir, concernant les exigences de forme, N. 35).

2. Appréciation

39 L'obligation d'information exige également implicitement qu'il s'agisse d'une décision individuelle **entièrement automatisée**. Pour l'appréciation de cette circonstance par les auteures, voir N. 31.

III. DROITS DE LA PERSONNE CONCERNÉE (AL. 2)

40 L'art. 21, al. 2, de la LPD confère divers droits à la personne concernée par une décision individuelle automatisée. Elle peut faire valoir son point de vue (A.) et faire réexaminer la décision par une personne physique (B.). Cela permet de souligner que l'information visée à l'al. 1 doit permettre à la personne concernée de faire valoir les droits consacrés à l'al. 2.

A. Droit de faire valoir son point de vue

41 La personne concernée par une décision individuelle automatisée doit avoir la possibilité de faire valoir son point de vue. **Sur demande**, elle doit, d'une part, pouvoir faire part de son point de vue sur le résultat de la décision individuelle automatisée. D'autre part, elle doit pouvoir obtenir des informations sur la manière dont cette décision a été prise. Les informations relatives au processus de prise de décision doivent notamment empêcher que le traitement des données ne repose sur des données incomplètes, inexactes ou obsolètes.

1. Particuliers

Les particuliers auront tout particulièrement intérêt à exercer ce droit de présentation de leur point de vue lorsque la décision individuelle automatisée s'avère **à tort défavorable** pour la personne concernée. Si, par exemple, la solvabilité du particulier concerné est rejetée, cela peut également avoir des conséquences négatives pour le responsable privé si, en raison de cette décision, aucune relation contractuelle ne vient à être établie entre les parties. 42

La loi ne fixe pas le **moment** où le point de vue doit être présenté. Cela peut donc avoir lieu avant ou après la prise de décision. Du point de vue du responsable privé, cela ne pose aucune difficulté tant que cette possibilité existe à *n'importe quel* moment. 43

Le responsable privé peut facturer **des frais** pour l'exercice du droit d'être entendu. Il peut toutefois avoir intérêt à les maintenir à un niveau bas afin de ne pas empêcher la conclusion éventuelle d'un contrat. 44

2. État

Dans le contexte étatique, la prise de position en matière de protection des données doit être comprise comme découlant du **droit d'être entendu** conformément à l'art. 29, al. 2, Cst. En tant que garantie procédurale constitutionnelle fondamentale, le droit d'être entendu doit impérativement être accordé dans toute procédure étatique. 45

Selon la jurisprudence du Tribunal fédéral, la personne concernée par une décision étatique doit pouvoir s'exprimer (par écrit) sur les éléments pertinents de l'état de fait **avant qu'**une décision affectant sa situation juridique ne soit prise. Toutefois, selon le message relatif à la LPD, l'exposé du point de vue peut également avoir lieu après le prononcé de la décision, par exemple par le biais d'un recours. Étant donné que le droit d'être entendu confère le droit de s'exprimer devant l'instance qui a rendu la décision, seul un recours non dévolutif – tel qu'une opposition ayant valeur de recours – peut être envisagé. L'objectif est d'obtenir une décision sous la forme d'une décision sur opposition de la part de l'autorité ayant rendu la décision initiale. 46

Le **délai d'opposition** résulte des lois de procédure applicables. Il est généralement de 30 jours. Les bases légales doivent être adaptées en 47

conséquence si des décisions individuelles automatisées doivent être introduites.

48 L'exposé de son point de vue dans le cadre de la procédure administrative ne doit pas entraîner des **frais (de procédure)** si élevés que la personne concernée y renonce pour cette raison. Des frais peuvent donc en principe être perçus pour le dépôt de la demande. Toutefois, au regard du principe de légalité, cela n'est possible que si la loi le prévoit.

B. Droit à un contrôle par une personne physique

49 L'art. 21, al. 2, LPD prévoit en outre le droit de la personne concernée à un contrôle par une personne physique de la décision individuelle automatisée. Cela peut s'avérer particulièrement important lorsque la personne concernée soupçonne d'être lésée par la décision individuelle automatisée.

50 L'examen doit être effectué par une **personne physique habilitée à prendre des décisions**, afin qu'elle puisse, le cas échéant, infirmer la décision. Elle est toutefois libre dans ses considérations et n'est pas tenue d'annuler la décision. La seule condition, selon l'avis présent, est qu'elle examine la décision en toute bonne foi.

51 Dans la pratique, ce droit à un réexamen a posteriori est jugé **insuffisant**, notamment au regard du risque de discrimination. Il conviendrait de vérifier de manière préventive si les systèmes de décision automatisés prennent involontairement des décisions discriminatoires.

52 Ni la loi ni le message relatif à la LPD ne mentionnent de **délai** précis dans lequel le droit à un réexamen par une personne physique doit être exercé. Pour les particuliers, il n'est pas possible de fixer un délai de manière générale ; celui-ci résultera des circonstances propres à chaque cas. Les organes fédéraux peuvent s'inspirer des délais de réexamen, car ceux-ci confèrent un droit similaire. La demande de réexamen n'est en principe soumise à aucun délai, sous réserve des dispositions légales spéciales. Toutefois, au regard du principe de légalité et afin d'éviter tout arbitraire, il semble judicieux qu'un délai soit explicitement fixé, au moins au niveau de l'ordonnance.

IV. EXCEPTIONS (AL. 3)

L'art. 21, al. 3, LPD prévoit, pour les décisions individuelles automatisées, **deux cas d'exception** dans lesquels ni l'obligation d'informer ni les droits supplémentaires de la personne concernée ne s'appliquent. Comme le soulignent à juste titre Vasella et Henseler, compte tenu de la clarté de la disposition légale et de la place systématique de la norme, il y a lieu de considérer que les exceptions à l'obligation d'informer prévues à l'art. 20 LPD concernant la collecte de données à caractère personnel ne sont pas transposables à l'obligation d'information relative aux décisions individuelles automatisées au sens de l'art. 21, al. 1, LPD. Cette distinction est également confirmée par le libellé de l'art. 20, al. 1, LPD. Même si une décision individuelle automatisée repose sur une base légale (cf. art. 20, al. 1, let. b, LPD), le responsable du traitement ne peut invoquer une exception à l'obligation d'information prévue à l'art. 21, al. 1, LPD. 53

La **première exception** prévue à l'art. 21, al. 3, let. a, LPD s'applique lorsque la décision individuelle automatisée est directement liée à la conclusion ou à l'exécution d'un contrat entre le responsable du traitement et la personne concernée et qu'elle correspond entièrement à la demande de cette dernière. Dans une telle configuration, le législateur a considéré que la personne concernée n'avait aucun intérêt digne de protection à obtenir des informations supplémentaires ou à exercer d'autres droits. 54

L'art. 21, al. 3, let. b, LPD mentionne comme **deuxième exception** le consentement explicite de la personne concernée à la décision individuelle automatisée. Les travaux préparatoires ne contiennent pas d'informations détaillées sur les exigences auxquelles doit satisfaire ce consentement. Selon la conception du législateur, un consentement valable présuppose au moins une information préalable et suffisante. Divers auteurs de la doctrine partent toutefois du principe que les conditions générales relatives au consentement à un traitement de données s'appliquent également dans le contexte des décisions individuelles automatisées. 55

V. DÉCISION INDIVIDUELLE AUTOMATISÉE PRISE PAR UN ORGANE FÉDÉRAL (AL. 4)

Enfin, l'art. 21, al. 4, LPD contient une disposition particulière applicable aux organes fédéraux au sens de l'art. 5, let. i, LPD. Cette disposition leur impose 56

l'obligation de signaler les décisions individuelles automatisées (A.). Elle prévoit en outre, dans certains cas, la non-applicabilité de l'art. 21, al. 2, LPD (B.). Cette disposition n'autorise toutefois pas les organes fédéraux à prendre des décisions individuelles automatisées en raison de l'absence de norme spécifique (C.).

A. Obligation de signalement

57 L'obligation de signalement des décisions rendues de manière automatisée a pour but de permettre à la personne concernée de reconnaître que la **décision n'a pas été prise par une personne physique**. La personne concernée dispose en principe d'un recours contre ces décisions. Le signalement lui permet d'exercer, dans le cadre de la procédure de recours, son droit d'être entendue (art. 29, al. 2, Cst.), en pouvant exposer son point de vue et en faisant réexaminer la décision par une personne physique.

58 La question se pose de savoir comment l'obligation de signalement s'articule avec l'obligation d'information prévue à l'art. 21, al. 1, LPD. En effet, contrairement à l'obligation d'information relative à la collecte de données à caractère personnel prévue à l'art. 19, al. 1, LPD, cette dernière ne s'éteint pas lorsque le traitement est prévu par la loi (art. 20, al. 1, let. b, LPD). Étant donné que les décisions individuelles automatisées au sein de l'administration doivent à l'avenir être introduites notamment dans le cadre de procédures de masse (cf. N. 16), on peut se demander comment le responsable public doit s'acquitter de l'obligation d'information (dans chaque cas particulier). L'indication, en revanche, semble plus ciblée au regard de l'économie de la procédure.

59 La mention doit figurer de manière évidente et facilement identifiable sur la décision automatisée. Selon l'avis défendu ici, il est jugé judicieux de placer cette mention après le contenu proprement dit de la décision, mais avant les voies de recours. La personne concernée apprend ainsi dans un premier temps que la décision a été prise de manière automatisée, avant d'être informée de ses possibilités de recours. Cela correspond à un ordre de lecture naturel. Si la mention figurait après les voies de recours, il y aurait un risque que la personne concernée ne prenne connaissance de cette information que trop tard, voire pas du tout, et qu'elle prenne ainsi une décision non éclairée quant à la voie de recours à engager.

B. Non-applicabilité de l'art. 21, al. 2, LPD

Les droits de la personne concernée, prévus à l'art. 21, al. 2, LPD, de faire valoir son point de vue et de faire réexaminer la décision individuelle automatisée par une personne physique s'appliquent en principe également aux décisions individuelles automatisées rendues par des organes fédéraux. Conformément à l'art. 21, al. 4, de la LPD, ces droits ne s'appliquent toutefois pas lorsque la personne concernée n'a pas à être entendue en vertu de l'art. 30, al. 2, de la PA ou d'une autre loi fédérale. 60

L'art. 30 de la PA précise le droit d'être entendu prévu à l'art. 29, al. 2, de la PA. Conformément à l'al. 1, les parties doivent en principe être entendues avant le prononcé d'une décision. Ce droit est restreint à l'al. 2. Il existe par exemple des exceptions au droit d'être entendu lorsqu'une décision est susceptible de recours (art. 30, al. 2, let. b, PA) ou lorsque les autorités font pleinement droit aux conclusions des parties (art. 30, al. 2, let. c, PA) . Cette disposition vise à éviter les doublons dans le processus décisionnel et à ne pas porter atteinte à la substance du droit d'être entendu. Dans le cadre de la procédure d'opposition, le droit d'être entendu peut être exercé a posteriori. En revanche, lorsque les demandes des parties sont entièrement satisfaites, cet intérêt disparaît. 61

En fin de compte, la dérogation prévue par la législation sur la protection des données a pour conséquence que la LPD n'accorde pas aux personnes concernées par une décision individuelle automatisée prise par l'État des droits plus étendus que ceux déjà prévus par la PA : si les parties doivent de toute façon être entendues conformément à l'art. 30, al. 1, PA, elles bénéficient également des droits – qui ne vont pas au-delà – de l'art. 21, al. 2, de la LPD. Si une exception au titre de l'art. 30, al. 2, de la PA s'applique et que la partie n'a pas à être entendue, celle-ci ne peut pas non plus se prévaloir du droit d'être entendu en matière de protection des données prévu à l'art. 21, al. 2, de la LPD. Les droits prévus à l'article 21, al. 2, de la LPD ont, en ce qui concerne les décisions automatisées relevant du droit fédéral, **un caractère déclaratoire** et ont, le cas échéant, même créé une insécurité juridique pour la personne concernée. 62

C. Absence d'intention générale de régularité

63 La doctrine soulève la question de savoir si, en créant l'article 21, al. 1, de la LPD, le législateur avait l'intention d'introduire en Suisse une norme générale d'admissibilité pour les décisions individuelles automatisées. Selon le Conseil fédéral, les décisions individuelles automatisées prises par l'État constituent des « décisions ordinaires » au sens de l' l'art. 5 PA, qui sont rendues sans intervention humaine. Contrairement à la réglementation européenne, qui établit, à l'art. 22, al. 1, de la DSGVO, une interdiction de principe de l'automatisation assortie d'une réserve d'autorisation et prévoit ainsi une illicéité générale (cf. N. 69 et suivants), le droit suisse semble ainsi admettre la licéité de telles décisions sans conditions particulières. Le renvoi général à l'art. 21 LPD donne l'impression que la LPD sert de norme générale d'admissibilité pour l'adoption de décisions individuelles automatisées dans la procédure administrative suisse. Une telle intention ne peut toutefois être déduite ni du message relatif à la LPD, ni être conciliée avec le principe de légalité (art. 5, al. 1, Cst.). Ce dernier exige, outre une base légale formelle (art. 164, al. 1, Cst.), une précision suffisante de la norme. Certes, la LPD est une loi formelle, mais sa précision semble insuffisante en ce qui concerne les décisions rendues de manière entièrement automatisée. Il est en outre choquant que la disposition ne prévoie aucun domaine d'application concret, mais implique simplement l'existence de décisions individuelles automatisées.

64 À cela s'ajoute le fait que, dans le cadre de la révision totale de la LPD en 2020, d'autres lois ont été complétées par la notion de « décision individuelle automatisée ». La LPD sert ainsi de point de départ à ces renvois dans les lois (de procédure) pertinentes.

VI. APPLICATION

65 La loi prévoit tout d'abord des sanctions pénales. Ainsi, les particuliers sont passibles d'une amende pouvant aller jusqu'à 250 000 CHF s'ils fournissent, par le biais d'une décision individuelle automatisée, des informations erronées, incomplètes ou s'ils omettent de fournir toute information (voir art. 60, al. 1, let. a, LPD). Pour qu'une sanction soit prononcée, il faut qu'une plainte pénale soit déposée dans les délais et qu'il y ait intention délibérée. Le régime des amendes ne s'applique pas aux organes fédéraux.

En outre, la LPD prévoit **des mesures de surveillance**. Ainsi, les violations des obligations prévues à l'art. 21 LPD peuvent être signalées au PFPDT. Dans ce cas, le PFPDT peut obliger le responsable du traitement à fournir les informations à la personne concernée et à lui accorder la possibilité d'exposer son point de vue ou de faire réexaminer la décision individuelle automatisée par une personne physique (voir art. 51, al. 3, let. c, LPD). Cela s'applique de la même manière aux responsables du secteur privé et du secteur public. 66

La LPD ne contient aucune disposition précisant si et comment le responsable du traitement doit **corriger** une décision individuelle automatisée erronée. C'est pourquoi certains lui reprochent de ne pas offrir une protection suffisante et efficace contre les conséquences des décisions individuelles automatisées. Dans le cas spécifique où la violation de l'obligation d'information et d'audition enfreint les principes de traitement prévus à l'art. 6 LPD, on peut y voir un traitement illicite des données par l'organe fédéral (art. 41, al. 1, LPD) ou une atteinte à la personnalité de la part des responsables privés (art. 30 LPD). Dans le contexte des décisions individuelles automatisées, la violation du principe de limitation de la finalité (art. 6, al. 3, LPD) est évidente. En conséquence, la personne concernée est en droit d' d'exiger la suppression des conséquences négatives du traitement illicite des données (voir l'art. 41, al. 1, let. b, LPD pour les organes fédéraux et l'art. 32, al. 2, LPD pour les particuliers). 67

En matière d'application du droit dans le contexte du droit public, la question de savoir quel est le rapport entre le droit à la suppression mentionné ci-dessus et les voies de recours prévues par le droit de la procédure administrative en cas de violation du droit d'être entendu reste **en suspens**. Cette insécurité juridique tient au fait que le droit d'être entendu ou de faire réexaminer la décision, prévu à l'art. 21, al. 2 LPD ne confère pas de droits allant au-delà du droit d'être entendu existant en vertu de l'art. 30, al. 1, PA. La problématique s'accentue lorsque l'action administrative liée à l'adoption d'une décision violant les obligations prévues à l'art. 21 LPD serait qualifiée de traitement illicite de données (cf. art. 41, al. 1, LPD) . Selon la LPD, la personne concernée dispose dans ce cas de la possibilité d'exiger la suppression des conséquences d'un traitement illicite (art. 41, al. 1, let. b, LPD). Cela suggère qu'une décision rendue en violation du droit d'être entendu devrait être annulée en raison d'un traitement illicite de données. Cela remettrait 68

notamment en cause la force de chose jugée des décisions après l'expiration des délais de recours.

VII. REMARQUES DE DROIT COMPARÉ

A. Réglementation européenne (art. 22 de la DSGVO)

69 La DSGVO contient une disposition comparable à l'art. 21 de la LPD. Sous le titre « Décisions individuelles automatisées, y compris le profilage », l'**art. 22, al. 1, de la DSGVO** accorde à une personne concernée le droit de ne pas être soumise à une décision fondée exclusivement sur un traitement automatisé – y compris le profilage – qui produit des effets juridiques à son égard ou qui l'affecte de manière significative de façon similaire.

70 La différence par rapport à l'article 21 de la LPD réside notamment dans l'**approche réglementaire**. Les avis exprimés dans la doctrine juridique concernant l'article 22 de la DSGVO divergent quant à savoir si la disposition européenne interdit en principe les décisions individuelles automatisées ou si elle accorde aux personnes concernées un droit d'opposition. La Cour de justice de l'Union européenne (CJUE) à La Haye part – sans grande justification – d'une interdiction de principe des décisions individuelles automatisées. En comparaison, le libellé de l'article 21, al. 1, de la LPD autorise en principe les décisions automatisées.

71 **L'article 22, al. 2, de la DSGVO** autorise toutefois les décisions individuelles automatisées à titre exceptionnel – et de manière exhaustive – lorsque la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable du traitement (let. a), si elle est autorisée en vertu de dispositions législatives de l'Union ou des États membres auxquelles le responsable du traitement est soumis et que ces dispositions prévoient des mesures appropriées pour garantir les droits et libertés ainsi que les intérêts légitimes de la personne concernée (let. b) ou si elle est prise avec le consentement explicite de la personne concernée (let. c). Dans l'ensemble, la réglementation suisse est donc moins restrictive que la DSGVO.

72 Conformément à l'**art. 22, al. 3, de la DSGVO**, le responsable du traitement prend, dans les cas visés à l'art. 22, al. 2, let. a et c, de la DSGVO, des mesures appropriées afin de préserver les droits et libertés ainsi que les intérêts

légitimes de la personne concernée, ce qui comprend au moins le droit d'obtenir l'intervention d'une personne de la part du responsable du traitement, d'exposer son point de vue et de contester la décision. D'autres exigences relatives à la décision individuelle automatisée découlent d'une multitude d'autres dispositions de la DSGVO, telles que les obligations d'information et le droit d'accès. Sur le fond, le droit européen va au-delà de l'article 21 de la LPD.

Enfin, **l'article 22, al. 4, de la DSGVO** prévoit, contrairement à la réglementation de la LPD, des restrictions particulières pour les données personnelles « nécessitant une protection particulière » (selon la terminologie suisse). 73

B. Casuistique

La LPD introduit la notion de décision individuelle automatisée dans le droit suisse. À ce jour, il n'existe aucune jurisprudence sur ce sujet en Suisse. Même si la LPD (suisse) et la DSGVO (européenne) consacrent des principes différents en matière de recours aux décisions individuelles automatisées – la LPD part du principe de l'admissibilité de telles décisions, tandis que la DSGVO établit une règle d'interdiction assortie d'une réserve d'autorisation (cf. N. 69 et suivants) – et que la pratique de l'UE ne peut donc pas être reprise sans réserve, celle-ci fournit néanmoins des indications pour la Suisse. 74

1. Distinction entre décisions partiellement et entièrement automatisées

L'art. 21 de la LPD contient exclusivement des dispositions relatives aux décisions individuelles entièrement automatisées (cf. N. 20 s.). Les premiers exemples issus de l'espace européen montrent que la distinction par rapport aux décisions partiellement automatisées peut s'avérer difficile. Deux exemples sélectionnés, qui ont fait l'objet d'un examen par la CJUE, sont présentés ci-après à ce sujet. 75

a. Autriche : l'algorithme AMAS

Dans un premier exemple, la mise en œuvre à titre expérimental du « système d'assistance aux opportunités sur le marché du travail » (AMAS) automatisé par le Service autrichien de l'emploi (AMS) a entraîné une discrimination systématique à l'égard des femmes et des personnes en situation de handicap. 76

Le système triait (de manière automatisée) les candidatures correspondant à une offre d'emploi en s'appuyant sur les données issues des dossiers de candidature des vingt dernières années. Les hommes ayant été embauchés plus fréquemment que les femmes par le passé, ces dernières (ainsi que les personnes en situation de handicap) n'étaient tout simplement pas convoquées à un entretien d'embauche. L'autorité autrichienne chargée de la protection des données est intervenue contre cette pratique. En décembre 2020, la Cour administrative fédérale autrichienne a rendu une décision concernant l'AMAS. Cette affaire ne portait pas en premier lieu sur l'interdiction de la discrimination, mais sur la question de la base juridique justifiant l'utilisation de l'AMAS. La réponse à cette question dépendait en fin de compte du fait que la procédure en question soit un processus entièrement automatisé ou partiellement automatisé, car ceux-ci sont soumis à des exigences différentes.

77 Les parties ont avancé les arguments divergents suivants :

Datenschutzbehörde	**Arbeitsmarktservice**
• Die Letztentscheidung werde zwar aufgrund von internen Richtlinien getroffen; diese entfalten allerdings keine Aussenwirkung und damit keine Bindung für die Behörde. • Ausserdem betrage die Beratungszeit für eine Einzelentscheidung regelmässig nur zehn Minuten. Dabei handle es sich nicht um eine eigentliche menschliche Aufsicht, sondern eine routinemässige Übernahme des durch das System vorgeschlagenen Entscheids. • Verfahren: Vollautomatisierung.	• Die Letztentscheidung liege bei einer natürlichen Person, die Richtlinien und Handlungsanweisungen befolgen muss. • Die den Einzelfall bearbeitenden Personen seien entsprechend geschult worden und unterlägen einer Begründungs- und Dokumentationspflicht. Mithin müssen sie sich für jeden Fall Zeit nehmen. • Verfahren: Teilautomatisierung (i.S.e. Entscheidungsempfehlung; angeführt durch die Autorinnen).

78 La juridiction autrichienne a suivi l'argumentation du Service de l'emploi. Elle a estimé que la directive était précise quant au déroulement de la procédure et qu'elle stipulait que la valeur calculée de manière automatisée devait être discutée lors d'un entretien de conseil avec les demandeurs d'emploi. La juridiction a donc qualifié la procédure d'automatisation partielle.

79 Pour la jurisprudence suisse, cela peut constituer une indication selon laquelle, pour distinguer l'automatisation partielle et de l'automatisation complète, le fait qu'une personne physique soit impliquée dans la procédure ne doit pas nécessairement être le critère déterminant. Il convient plutôt de prendre en compte l'ensemble des circonstances propres à chaque cas particulier.

b. Allemagne : l'exemple de la Schufa

La Schufa est un organisme regroupant des établissements de crédit allemands et d'autres entreprises, auprès duquel les cocontractants peuvent obtenir des renseignements sur des emprunteurs potentiels. Elle fournit, sur demande, un score ou une note censé indiquer dans quelle mesure la personne concernée s'acquitte de ses obligations de paiement de manière fiable. 80

Après que certaines personnes en Allemagne eurent intenté une action en justice contre la Schufa, notamment parce que leurs données n'avaient pas été effacées et qu'elles n'avaient pas obtenu l'accès à leurs données, le tribunal administratif de Wiesbaden a saisi la CJUE afin de déterminer si le scoring de la Schufa constituait une décision fondée sur un traitement automatisé – y compris le profilage – au sens de l'article 22 de la DSGVO. 81

La CJUE a statué le 7 décembre 2023 que le scoring de la Schufa relevait de l'article 22 de la DSGVO relatif aux décisions automatisées. Elle a estimé que les trois conditions suivantes, qui doivent être remplies cumulativement en vertu de l'article 22, al. 1, de la DSGVO, étaient réunies : 82

- *Décision :* la CJUE a considéré que le scoring de crédit, en tant que fondement du refus de crédit qui s'ensuit, constituait (également) une décision, d'autant plus que les décisions peuvent également inclure des mesures et que, par conséquent, cette notion doit être interprétée au sens large. Selon la CJUE, une interprétation plus restrictive comporte le risque d'un contournement de l'article 22 de la DSGVO, puisque, par exemple, le calcul du score de crédit ne serait pas soumis aux exigences relatives au traitement de catégories particulières de données à caractère personnel (article 22, al. 4, de la DSGVO).
- *Traitement de données exclusivement automatisé :* cette condition est remplie, d'autant plus que les traitements de données effectués par la Schufa constituent un profilage au sens de l'article 4, point 4 DSGVO et que la valeur de probabilité a en outre été déterminée de manière entièrement automatisée.
- *Effet juridique ou atteinte substantielle :* Étant donné que la Schufa a fondé son action, et donc le refus du crédit, de manière déterminante sur la valeur de probabilité issue de l'évaluation de solvabilité, il y a atteinte substantielle à la personne concernée.

83 Cet arrêt étend l'applicabilité de l'article 22 de la DSGVO au scoring de crédit effectué par la Schufa, qui intervient avant la décision proprement dite de refus du crédit. La CJUE exige toutefois, à titre restrictif, que la décision automatisée de refus du crédit se fonde de manière déterminante sur le scoring de crédit, considéré comme une sorte de décision préliminaire. Les conséquences de cette décision sont d'autant plus importantes que les décisions automatisées au sens de l'article 22, al. 1, de la DSGVO sont, en principe, considérées comme interdites. Une exception ne s'applique que si la décision, conformément à l'al. 2, est :

- nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable du traitement (let. a) ;
- autorisée en vertu du droit de l'Union ou du droit des États membres (let. b) ;
- prise avec le consentement explicite de la personne concernée (let. c).

2. Concernant l'atteinte substantielle au sens de l'article 21, al. 2, de la LPD

84 La question de la gravité de l'atteinte subie par la personne concernée du fait d'une décision individuelle automatisée ne peut être appréciée qu'au regard des circonstances propres à chaque cas. Trois cas survenus aux Pays-Bas permettront d'illustrer quand une atteinte est substantielle ou non.

a. Pays-Bas : le système SyRI

85 En 2014, une loi instaurant le système de lutte contre la fraude SyRI (Systeem Risico Indicatie) a été adoptée aux Pays-Bas. SyRI était un outil algorithmique de détection de la fraude, limité aux quartiers néerlandais dont la population était touchée par la pauvreté ou comptait des minorités, et qui établissait des profils de risque pour des individus afin de détecter différentes formes de fraude – notamment dans les domaines fiscal et des prestations sociales. En 2020, un tribunal néerlandais a ordonné l'arrêt immédiat du programme, au motif qu'il violait la CEDH.

86 Bien que le système ne rendît pas de décision individuelle automatisée, cette affaire illustre clairement les cas dans lesquels il y a manifestement atteinte substantielle. En effet, selon les considérations judiciaires, un tel signalement

de risque a déjà un impact substantiel sur la vie privée de la personne concernée.

b. Tribunal d'arrondissement d'Amsterdam : service de taxi Uber

Une action en justice a été intentée contre le service de taxi Uber pour violation de l'article 22 de la DSGVO, après qu'Uber eut fait bloquer automatiquement les comptes de conductrices et conducteurs soupçonnés d'activités frauduleuses. Étant donné que ceux-ci pouvaient faire réactiver leurs comptes après vérification, le tribunal d'arrondissement a écarté toute violation de l'article 22 de la DSGVO. La suspension temporaire des comptes n'entraînait pas de conséquences graves, à long terme ou durables, comme l'exige l'article 22 de la DSGVO. De plus, les données collectées étaient des données factuelles, telles que la localisation et le trafic, qui sont enregistrées indépendamment du comportement du conducteur. 87

c. Tribunal d'arrondissement d'Amsterdam : application Ola

L'application « Ola » avait imposé à ses utilisateurs des retenues sur le prix du trajet ou des amendes sur la base des données collectées par le système. Le tribunal d'arrondissement a confirmé l'existence d'effets significatifs au sens de l'article 22 de la DSGVO. L'imposition d'amendes a eu des conséquences immédiates et définitives pour les personnes concernées. De plus, des « données de performance » exhaustives, se rapportant au comportement général et continu d'une personne, ont été collectées. 88

3. Enseignements pour le droit suisse

La distinction entre une décision individuelle entièrement automatisée au sens de l'art. 21, al. 1, LPD et une décision partiellement automatisée pourrait s'avérer difficile à établir dans la pratique. La marge de manœuvre décisionnelle humaine dans chaque cas particulier peut constituer un indice. Si celle-ci est importante, il y a lieu de partir du principe qu'il s'agit d'une décision partiellement automatisée. De même, les directives internes à l'administration, la formation des collaborateurs ainsi que la possibilité pour les personnes concernées de faire valoir leurs arguments peuvent constituer des indices de l'existence d'une décision individuelle partiellement automatisée. Dans les deux cas, l'art. 21 LPD n'est pas applicable. En 89

revanche, si une décision est prise par un tiers, il peut tout de même s'agir d'une décision individuelle automatisée au sens de l'art. 21 LPD.

90 De même, il peut s'avérer difficile de tracer une distinction entre les décisions qui entraînent une atteinte considérable et celles qui n'en entraînent pas. Les aspects suivants peuvent servir à la classification :

- *le caractère immédiat de l'impact de la décision sur la personne concernée ;*
- *le caractère temporaire ou définitif de la décision ;*
- *l'influence potentielle de la décision sur le comportement ou la prise de décision de la personne concernée ;*
- *la question de la restriction d'éventuelles sources de revenus ou d'une éventuelle perte financière pour la personne concernée.*

VIII. PERSPECTIVES

91 L'automatisation des processus et des procédures décisionnelles progresse rapidement tant dans le secteur privé que dans le secteur public. Le Conseil fédéral part ainsi du principe que les décisions automatisées seront à l'avenir plus fréquentes. L'article 21 de la LPD oblige les responsables du traitement à informer les personnes concernées des décisions individuelles automatisées et à leur accorder certains droits de protection. Il semble toutefois critique que ces obligations ne s'appliquent qu'aux décisions entièrement automatisées. Les décisions partiellement automatisées (aide à la décision ou contrôle des décisions) ne relèvent pas du champ d'application de la norme. Cela pose problème, car de tels systèmes sont plus répandus dans la pratique et peuvent, selon la complexité de l'algorithme utilisé, avoir une influence considérable sur le résultat de la décision. Il en résulte des lacunes en matière de protection, notamment en ce qui concerne la transparence et la protection des droits fondamentaux. Dans ce contexte, il s'impose d'étendre le champ d'application de l'article 21 de la LPD aux décisions partiellement automatisées. Cette préoccupation a été reprise dans le débat juridique sur l'utilisation des systèmes automatisés. Par ailleurs, la nécessité d'agir a également été prise en compte dans le processus législatif.

BIBLIOGRAPHIE

Alon Barkat Saar/Busuioc Madalina, Human-AI Interactions in Public Sector Decision Making : « Automation Bias » and « Selective Adherence » to Algorithmic Advice, JPART 33 (2023), S. 153 ff.

Alpaydin Ethem, Machine Learning, Cambridge 2016.

Bieri Adrian/Powell Julian, Kommentierung zu Art. 21 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar, Datenschutzgesetz, Zürich 2023.

Bieri Adrian/Powell Julian, Informationspflicht nach dem totalrevidierten Datenschutzgesetz, AJP 12 (2020), S. 1533–1542.

Braun Binder Nadja, Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung, SJZ 115 (2019), S. 467–476 (zit. Künstliche Intelligenz).

Braun Binder Nadja, Als Verfügungen gelten Anordnungen der Maschinen im Einzelfall…–Dystopie oder künftiger Verwaltungsalltag?, ZSR 139 (2020), S. 253–278 (zit. Dystopie).

Braun Binder Nadja, Automatisierte Entscheidungen: Perspektive Datenschutzrecht und öffentliche Verwaltung, SZW 2020, S. 27–34 (zit. Automatisierte Entscheidungen).

Braun Binder Nadja, Staat, Mensch, Algorithmus, BJM 2023, S. 2–19 (zit. Staat).

Braun Binder Nadja, Der Untersuchungsgrundsatz als Herausforderung automatisierter Verfahren, zsis) 2020, abrufbar unter https://www.zsis.ch/artikel/der-untersuchungsgrundsatz-als-herausforderung-vollautomatisierter-verfahren, besucht am 19.3.2026 (zit. Untersuchungsgrundsatz).

Braun Binder Nadja, Algorithmic Regulation – Der Einsatz algorithmischer Verfahren im staatlichen Steuerungskontext, in: Hermann Hill/Joachim Wieland (Hrsg.), Zukunft der Parlamente: Speyer Konvent in Berlin, Berlin 2018, S. 107–120 (zit. Algorithmic Regulation).

Braun Binder et al., Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht, Jusletter vom 28.6.2021 (zit. Handlungsbedarf).

Braun Binder Nadja et al., Einsatz Künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen, Schlussbericht vom 28. Februar 2021 zum Vorprojekt IP6.4, abrufbar unter https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/kanton/digitale-verwaltung-und-e-government/projekte_digitale_transformation/ki_einsatz_in_der_verwaltung_2021.pdf, besucht am 19.3.2026 (zit. Studie 2021).

Braun Binder Nadja/Obrecht Liliane, Algorithmisch überprüfte Steuererklärung im ordentlichen gemischten Veranlagungsverfahren, zsis 2023, abrufbar unter https://www.zsis.ch/artikel/algorithmisch-ueberpruefte-steuererklaerung-im-ordentlichen-verfahren, besucht am 19.3.2026.

Braun Binder Nadja/Thouvenin Florent/Volz Stephanie/Obrecht Liliane, Schutz vor algorithmischer Diskriminierung, Rechtsgutachten, November 2025, abrufbar unter https://www.ekr.admin.ch/pdf/D_Gutachten_Schutz_vor_algorithmischer_Diskriminierung.pdf, besucht am 19.3.2026.

Braun Binder Nadja/Ulbrich Christian, Die grosse Verwirrung – KI und Automatisierung in Staat und Wirtschaft, NZZ 27.4.2023, abrufbar unter https://www.nzz.ch/meinung/die-grosse-verwirrung-ki-und-automatisierung-in-staat-und-wirtschaft-ld.1729694, besucht am 19.3.2026.

Büyüksagis Erdem, Décisions algorithmiques: mieux vaut responsabiliser qu'informer, REAS 2020, S. 225–242 (zit. Décisions algorithmiques).

Büyüksagis Erdem, Responsabilité pour les systèmes d'intelligence artificielle, REAS 2021, S. 12–24 (zit. Responsabilité).

Bull Hans Peter, Verwaltung durch Maschinen, Köln/Berlin 1964.

Christen Markus et al., Wenn Algorithmen für uns entscheiden: Chancen und Risiken der künstlichen Intelligenz, TA-SWISS Studie, April 2020.

Daedelow Romy, Wenn Algorithmen (unfair) über Menschen entscheiden..., Jusletter 26.11.2018.

Dentand Claire, Wer soll entscheiden: Maschine oder Mensch?, Jusletter IT 30.9.2021.

Epiney Astrid, Kommentierung zu Art. 5 BV, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar, Bundesverfassung, 2. Aufl., Basel 2025.

Ernst Christian, Algorithmische Entscheidungsfindung und personenbezogene Daten, JuristenZeitung 21 (2017), S. 1026–1036.

Ernst Hartmut/Schmidt Jochen/Beneken Gerd, Grundkurs Informatik, 8. Aufl., Wiesbaden 2023.

Flueckiger Christian, Kommentierung zu Art. 21 DSG, in: Meier Philippe/Métille Sylvain (Hrsg.), Loi sur la protection des données, Commentaire Romand, Basel 2023.

Glaser Andreas, Einflüsse der Digitalisierung auf das schweizerische Verwaltungsrecht, SJZ 114 (2018), S. 181–190.

Glatthaar Matthias, Robot Recruiting, SZW 2020, S. 43–52.

Gordon Clara-Ann/Lutz Tanja, Haftung für automatisierte Entscheidungen – Herausforderungen in der Praxis, SZW 2020, S. 53–61.

Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich 2020.

Henseler Simon, EuGH C-634/21 – Anträge GA: Kreditscore (der SCHUFA) als automatisierte Entscheidung, https://datenrecht.ch/eugh-c-634-21-antraege-ga-kreditscore-der-schufa-als-automatisierte-entscheidung/, besucht am 12.5.2023 (zit. EuGH).

Henseler Simon, Datenschutz beim Kreditscoring von Auskunfteien: Eine Untersuchung zum Profiling (mit hohem Risiko) und zur automatisierten Entscheidung, Zürich 2025, abrufbar unter https://eizpublishing.ch/wp-content/uploads/2025/09/Datenschutz-beim-Kreditscoring-von-Auskunfteien-Digital-V1_02-20250814.pdf, besucht am 19.3.2026 (zit. Kreditscoring).

Kiener Regina/Rütsche Bernhard/Kuhn Matthias, Öffentliches Verfahrensrecht, 3. Aufl., Zürich 2021.

Konrad Lischka/Anita Klingel, Wenn Maschinen Menschen bewerten, Internationale Fallbeispiele für Prozesse algorithmischer

Entscheidungsfindung, Arbeitspapier, Gütersloh 2017, abrufbar unter https://www.bertelsmann-stiftung.de/doi/10.11586/201702, besucht am 19.3.2026.

Lötscher Cordula, Wenn das Auto den Laster nicht sieht, Jusletter IT 24.11.2016.

Martini Mario, Blackbox Algorithmus: Grundfragen einer Regulierung Künstlicher Intelligenz, Berlin 2019.

Mathys Roland/Reinhart Helen, Bestimmung von Vertragskonditionen im Rahmen automatisierter Entscheidungen, SZW 2020, S. 35–42.

Mehmedovic Senida, Le droit d'accès à une décision individuelle automatisée, Jusletter 19.9.2022.

Meyer Christian, Digitale Formulare als Angelpunkt automatisierter Verwaltungsverfahren, ZSR I 2022, S. 365–383.

Morand Anne-Sophie, Warum das europäische KI-Gesetz auch die Schweiz betrifft, Interview in der Netzwoche mit René Jaun, 10. Mai 2023, abrufbar unter https://www.netzwoche.ch/interviews/2023-05-10/warum-das-europaeische-ki-gesetz-auch-die-schweiz-betrifft, besucht am 19.3.2026 (zit. Interview).

Obrecht Liliane, Verfügung und automatisierte Einzelentscheidung – *same same but different*?, ex/ante, 2022 Nr. 2, S. 38–45.

Pärli Kurt/Flück Nathalie, Kommentierung zu Art. 21 DSG, in Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz (DSG), 2. Aufl., Bern 2023.

Pesapane Filippo/Codari Marina/Sardanelli Francesco, Artificial intelligence in medical imaging: threat or opportunity? – Radiologists again at the forefront of innovation in medicine, EurRadiol Exp 2018, abrufbar unter https://doi.org/10.1186/s41747-018-0061-6, besucht am 19.3.2026.

Plattner Roger, Digitales Verwaltungshandeln, Zürich 2021, abrufbar unter https://suigeneris-verlag.ch/img/uploads/pdf/oa_pdf-021-1633456506.pdf, besucht am 19.3.2026.

Powell Julian/Obrecht Liliane, Regelung automatisierter Einzelentscheidungen im Lichte der KI-Konvention des Europarates, SJZ 122 (2026), S. 287–299.

Prince Anya E.R./Schwarcz Daniel, Proxy Discrimination in the Age of Artificial Intelligence and Big Data, Iowa Law Review 2020, S. 1257–1318.

Räz Tim, COMPAS: zu einer wegweisenden Debatte über algorithmische Risikobeurteilung, Forensische Psychiatrie, Psychologie, Kriminologie 2022, S. 300–306.

Rechsteiner David, Der Algorithmus verfügt, Jusletter 26.11.2018.

David Rosenthal, Der Entwurf für ein neues Datenschutzgesetz, in: Jusletter 27.11.2017 (zit. Entwurf).

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16.11.2020 (zit. nDSG).

Roth Simon, Die automatisierte Einzelentscheidung, digma 2017, S. 104–109.

Škorjanc Žiga, Automatisierte Kreditentscheidungen, CB 2020, S. 70–74.

Schindler Benjamin, Kommentierung zu Art. 5 BV, in: Ehrenzeller Bernhard et al. (Hrsg.), St. Galler Kommentar, Bundesverfassung, 4. Aufl., Zürich/St. Gallen 2023 (zit. SGK).

Schmidt Christoph, Quo vadis, Finanzverwaltung? Potenziale und Herausforderungen eines künftigen behördlichen KI-Einsatzes, Teil I: Entscheidungsunterstützung im Rahmen der hybridgen Fallbearbeitung, REthinking tax, Januar 2022, S. 70–81 (zit. Teil I).

Schmidt Christoph, Quo vadis, Finanzverwaltung? Potenziale und Herausforderungen eines künftigen behördlichen KI-Einsatzes, Teil II: Spezifische Chancen und Problemfelder der vollständigen Entscheidungsautomatisierung im Überblick, REthinking tax, September 2022, S. 31–42 (zit. Teil II).

Stöcklin Fabia, Robot Recruiting, sui generis 2022, abrufbar unter https://sui-generis.ch/article/view/4045/2949, besucht am 19.3.2026.

Styczynski Zbigniew A./Rudion Krzysztof/Naumann André, Einführung und Grundbegriffe der Expertensysteme, in: Styczynski Zbigniew A./Rudion Krzysztof/Naumann André (Hrsg.), Einführung in Expertensysteme, Berlin 2017, S. 1–20.

Thouvenin Florent et al., Positionspapier «Ein Rechtsrahmen für Künstliche Intelligenz», Zürich 2021, abrufbar unter https://www.dsi.uzh.ch/de/research/projects/strategy-lab/strategy-lab-21.html, besucht am 19.3.2026.

Thouvenin Florent/Früh Alfred, Automatisierte Entscheidungen: Grundfragen aus der Perspektive des Privatrechts, SZW 2020, S. 3–17.

Thouvenin Florent/Früh Alfred/George Damian, Datenschutz und automatisierte Entscheidungen, Jusletter 26.11.2018.

Thouvenin Florent/Früh Alfred/Henseler Simon, Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right?, EDPL 2 (2022), S. 183–198.

Thurnherr Daniela, Automatisierte Verwaltungsverfahren auf Bundesebene, in: Braun Binder Nadja/Bussjäger Peter/Eller Mathias (Hrsg.), Auswirkungen auf die Erlassung und Zuordnung behördlicher Entscheidungen, Wien/Hamburg 2021, S. 133–157.

Tsai Chun-Wie/Lai Chin-Feng/Chao Han-Chieh/Vasilakos Athanasios V., Big data analytics: a survey, Journal of Big Data 2015, abrufbar unter https://link.springer.com/article/10.1186/s40537-015-0030-3, besucht am 19.3.2026.

Vasella David/Henseler Simon, Kommentierung von Art. 21 DSG, in Blechta Gabor-Paul/Vasella David (Hrsg.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz, 4. Aufl., Basel 2014 (zit. BSK).

Waldmann Bernhard, Kommentierung zu Art. 29 BV, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar, Bundesverfassung, 2. Aufl., Basel 2025.

Weber Rolf H., Automatisierte Entscheidungen: Perspektive Grundrechte, SZW 2020, S. 18–26 (zit. Grundrechte).

Weber Rolf H., Dürfen Maschinen über Menschen entscheiden?, Eine rechtliche Auslegeordnung im Lichte neuer Technologien, Schweizer Monat 2019, Ausgabe 1063, S. 72–74 (zit. Maschinen).

Weder Regina, Verfahrensgrundrechtliche Anforderungen an automatisierte Verwaltungsverfahren, in: Simmler Monika (Hrsg.), Smart Criminal Justice, Basel 2021, S. 237–262.

Wiederkehr René/Meyer Christian, Schranken, Ausnahmen und Relativierungen des rechtlichen Gehörs: Insbesondere mit Blick auf automatisierte Verwaltungsverfahren, AJP 2022, S. 1092–1108.

Wiederkehr René/Meyer Christian/Böhme Anna, Orell Füssli Kommentar, Bundesgesetz über das Verwaltungsverfahren und weiteren Erlassen, Zürich 2022.

Winkler Markus, Credit Scoring, AML Software & Risk Profiling: Automatisierte Entscheidungen im Rahmen von Finanzdienstleistungen, SZW 2020, S. 62–72.

MATÉRIAUX

Bundesamt für Justiz, Rechtliche Basisanalyse im Rahmen der Auslegung zu den Regulierungsansätzen im Bereich künstliche Intelligenz, August 2024 (zit. BJ, Rechtliche Basisanalyse).

Botschaft zur Änderung des Schwerverkehrsabgabegesetzes und zum Verpflichtungskredit für die Finanzierung eines neuen Systems für die Erhebung der leistungsabhängigen Schwerverkehrsabgabe vom 31. August 2022, BBl 2022 2323 (zit. Botschaft SVAG 2022).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 6941 7192 ff. (zit. Botschaft DSG 2017).

bitkom e.V. - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Entscheidungsunterstützung mit Künstlicher Intelligenz, Berlin 2017, abrufbar unter https://www.bitkom.org/sites/main/files/file/import/171012-KI-Gipfelpapier-online.pdf, besucht am 19.3.2026.

Bundesamt für Justiz, Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2017 (zit. Erläuternder Bericht Vorentwurf DSG).

Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten

bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003, BBl 2003 2101 (zit. Botschaft DSG 2003).

Richtlinien für die Bearbeitung von Personendaten in der Bundesverwaltung vom 16. März 1981, BBl 1981 I 1298 (zit. Richtlinien 1981).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 22 LPD

Un commentaire de Rehana C. Harasgama / Dario Haux

PROPOSITION DE CITATION

Rehana C. Harasgama/Dario Haux, Kommentierung zu Art. 22 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Harasgama/Haux, N. XXX zu Art. 22 DSG.

Art. 22 Analyse d'impact relative à la protection des données personnelles

[1] Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles. S'il envisage d'effectuer plusieurs opérations de traitement semblables, il peut établir une analyse d'impact commune.

[2] L'existence d'un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Un tel risque existe notamment dans les cas suivants:

a. traitement de données sensibles à grande échelle;

b. surveillance systématique de grandes parties du domaine public.

[3] L'analyse d'impact contient une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, ainsi que les mesures prévues pour protéger sa personnalité et ses droits fondamentaux.

[4] Le responsable du traitement privé est délié de son obligation d'établir une analyse d'impact s'il est tenu d'effectuer le traitement en vertu d'une obligation légale.

[5] Le responsable du traitement privé peut renoncer à établir une analyse d'impact lorsqu'il recourt à un système, un produit ou un service certifié conformément à l'art. 13 pour l'utilisation prévue ou qu'il respecte un code de conduite au sens de l'art. 11 remplissant les conditions suivantes:

a. il repose sur une analyse d'impact relative à la protection des données personnelles;

b. il prévoit des mesures pour protéger la personnalité et les droits fondamentaux de la personne concernée;

c. il a été soumis au PFPDT.

TABLE DES MATIÈRES

En bref ... 336
I. Généralités ... 336
A. Aperçu ... 336
B. Historique ... 338
C. Objectif de la norme ... 340
II. Contenu ... 341
A. Destinataires ... 341
B. Le risque élevé ... 342
C. Mise en œuvre de la DSFA ... 345
1. Introduction ... 345
2. Déroulement ... 345
3. Réalisation d'une DSFA commune ... 348
4. Organisation ... 348
D. Exceptions ... 349
III. Violation de l'obligation de procéder à une AIPD ... 351
IV. Défis et pertinence pratique ... 351
V. Comparaison avec le droit de l'UE ... 352
Bibliographie ... 354
Matériaux ... 355

EN BREF

L'art. 22 LPD régit les conditions de réalisation d'une analyse d'impact relative à la protection des données (AIPD). L'article s'inspire des dispositions des art. 35 f. DSGVO. A l'aide de l'analyse des risques en matière de protection des données, une évaluation de ces risques doit être effectuée au préalable lors d'un traitement de données prévu qui entraînera vraisemblablement des risques élevés pour la personnalité ou les droits fondamentaux des personnes concernées. Ainsi, des mesures appropriées pour minimiser les risques doivent être définies et prises avant le début du traitement des données. Selon la loi, il y a notamment un risque élevé en cas (i) de traitement à grande échelle de données sensibles (p. ex. données relatives à la santé) ou (ii) de surveillance systématique à grande échelle de zones publiques (p. ex. installation de caméras de surveillance dans un parc). La liste des risques élevés mentionnés à l'article 22 n'est toutefois pas exhaustive. Typiquement, les risques élevés résulteront de l'utilisation de nouvelles technologies et de nouveaux processus, tels que les systèmes algorithmiques ("intelligence artificielle"), les systèmes DLT ou l'analyse des données volumineuses. Toutefois, l'activité de traitement prévue peut également être considérée comme présentant un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées en raison d'autres facteurs, par exemple parce que des enfants sont concernés, que des décisions individuelles automatisées sont prises ou que des données personnelles sont transmises à un réseau complexe de sous-traitants. La violation de l'obligation prévue à l'article 22 n'est toutefois pas directement punissable.

I. GÉNÉRALITÉS

A. Aperçu

1 Contrairement au RGPD, la LPD révisée ne prévoit pas d'obligation générale de rendre des comptes. Elle introduit toutefois l'obligation d'effectuer une analyse d'impact relative à la protection des données (AIPD) pour les traitements de données présentant des risques élevés, ce qui constitue en fin de compte une obligation de rendre des comptes pour certains traitements de données. L'AIPD est inscrite dans la loi non seulement au niveau fédéral, mais aussi dans de nombreux cantons. A Zurich, par exemple, l'obligation

correspondante figure au § 10 al. 1 de la loi sur la protection des données (IDG), en liaison avec un contrôle préalable (voir le commentaire de l'art. 23 concernant la procédure de consultation préalable au niveau fédéral).

Avec la révision, la DSFA est ancrée dans la loi suisse sur la protection des données pour tous les responsables - pour les responsables privés ainsi que pour les organes fédéraux. C'est pourquoi le libellé de la disposition couvre à la fois les risques élevés pour la personnalité (pour le traitement des données par les responsables privés) et pour les droits fondamentaux (pour le traitement des données par les organes fédéraux) des personnes concernées. L'AIPD sert à identifier et à évaluer à un stade précoce les risques potentiels d'un traitement de données prévu, à définir et à mettre en œuvre des mesures de réduction des risques. Ces démarches doivent être entreprises avant que le traitement de données prévu ne commence (voir le but plus loin, n. 8 ss.). L'application de l'article 22 est une conséquence de l'approche basée sur les risques de la LPD, qui se manifeste de manière particulièrement claire dans la mise en œuvre des articles 22 et 23. 2

Une importance croissante est accordée à la DSFA. Cela est principalement justifié par la diffusion croissante de systèmes algorithmiques avancés ou de nouvelles technologies comparables dans tous les domaines de la vie, comme les technologies de ledger distribué ou l'internet des objets. Nombre de ces applications impliquent des données personnelles et il n'est pas exclu que la personnalité ou les droits fondamentaux des personnes concernées soient exposés à des risques élevés lors de l'utilisation de ces technologies. Dans ces cas, une AIPD est donc nécessaire. Le ou la responsable est encouragé(e) à se pencher préalablement de manière analytique sur le traitement de données prévu. Parallèlement, il convient de noter que certains processus, en particulier dans le cas des systèmes algorithmiques, ne sont guère compréhensibles et que leur potentiel ne peut pas être défini de manière définitive (problématique dite de la "boîte noire"). En conséquence, les données personnelles traitées et les finalités du traitement ne peuvent éventuellement pas être clairement définies et délimitées dans un cas particulier, d'autant plus qu'il est souvent fait appel à de nombreux sous-traitants et autres tiers pour traiter les données et que les analyses de données volumineuses sur lesquelles reposent les systèmes offrent un potentiel encore imprévisible. Dans ces cas, la DSFA peut donc être une "entreprise ambitieuse", mais sa réalisation doit être prise d'autant plus au sérieux. Plus on 3

y parviendra, plus il sera facile de garantir une utilisation fiable et transparente de ces technologies.

B. Historique

4 Avant la révision totale, la LPD suisse ne prévoyait pas explicitement l'obligation pour les personnes privées traitant des données de procéder à une DSFA. Toutefois, les organes fédéraux étaient déjà tenus, sous l'ancienne LPD, de notifier au responsable interne de la protection des données ou au PFPDT les projets ayant pour objet le traitement automatisé de données personnelles (art. 20 al. 2 aLPD). Cette notification était liée à l'obligation pour les autorités fédérales concernées d'élaborer un concept de sécurité et de protection des informations ("concept SIPD") pour le traitement de données prévu. Selon le message, cette procédure était comparable à la DSFA. Pour les responsables privés, la DSFA se fondait dans certains cas sur l'article 7 aDSG. En outre, les principes de traitement des données ont toujours exigé que les conséquences d'un traitement de données soient toujours prises en compte. En outre, dans le cadre de ses conseils, le PFPDT a déjà exigé dans certains cas la présentation d'une AIPD aux personnes privées traitant des données, en particulier lorsqu'il s'agissait de traitements de données à haut risque. L'introduction de l'obligation d'effectuer une AIPD a notamment été motivée par des prescriptions à l'échelle de l'UE conformément à l'art. 8bis P-SEV 108 et à l'art. 27 s. de la directive (UE) 2016/680. L'art. 35 s. CPD prévoit des dispositions analogues. RGPD contient des dispositions analogues pour les responsables de traitement qui entrent dans le champ d'application du RGPD, mais qui n'engagent pas directement la Suisse dans le cadre de la législation.

5 Au niveau international, l'instrument s'appuie sur une longue histoire qui remonte aux années 1990. C'est à cette époque que les premières "Privacy Impact Assessments" ont été développées, tant dans la directive européenne sur la protection des données (art. 20, directive 95/46/CE), qui a été remplacée par le RGPD, que dans les pays anglo-saxons. D'autres États membres de l'UE, comme la France et l'Allemagne, ont émis des recommandations correspondantes sur la base de la directive 95/46/CE. Ces directives non contraignantes visaient à minimiser ou, si possible, à exclure d'emblée les risques éventuels, d'autant plus qu'une telle orientation préventive s'est toujours avérée plus simple et moins coûteuse que l'adaptation des processus, par exemple après coup, en vue d'une enquête par

l'autorité de surveillance compétente. Ces objectifs devaient être atteints notamment par une description des "flux d'informations", l'implication et la discussion avec les "parties prenantes" ainsi que par la rédaction de rapports. On peut en outre citer à titre d'exemple les dispositions de l'ancienne loi fédérale sur la protection des données (aBDSG) en Allemagne, qui prévoyait à l'article 3, al. 9, aBDSG une protection accrue pour des types particuliers de données. Ces données particulières étaient, entre autres, des données relatives aux opinions politiques ou à la santé. Avant que ces données puissent être traitées par des organisations, le délégué à la protection des données compétent devait procéder à ce que l'on appelle un "contrôle préalable" afin de garantir un traitement approprié (§ 4d al. 5 aBDSG).

Le processus législatif en Suisse s'est manifestement rattaché à tous ces développements en prévoyant une DPA dans toutes les versions préliminaires de la LPD totalement révisée. Dans l'avant-projet, l'art. 22 et l'art. 23 LPD y afférent étaient réunis en un seul article 16 AP-LPD. L'art. 16, al. 3, AP-LPD était toutefois plus strict que la disposition actuellement en vigueur. L'article prévoyait que tant le résultat que les mesures prises de chaque AIPD devaient être notifiés au PFPDT. Dans la P-LPD, l'analyse d'impact a ensuite été regroupée en deux articles et adaptée à la structure de l'art. 35 RGPD. La liste des traitements à haut risque, qui impliquent donc obligatoirement la réalisation d'une AIPD, comprenait également le profilage dans le projet (art. 20 al. 2 let. b P-LPD). Dans le texte de loi final, ce processus de traitement a toutefois été retiré de la liste des traitements de données à haut risque sur la base des délibérations parlementaires et en accord avec la systématique législative en vigueur. Cette mesure doit être saluée, d'autant plus que dans de nombreux cas, le profilage ne sera pas considéré comme particulièrement sensible et qu'une AIPD ne serait donc pas justifiée. 6

La DSFA est désormais normalisée à l'article 22 LPD et s'applique aussi bien aux responsables privés qu'aux organes fédéraux. La norme légale va ainsi au-delà de l'obligation qui existait auparavant pour les organes fédéraux en vertu de l'art. 20 al. 2 OLPD et l'élargit. Dans le cadre de la nouvelle norme introduite par la révision totale, il manque - à l'exception de l'art. 14 OLPD sur l'obligation de conservation de deux ans - d'autres dispositions d'exécution qui pourraient simplifier la mise en œuvre dans la pratique. 7

C. Objectif de la norme

8 Le respect des conditions de l'article 22 sert à garantir qu'un traitement de données prévu n'entraîne pas une violation de la LPD. L'AIPD vise à sensibiliser le responsable du traitement aux traitements de données à haut risque, tels que l'utilisation de systèmes algorithmiques ("intelligence artificielle") ou de Big Data Analytics, l'utilisation de logiciels de reconnaissance faciale, l'introduction d'une base de données de patients ou dans le cadre d'un profilage à haut risque. Il s'agit donc d'une "auto-évaluation en matière de protection des données" pour les traitements de données présentant des risques particulièrement élevés. L'article 22 est une émanation des principes de protection des données ainsi que du principe de protection des données par la technique et des paramètres par défaut favorables à la protection des données (article 7). Ainsi, il s'agit dans un premier temps d'identifier les risques et dans un deuxième temps de les évaluer de manière analytique. Le responsable doit alors faire un pronostic sur les conséquences possibles d'un traitement de données prévu pour les personnes concernées. Il s'agit de savoir comment et dans quelle mesure le traitement de données prévu aura un impact sur les personnes concernées. Enfin, la norme vise, sur la base des résultats de l'analyse effectuée, à développer et à mettre en œuvre des mesures appropriées pour (i) atténuer les risques identifiés du traitement de données prévu, (ii) en tirer des conclusions à long terme et (iii) se comporter globalement de manière conforme à la protection des données. Si elle y parvient, la DSFA offre en outre la possibilité de prouver au PFPDT que les prescriptions du droit de la protection des données sont respectées et de réaliser des économies à long terme. Dans ce sens, l'art. 22 exige du responsable qu'il poursuive de manière autonome sa réflexion et qu'il examine les risques qui en résultent par rapport au traitement de données prévu : le traitement de données prévu est-il conforme aux prescriptions de la législation sur la protection des données ? Les principes généraux de protection des données sont-ils respectés ? Le traitement des données est-il proportionné ? La sécurité des données est-elle menacée par le traitement prévu ? Y a-t-il d'autres risques pour la personnalité ou les droits fondamentaux des personnes concernées ? Ces questions doivent être abordées indépendamment de l'importance du risque, ce qui permet au législateur de miser en grande partie sur une "mentalité d'action". Cela doit permettre de réduire les risques liés au traitement des données à un niveau jugé raisonnable.

L'obligation de documentation et de conservation prévue à l'article 14 OLPD complète l'obligation de procéder à une AIPD pour les traitements de données présentant des risques élevés. Ainsi, le responsable du traitement est tenu de documenter le DSFA effectué et de le conserver pendant au moins deux ans après la fin du traitement des données. Ainsi, en cas d'enquête du PFPDT, le responsable est en mesure de justifier le traitement à haut risque des données et de montrer comment les risques élevés sont contrés. Il ressort de cette disposition que la DSFA est une obligation de rendre compte complémentaire, tant vis-à-vis du PFPDT que des personnes concernées. 9

II. CONTENU

A. Destinataires

L'art. 22 s'adresse avant tout à deux acteurs : les organes fédéraux et les responsables privés, puisqu'il s'agit d'évaluer les risques du traitement de données en question par rapport à la personnalité et aux droits fondamentaux des personnes concernées. Les organes fédéraux avaient déjà une obligation similaire dans l'aDSG. Les responsables privés, tout comme les organes fédéraux, sont concernés par cette obligation s'ils tombent dans le champ d'application de la LPD conformément à l'article 3 al. 1. Cela signifie que les responsables privés ayant leur siège à l'étranger sont également soumis à cette obligation, pour autant que leur activité de traitement des données ait des répercussions en Suisse conformément au principe de l'effet et que les autres conditions de l'article 22 soient remplies (voir le commentaire de l'article 3 pour plus de détails sur le principe de l'effet). 10

Les sous-traitants ne sont pas, à juste titre, soumis à l'obligation de procéder à une AIPD, d'autant plus qu'ils traitent les données pour le compte d'un responsable du traitement et que ce dernier décide en principe de la finalité et des moyens d'un traitement de données. L'évaluation des risques ne relève donc en principe pas de leur sphère. Alors que la LPD, contrairement à l'art. 28, al. 3, let. f, RGPD, ne prévoit pas d'obligation d'assistance des sous-traitants envers les responsables lors de la réalisation d'une AIPD, une obligation d'assistance des sous-traitants peut toutefois aller dans leur sens. Dans la pratique, une telle obligation fera souvent partie des accords contractuels entre le responsable du traitement et le sous-traitant. Les principes de protection des données énoncés à l'article 6 imposent toutefois 11

aux sous-traitants de veiller à ce que le traitement des données qui leur est confié soit conforme aux principes de protection des données. Si tel n'est pas le cas, le responsable doit être informé que l'activité de traitement des données doit être adaptée. Le cas échéant, il convient même de proposer la réalisation d'une AIPD.

B. Le risque élevé

12 Al. 22 prévoit que la DSFA doit être effectuée dans tous les cas où il existe un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. En conséquence, il n'est pas nécessaire de procéder à une AIPD pour chaque traitement de données. Cela correspond à l'approche basée sur les risques de la LPD, mais en l'occurrence, ce sont les risques pour les personnes concernées qui sont spécifiquement au premier plan et non les risques qui résultent pour les responsables.

13 Le risque élevé résulte de la nature, de l'étendue, des circonstances et de la finalité du traitement des données. Ces critères sont comparables aux risques qui doivent être pris en compte dans le cadre de la définition des mesures de sécurité des données conformément à l'article 1 al. 3 du RGPD. En ce sens, le risque élevé existe notamment, mais pas exclusivement, lorsque de nouvelles technologies sont utilisées. Plus ces actions et ces fichiers de données sont étendus et sensibles, plus on peut supposer l'existence d'un risque élevé. Le traitement de données prévu doit être examiné, entre autres, sous l'angle de l'impact sur l'identité, l'autodétermination ou la dignité de la personne concernée. Le risque élevé ne doit pas se manifester effectivement : Il s'agit d'identifier et d'évaluer les risques potentiels qui pourraient survenir dans le cadre du traitement des données.

14 Conformément aux let. a et b, il y a risque élevé au sens d'une fiction lorsque (i) des données personnelles sensibles sont traitées à grande échelle (p. ex. lorsque des informations sur le casier judiciaire sont publiées dans un registre public, lors de l'utilisation d'applications de santé qui procèdent à des évaluations des données et établissent des diagnostics ou lors d'essais cliniques) ou (ii) des domaines publics sont surveillés de manière globale et systématique (p. ex. la surveillance d'une aire de jeux ou d'un parc publics ou la surveillance systématique de l'utilisation d'Internet par les collaborateurs). La loi n'énumère pas d'autres traitements de données pour lesquels une AIPD doit obligatoirement être effectuée. En revanche, le RGPD prévoit par

exemple plus largement que les autorités de surveillance doivent publier des listes de traitements de données nécessitant obligatoirement une AIPD.

Selon le libellé de l'art. 22 al. 2, ni le profilage à haut risque ni la prise de décision individuelle automatisée ne sont considérés comme des activités de traitement de données nécessitant obligatoirement une AIPD. Cela semble surprenant à première vue, d'autant plus que le profilage à haut risque implique par définition un risque élevé pour la personne concernée et que les décisions individuelles automatisées entraînent des conséquences juridiques ou d'autres conséquences qui affectent considérablement la personne concernée. Dans ce contexte, le profilage à haut risque doit toujours faire l'objet d'une AIPD. En revanche, la situation est différente et plus complexe pour les décisions automatisées, d'autant plus que la DSFA évalue le traitement des données en tant que tel, ce qui n'est pas nécessairement délicat pour ces décisions individuelles automatisées. Ce qui est délicat ici, c'est avant tout le résultat de la décision, qui est réglé à l'article 21. Une AIPD doit néanmoins être effectuée lorsque le traitement des données qui conduit à la décision individuelle automatisée pourrait en soi entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. 15

Le message énumère d'autres traitements de données susceptibles d'entraîner un risque élevé, notamment en cas de traitement de grandes quantités de données, de transmission de données à des États tiers (dans ce contexte, il convient de mentionner le Data Transfer Impact Assessment ; cf. le commentaire relatif à l'art. 16 s.) ou dans la mesure où un grand nombre de personnes peuvent avoir accès aux données. Dans chaque cas, il faut toutefois toujours vérifier s'il existe effectivement un risque élevé. 16

Ni la LPD ni l'OLPD ne contiennent de prescriptions plus précises concernant la détermination du risque élevé. Il faut donc toujours vérifier, sur la base du traitement de données concrètement prévu, s'il y a lieu de procéder à une AIPD. Les lignes directrices de l'UE peuvent servir d'aide à cet égard. DSGVO prévoient neuf critères selon lesquels un risque élevé peut être déterminé. Dès qu'un traitement de données prévu remplit deux de ces neuf critères, les 17

lignes directrices prévoient l'obligation de procéder à une AIPD. Les neuf critères sont les suivants :

- Évaluation ou classification de personnes ou d'aspects de la personnalité à l'aide de données ;
- Prise de décision automatisée ayant un effet juridique sur les personnes physiques ou un effet similaire ;
- Surveillance systématique ;
- Traitement de données confidentielles ou hautement personnelles ;
- Traitement de données à grande échelle ;
- Comparaison ou fusion de différents ensembles de données, sauf si l'on pouvait s'y attendre ;
- Traitement de données de personnes vulnérables (p. ex. enfants, employés ou patients) ;
- utilisation ou application innovante de nouvelles solutions technologiques ou organisationnelles (p. ex. intelligence artificielle, Big Data Analytics ou technologies basées sur la blockchain), étant donné que leur risque en matière de protection des données n'a souvent pas encore été évalué avec précision ; et
- les cas où le traitement des données empêche les personnes concernées d'exercer un droit ou d'utiliser un service ou d'exécuter un contrat.

Alors que les lignes directrices de l'UE ne sont pas applicables en Suisse, elles peuvent être consultées pour la réalisation d'une AIPD en droit suisse et européen de la protection des données en raison des conditions légales comparables. Il n'est en outre pas exclu que le PFPDT publie des lignes directrices similaires ou qu'il applique par analogie à la Suisse les listes d'opérations de traitement de données des différentes autorités de surveillance de l'UE conformément à l'art. 35 al. 4 RGPD, qui exigent obligatoirement une AIPD. La pratique assurera une plus grande sécurité juridique en ce qui concerne l'évaluation du risque élevé.

C. Mise en œuvre de la DSFA

1. Introduction

L'article 22 donne des indications claires sur les cas dans lesquels le responsable du traitement doit procéder à une DSFA et sur les éléments à prendre en considération lors de la mise en œuvre. Cela inclut le fait que l'évaluation des risques doit être effectuée et documentée de manière structurée. La documentation doit en outre résister à la consultation du PFPDT si, malgré les mesures mises en œuvre, le traitement des données continue d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées (art. 23 al. 1 ; voir à ce sujet le commentaire détaillé de l'art. 23). 18

2. Déroulement

La DSFA doit être effectuée par le responsable du traitement avant le lancement d'une activité de traitement de données nouvelle ou actualisée. Cela permet d'identifier au préalable les risques du traitement de données prévu et de mettre en œuvre les mesures correspondantes avant que des violations de la loi ne se produisent. Le principe est le suivant : le plus tôt sera le mieux. La réalisation initiale unique du DSFA ne suffit toutefois pas. Il est nécessaire de procéder à d'autres tests au cours du projet afin de vérifier si les éventuelles adaptations apportées au traitement des données conduisent à une autre évaluation et si d'autres mesures apparaissent ainsi plus appropriées, voire obsolètes. 19

Sur le plan du contenu, la DSFA suppose trois étapes, définies à l'al. 3. Il s'agit, premièrement, de la phase préparatoire, au cours de laquelle le traitement des données est décrit le plus précisément possible. Deuxièmement, la phase d'évaluation permet d'évaluer les risques et, sur cette base, de prendre des mesures pour gérer ou maîtriser ces risques dans une troisième étape. 20

Avant de procéder à ces trois étapes, les responsables privés devraient toutefois vérifier s'ils sont légalement tenus de traiter les données. S'il existe une obligation légale de traitement, ils sont exemptés de l'obligation d'effectuer une AIPD (article 22, al. 4). En outre, l'autorité fédérale ou le responsable privé devrait d'abord procéder à une évaluation préalable. Il s'agit d'une évaluation générale et plutôt superficielle des risques, destinée à vérifier 21

si le traitement de données prévu peut présenter un risque élevé (cf. risque élevé, n. 12 ss). De cette manière, il est possible de déterminer à l'avance si une AIPD est vraiment nécessaire. Si le responsable conclut que le traitement de données prévu n'entraînera vraisemblablement pas de risque élevé, aucune DSFA n'est nécessaire. Une telle décision devrait toutefois être documentée et conservée à des fins de preuve. Toutefois, si le responsable du traitement conclut, sur la base de cette évaluation préalable, que le traitement de données en question pourrait entraîner un risque élevé, la DSFA doit en principe être effectuée. Il n'y a d'exception que dans les cas visés à l'article 22 al. 5.

22 La phase préparatoire comprend une présentation détaillée de l'activité (prévue) de traitement des données. La loi ne précise ni ce que doit contenir cette description, ni le niveau de détail qu'elle doit atteindre. Selon la complexité de l'activité de traitement des données prévue, la DSFA peut donc être plus ou moins longue. La description devrait toutefois comprendre au moins le type de données traitées et les catégories de personnes concernées, l'exposé de la finalité poursuivie, la durée de conservation, les opérations de traitement, les destinataires ainsi que le lieu de traitement et de conservation. Dans le cas contraire, il n'est pas possible de procéder à une évaluation complète des risques. Cette description doit faire apparaître pourquoi quelles données personnelles doivent être traitées et comment. Dans le cadre de cette description, il convient d'aborder les technologies et les systèmes sous-jacents ainsi que les bases juridiques pertinentes afin de pouvoir, sur cette base, identifier et mettre en œuvre à temps un éventuel besoin d'intervention législative.

23 Vient ensuite la phase d'évaluation, au cours de laquelle la nécessité et la proportionnalité du traitement des données sont mises en relation avec les risques potentiels. Les conséquences négatives du traitement des données pour la personnalité ou les droits fondamentaux de la personne concernée sont ainsi évaluées. Les risques élevés ou les conséquences négatives du traitement des données peuvent se manifester de différentes manières : Ainsi, un traitement de données peut entraîner une atteinte à la réputation ou le traitement de données erronées peut avoir pour conséquence l'établissement de pronostics ou de diagnostics erronés dans le domaine médical. On peut également imaginer des situations dans lesquelles une personne est licenciée de manière injustifiée ou des pertes de confiance vis-à-vis des autorités, du

responsable privé ou des amis et de la famille. En outre, le traitement des données peut également avoir des conséquences financières. La probabilité et la gravité de ces risques et de risques comparables doivent être analysées au cours de la phase d'évaluation.

Lors de l'évaluation des risques, il convient de respecter les principes de protection des données, en particulier ceux de la minimisation des données, de la protection des données par la technique et des paramètres par défaut favorables à la protection des données (voir à ce sujet le point 4). L'autodétermination informationnelle de la personne concernée revêt également une importance particulière, mais pas les intérêts du responsable du traitement. Une pesée des intérêts en vue des mesures à prendre entre les intérêts de la personne concernée (intérêt à la protection des données, intérêt à la liberté de disposer de ses propres données) et ceux du responsable (intérêt au traitement des données) peut toutefois avoir lieu ultérieurement. Bien que les données pertinentes pour l'AIPD ne doivent pas nécessairement être "sensibles", la "nature délicate" des données doit être prise en compte dans le cadre de l'AIPD en question et des mesures à prendre. En conséquence, le nombre ainsi que la sensibilité des données doivent être pris en compte dans cette phase. La phase d'évaluation comprend l'estimation de la gravité des risques et de la probabilité de leur survenance. Bien que cette phase doive permettre d'identifier un risque potentiellement élevé, il se peut que les risques n'apparaissent qu'après la réalisation du DSFA. En ce sens, les trois phases susmentionnées ne peuvent pas être strictement séparées. 24

Après avoir évalué, lors de la phase d'évaluation, si le traitement des données comporte un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, la troisième phase consiste à définir des mesures de réduction des risques. Au cours de cette phase, le responsable doit donc non seulement être conscient des risques existants, mais aussi prendre une décision sur la manière de les contrer. Les mesures peuvent être organisationnelles, techniques, juridiques ou contractuelles. Le responsable doit analyser comment l'activité de traitement des données prévue peut être adaptée afin de réduire le risque élevé à un niveau raisonnable. De telles mesures peuvent être par exemple la limitation des catégories de données, la limitation de l'accès aux données, le cryptage des données, le changement d'un sous-traitant impliqué, le changement du lieu de traitement, l'inclusion de certaines obligations dans les contrats avec des tiers en rapport avec le 25

traitement des données, etc. Ces mesures doivent toutefois être appropriées pour réduire les risques spécifiquement identifiés et ne peuvent pas être appliquées par défaut, c'est-à-dire de manière générale par rapport à tous les risques liés aux activités de traitement des données qui nécessitent une AIPD. Elles doivent être définies au cas par cas.

26 La LPD ne précise pas si la réalisation d'une AIPD doit être unique ou régulière. Cela dépend de l'activité de traitement des données : Si elle est unique, une AIPD effectuée une seule fois suffit. En revanche, si le traitement des données est effectué sur une longue période et que l'évolution des circonstances fait apparaître des risques nouveaux ou plus élevés, la DSFA devrait être répétée. En principe, la DSFA devrait toutefois être répétée tous les trois ans environ. Il reste à voir si cette recommandation fera ses preuves à long terme compte tenu de l'évolution rapide et de l'ampleur croissante des innovations technologiques, mais cela semble peu probable à l'heure actuelle.

27 Sur le plan temporel, il faut également tenir compte du délai de conservation. Conformément à l'article 14 de l'OCPD, la documentation requise pour la DSFA doit être conservée pendant deux ans. Le délai commence à courir à la fin du traitement des données.

3. Réalisation d'une DSFA commune

28 Le responsable du traitement a le droit de procéder à une DSFA commune dans le cas de plusieurs opérations de traitement de données comparables. Cela ne s'applique toutefois que si tant les risques que les contre-mesures sont similaires. Cette possibilité vise à réduire la charge de travail et les coûts pour le responsable du traitement. Il est toutefois douteux que ce droit conduise réellement à un allègement de la charge de travail des responsables ; à moins qu'une plateforme de traitement ou une application donnée ne soit utilisée dans différents secteurs ou projets.

4. Organisation

29 La réalisation d'une AIPD n'incombe pas uniquement à une personne, un service ou une unité spécifique au sein du responsable du traitement. Comme toute autre analyse des risques, il s'agit d'un processus qui doit impliquer plusieurs personnes, services et départements de manière transversale. Au sein d'une entreprise, la DSFA implique généralement la direction du projet, le service informatique et/ou le responsable de la sécurité des informations, le

service ou le conseiller chargé de la protection des données, le service juridique, le service des risques et de la conformité et d'autres personnes clés. Chaque personne impliquée est essentielle pour certaines étapes de la DSFA. Ainsi, le chef de projet est particulièrement important pour la phase préparatoire, car il est le mieux placé pour décrire le traitement (prévu) des données. Le service juridique et de protection des données est chargé d'évaluer les risques conformément à la protection des données et au droit applicable. D'autres départements sont particulièrement pertinents pour déterminer les mesures de réduction des risques. Les sous-traitants qui interviennent dans l'opération de traitement des données prévue doivent également être impliqués dans le cadre de l'AIPD. Comme pour tout projet, il est particulièrement important qu'une personne, un service ou une unité dirige la DSFA et garde une vue d'ensemble de l'ensemble du processus. Cette direction est généralement assurée par le conseiller à la protection des données ou le chef de projet au niveau opérationnel. Les sous-traitants qui interviennent dans l'opération de traitement des données prévue devraient être impliqués dans le cadre de la DSFA.

Du point de vue du responsable, il est donc judicieux de définir un service ou une unité qui connaît les exigences légales en matière de DSFA et qui dispose des connaissances techniques nécessaires pour effectuer une DSFA. Il s'agit généralement du service ou de l'unité responsable de la protection des données. Selon l'orientation ou le modèle d'entreprise des responsables, il peut être utile de créer un modèle, y compris des instructions, pour la réalisation d'une DSFA, auquel on pourra se référer au cas par cas. De cette manière, les exigences légales seront respectées sans que certains aspects soient oubliés. 30

D. Exceptions

En plus de l'obligation générale de procéder à une AIPD dans les cas où un traitement de données entraîne un risque élevé pour les personnes concernées, les al. 4 et 5 définissent certaines exceptions. 31

L'article 22 al. 4, prévoit que les responsables de traitement privés peuvent être exemptés de l'obligation de procéder à une AIPD dans des cas particuliers, à condition qu'ils soient légalement tenus de traiter les données. Au cours du processus législatif, cette exception a été justifiée par le fait que les risques potentiels dans ces cas ont déjà été évalués et qu'il n'est donc pas 32

nécessaire d'aller plus loin dans la réalisation de la DSFA. Il est toutefois souligné à juste titre que l'exception se réfère uniquement à la question de la licéité du traitement des données, et non à la manière dont les données sont traitées. Ainsi, le DSGVO est plus strict à cet égard et exige que l'analyse des risques effectuée dans le cadre de la législation se rapporte à l'activité de traitement concrète pour que l'exception s'applique (voir N. 40). En outre, il faut également tenir compte des cas dans lesquels le traitement des données n'est pas effectué exclusivement pour remplir l'obligation légale en question. Des obligations légales de traitement de données par des personnes privées se trouvent par exemple dans la loi fédérale sur la lutte contre le blanchiment d'argent et le financement du terrorisme (art. 30 LBA) ou la transmission de données de collaborateurs par un employeur pour remplir des obligations relevant du droit des assurances sociales (art. 84 LAMal). Il est évident que les autorités fédérales ne sont pas concernées par cette exception : Elles ne peuvent toujours traiter des données que sur la base d'une base légale.

33 L'art. 22 al. 5 prévoit une autre exception. Selon cette disposition, les responsables privés peuvent renoncer à l'établissement de la DPA si certaines conditions relatives à la certification d'un traitement de données ou au respect de codes de conduite approuvés sont remplies. Ces exceptions ne s'appliquent pas aux autorités fédérales. D'une part, c'est le cas lorsque le responsable utilise un système, un produit ou un service dont l'utilisation est certifiée conformément à l'article 13 (voir à ce sujet le commentaire détaillé de l'article 13 LPD). D'autre part, l'obligation n'est pas applicable dans les cas où le responsable respecte un code de conduite au sens de l'art. 11, (i) qui se fonde sur une AIPD, (ii) qui prend des mesures spécifiques pour protéger la personnalité et les droits fondamentaux des personnes concernées et (iii) qui a été soumis au PFPDT. Actuellement, il n'existe pas de tels codes de conduite en Suisse. On peut toutefois en imaginer pour les branches dans lesquelles les participants à la branche collaborent étroitement et développent ensemble des processus standardisés, comme par exemple dans les banques et les assurances, dans les entreprises technologiques ou médiatiques ou dans la branche publicitaire. Dans l'UE, l'élaboration de codes de conduite ou de règles comparables est régie par l'article 40 du RGPD, et l'on connaît actuellement, entre autres, le Code de conduite de l'UE sur le cloud, qui sert de code de conduite harmonisé pour l'industrie du cloud au sein de l'UE.

III. VIOLATION DE L'OBLIGATION DE PROCÉDER À UNE AIPD

Si un responsable du traitement ne procède pas à la DSFA alors qu'il y serait tenu en vertu de l'article 22, l'article 51 al. 3 let. d, doit être respecté. Selon cet article, le PFPDT peut ordonner, sous peine de sanctions, que le responsable procède à une FISD. En revanche, les personnes concernées n'ont pas le droit d'intenter une action en justice pour obtenir l'exécution de la DSFA. 34

Si le PFPDT constate, dans le cadre d'une enquête, qu'un traitement de données entraîne un risque élevé, il peut ordonner que le traitement des données soit adapté, suspendu ou totalement interrompu jusqu'à ce qu'une AIPD ait été effectuée (art. 51 al. 1 en relation avec l'art. 49 f). Cela peut entraîner des retards considérables pour le responsable, ce qui entraîne à son tour des coûts élevés et des efforts supplémentaires pour le responsable. Comme les résultats d'une enquête peuvent en outre être publiés par le PFPDT (art. 57 al. 2), il existe en outre des risques considérables pour la réputation du responsable. 35

La violation de l'obligation de procéder à une AIPD n'est pas soumise à une amende en tant que telle. Cette réglementation semble judicieuse compte tenu du fait que cette obligation est en premier lieu un devoir de diligence (composé d'une obligation de documentation et de responsabilité). Dans l'UE, on procède différemment (cf. n. 40 ss.). Il faut toutefois partir du principe que les responsables respecteront tout de même leurs obligations conformément à la LPD. D'une part, parce que les autorités devaient déjà tenir compte d'une telle obligation sous l'aDSG. D'autre part, des responsables privés, notamment des groupes, effectuaient également des FDS avant l'entrée en vigueur de la LPD totalement révisée, par exemple parce que le traitement de données concerné relevait du RGPD ou parce que le PFPDT l'avait exigé. 36

IV. DÉFIS ET PERTINENCE PRATIQUE

Avec l'entrée en vigueur de la nouvelle version de l'article 22, il apparaît que les conditions normatives d'une DSFA présentent un degré de complexité élevé. Cela vaut en particulier pour la mise en œuvre par les petites et moyennes entreprises (PME), dont l'importance économique ne doit pas être sous-estimée en Suisse. Pour elles, il pourrait s'avérer difficile de mettre en œuvre les différentes étapes conformément à l'article 22. Cela vaut en 37

particulier pour la phase de préparation et la phase de mesures (voir à ce sujet n. 18 ss.), qui prennent beaucoup de temps, ne serait-ce qu'en raison de la procédure analytique nécessaire. Dans certains cas, cela devrait générer des coûts considérables. Il faut donc s'attendre à ce que le besoin de modèles, de conseils et d'assistance de la part du PFPDT augmente fortement dans un proche avenir. A cet égard, l'obligation des autorités de surveillance européennes de publier des listes définissant les cas dans lesquels une AIPD est obligatoire doit être considérée comme un pas dans cette direction (art. 35, al. 4, RGPD ; cf. n. 43).

38 Avec l'utilisation croissante de systèmes algorithmiques et d'autres applications (voir N. 2), la DSFA va également gagner en importance. Les responsables doivent évaluer précisément, au cas par cas, les risques qui semblent appropriés et si l'utilisation de tels systèmes en vaut la peine. Cette approche analytique avant le lancement effectif du projet ne devrait pas être nouvelle, surtout pour les grandes entreprises, d'autant plus que des Privacy Impact Assessments correspondants ont déjà été réalisés avant la révision totale (voir N. 4 s. et 35) et qu'elles devraient connaître des obligations comparables au niveau de l'UE en vertu du DSGVO.

39 La DSFA montre en outre clairement que dans le domaine des nouvelles technologies de rupture, les différents domaines juridiques se chevauchent et que l'on observe un mélange croissant de questions juridiques et de questions relatives à la technologie utilisée. Les discussions autour de l'Artificial Intelligence Act ("AI Act") sont un exemple de cette évolution. Comme la DSFA prévue à l'article 22 de la LPD, le dernier texte en date repose sur une approche fortement basée sur les risques, qui fait la distinction entre un risque limité, élevé et inacceptable. Ainsi, en particulier pour les applications à haut risque définies dans l'annexe III de l'AI Act, l'article 43 de l'AI Act impose une procédure d'évaluation de la conformité qui s'appuie notamment sur l'annexe VI. Ces prescriptions doivent être comprises, tout comme la DSFA selon la LPD, comme un processus préventif et continu qui comprend des aspects tant juridiques que techniques et qui sert plus largement à la transparence et donc à la confiance des utilisatrices.

V. COMPARAISON AVEC LE DROIT DE L'UE

40 De manière générale, la mise en œuvre de la DSFA selon la LPD est comparable aux prescriptions du DSGVO applicables dans toute l'UE. En

même temps, les art. 22 f. LPD sont moins stricts que les art. 35 f. DSGVO. Dans l'UE, une AIPD doit également être effectuée lorsqu'un traitement de données peut entraîner un risque élevé pour les droits et libertés des personnes physiques. Contrairement à l'art. 22 LPD, l'art. 35 al. 3 let. a RGPD prévoit en outre explicitement une DSFA pour les décisions individuelles automatisées.

Les let. a à d de l'art. 35 al. 7 règlent des étapes comparables à celles de l'art. 22 LPD, qui doivent être prises en compte lorsqu'une DSFA est effectuée. Ainsi, la phase préparatoire est comparable à la let. a, la phase d'évaluation aux let. b et c et la phase de mise en œuvre des mesures à la let. d. Bien qu'en Suisse, il faille également partir du principe qu'une AIPD doit éventuellement être effectuée à nouveau dans le cadre du traitement des données en raison de l'évolution des circonstances, l'art. 35 al. 11 RGPD le prévoit même explicitement dans certains cas. 41

Alors que l'art. 35 al. 2 RGPD implique une obligation de consulter le délégué à la protection des données ("Data Protection Officer"), du moins si un tel délégué a été désigné, l'art. 35 al. 9 RGPD prévoit même que le responsable peut consulter les personnes concernées lors de la mise en œuvre de la DSFA. La LPD ne contient pas une telle disposition. La consultation du délégué à la protection des données n'a aucune influence sur le contenu de l'AIPD, d'autant plus que le rôle du délégué à la protection des données n'est pas concrétisé. Par contre, le fait de recueillir le point de vue des personnes concernées a pour objectif la transparence de la part du responsable du traitement ainsi que l'autodétermination des personnes concernées. Ces consultations renforcent le sens et l'objectif de la DSFA en montrant une fois de plus que les risques à évaluer sont ceux du traitement des données pour les personnes concernées et donc pas en premier lieu des risques pour le responsable. 42

Contrairement à la Suisse, l'art. 35 al. 4 RGPD impose aux autorités de contrôle de tenir une liste des opérations de traitement pour lesquelles une AIPD doit être effectuée dans tous les cas (listes dites positives). En substance, le législateur européen établit ainsi une obligation de fait de procéder à une AIPD dans les cas définis par les autorités de contrôle. En outre, les autorités de contrôle sont autorisées à tenir des listes facultatives d'activités de traitement des données pour lesquelles une AIPD n'est pas nécessaire (listes dites négatives ; art. 35 al. 5 RGPD). Ces listes sont soumises à la procédure de 43

cohérence si elles comprennent "des activités de traitement liées à l'offre de biens ou de services aux personnes concernées ou à l'observation de leur comportement dans plusieurs États membres, ou qui sont susceptibles d'affecter de manière significative la libre circulation des données à caractère personnel au sein de l'Union" (art. 35 al. 6 RGPD). La LPD ne prévoit pas d'obligation de tenir des listes positives ou négatives, bien que cela contribuerait à la sécurité juridique.

44 Alors que l'art. 22 al. 5 LPD stipule explicitement qu'il n'est pas nécessaire de procéder à une AIPD si un code de conduite au sens de l'art. 11 LPD est respecté et si les conditions supplémentaires énoncées à l'al. 5 sont remplies, de tels codes de conduite ne doivent, selon le RGPD, être pris en compte dans l'AIPD que dans le cadre de l'évaluation des effets du traitement de données concerné. Elles ne dispensent toutefois pas le responsable du traitement de l'obligation d'effectuer une DSFA si celle-ci est légalement obligatoire.

45 Enfin, l'art. 35 al. 10 RGPD prévoit, à l'instar de l'art. 22 al. 4 LPD, qu'il n'est pas nécessaire de procéder à une AIPD lorsqu'un traitement de données repose sur une base légale. L'exception prévue par le DSGVO est toutefois plus restrictive : L'exception ne s'applique que si une DSFA a été effectuée dans le cadre de l'adoption de la base juridique et si la base juridique régit le ou les traitements concrets. L'importance pratique devrait donc être limitée. En outre, il existe une exception selon l'art. 35 al. 10 RGPD, dans la mesure où le traitement des données est effectué dans l'intérêt public ou dans l'exercice de l'autorité publique.

46 Le RGPD prévoit des amendes allant jusqu'à 10 millions d'euros ou jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent en cas de violation de l'obligation de procéder à une AIPD (art. 83 al. 4 let. a RGPD). Cette amende est contraire à la LPD, qui ne prévoit pas d'amende pour une telle violation (cf. N. 35).

BIBLIOGRAPHIE

Baeriswyl Bruno, Der «grosse Bruder» DSGVO und das revDSG: Ein vergleichender Überblick, S. 8–15.

Blonski Dominika, Kommentierung zu Art. 22 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Aufl., Zürich/Basel, 2023

Blonski Dominika, DSFA und Vorabkonsultation, digma 2020, S. 28–32.

Früh Alfred/Haux Dario, Foundations of Artificial Intelligence and Machine Learning, Weizenbaum Series 29, DOI: 10.34669/WI.WS/29.

Klaus Samuel, KI trifft Datenschutz – Risiken und Lösungsansätze, in: Epiney Astrid/Rovelli Sophia, Künstliche Intelligenz und Datenschutz, Zürich 2021, S. 81–95.

Lobsiger Adrian, Hohes Risiko – kein Killerargument gegen Vorhaben der digitalen Transformation, SJZ 2023, S. 311–319.

Pfaffinger Monika, Das Recht auf informationellen Systemschutz. Plädoyer für einen Paradigmenwechsel im Datenschutzrecht, Habil., Baden-Baden 2022.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16. November 2020.

Schönbächler Matthias R., Zum neuen Schweizer Datenschutzrecht, ZBJV 2023, S. 171–195.

Schürmann Kathrin, Datenschutz-Folgenabschätzung beim Einsatz Künstlicher Intelligenz: Bewertung und Minimierung der Risiken, ZD 2022, S. 316–321.

Vasella David, Widersprüche im Datenschutzrecht, digma 2020, S. 174–179.

Vasella David/Sievers Jacqueline, Der «Swiss Finish» im Vorentwurf des DSG, digma 2017, S. 44–49.

Widmer Michael, Datenschutz-Folgenabschätzung, digma 2017, S. 224–231.

Kühling Jürgen/Benedikt Buchner, Datenschutz-Grundverordnung BDSG, Kommentar, 3. Aufl., München, 2020.

Rosenthal David/Gubler Seraina, Die Strafbestimmungen des neuen DSG, SZW/RSDA 2021, S. 52–64.

MATÉRIAUX

Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017, S. 6941 ff., abrufbar unter: https://fedlex.data.admin.ch/eli/fga/2017/2057, besucht am 5.6.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 23 LPD

Un commentaire de Rehana C. Harasgama / Dario Haux

PROPOSITION DE CITATION

Rehana C. Harasgama/Dario Haux, Kommentierung zu Art. 23 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Harasgama/Haux, N. XXX zu Art. 23 DSG.

Art. 23 Consultation préalable du PFPDT

[1] Le responsable du traitement consulte le PFPDT préalablement au traitement lorsque l'analyse d'impact relative à la protection des données révèle que, malgré les mesures prévues par le responsable du traitement, le traitement envisagé présente encore un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

[2] Le PFPDT communique au responsable du traitement ses objections concernant le traitement envisagé dans un délai de deux mois. Ce délai peut être prolongé d'un mois lorsqu'il s'agit d'un traitement de données complexe.

[3] Si le PFPDT a des objections concernant le traitement envisagé, il propose au responsable du traitement des mesures appropriées.

[4] Le responsable du traitement privé peut renoncer à consulter le PFPDT s'il a consulté son conseiller à la protection des données au sens de l'art. 10.

TABLE DES MATIÈRES

En bref ... 360
I. Généralités ... 360
A. Aperçu ... 360
B. Historique ... 360
C. But de la norme ... 361
II. Contenu ... 362
A. Destinataires ... 362
B. Traitement "planifié ... 362
C. Consultation ... 363
1. Introduction ... 363
2. Informations à fournir ... 364
3. Procédure du PFPDT ... 365
4. Délai ... 367
D. Exceptions ... 367
III. Violation de l'obligation de consulter le PFPDT ... 369
IV. Défis et pertinence pratique ... 369
V. Comparaison avec le droit de l'UE ... 370
Bibliographie ... 372
Matériaux ... 372

EN BREF

L'article 23 est le corollaire de l'article 22. Si, dans le cadre d'une AIPD, le responsable du traitement constate qu'il existe un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, malgré les mesures prises pour atténuer le risque, une consultation du PFPDT est nécessaire. Les conditions, les délais et les conséquences de cette consultation sont énumérés et spécifiés. Le PFPDT examine le traitement de données prévu sous l'angle du respect de la LPD. Le PFPDT exprime ses objections au traitement de données prévu dans une prise de position qui contient également des recommandations sur les mesures possibles. Cet avis est transmis au responsable du traitement. Le PFPDT peut également exercer ses compétences selon les articles 49 et 51 et suivants après la consultation selon l'article 23. Une violation de l'obligation découlant de l'art. 23 n'est toutefois pas punissable.

I. GÉNÉRALITÉS

A. Aperçu

1 L'art. 23 décrit les conditions de la consultation du PFPDT. Il s'agit d'une procédure étroitement liée à l'analyse d'impact relative à la protection des données (AIPD) prévue à l'article 22. Si, au cours d'une AIPD, le responsable constate que le traitement de données prévu présente encore un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, malgré les mesures prises, le PFPDT doit être consulté au préalable. Dans ce cas, le PFPDT examine la compatibilité du traitement de données prévu avec le droit de la protection des données ainsi qu'avec les conditions de sécurité de l'information. Le PFPDT communique ensuite ses objections au responsable du traitement dans un délai de deux à trois mois en prenant position. Le PFPDT est alors tenu de proposer des mesures appropriées pour faire face aux risques identifiés.

B. Historique

2 L'obligation de procéder à une AIPD et de consulter le PFPDT lorsque le traitement de données prévu entraîne un risque élevé pour les personnes

concernées malgré les mesures prises n'existait pas avant la révision totale de la LPD. Cette obligation n'existait pas non plus pour les autorités fédérales qui devaient effectuer une AIPD conformément à l'art. 22 aDSG. La Convention européenne sur la protection des données (STE 108+) n'exige pas non plus l'introduction de cette obligation. Cependant, certaines lois cantonales sur la protection des données prévoyaient déjà cette obligation, par exemple dans le canton de Zurich à l'art. 10 IDG ou dans le canton de Berne à l'art. 17a KDSG.

La possibilité ou la nécessité de la consultation se fonde toutefois sur des dispositions du droit européen datant de 2008, notamment l'article 20 de la directive 95/46/CE, selon lequel les traitements présentant certains risques pour les personnes, notamment en ce qui concerne les droits et les libertés, doivent déjà être examinés au préalable par le délégué à la protection des données. Cette réglementation se retrouve encore aujourd'hui à l'art. 28 de la directive 2016/680/UE en vigueur, qui a dû être transposée en Suisse en raison de l'acquis de Schengen dans le domaine de la prévention, de la recherche, de la détection ou de la poursuite transfrontalières d'infractions pénales ou de l'exécution de peines, ainsi qu'à l'art. 36 du RGPD, qui a été transposé de manière comparable. 3

L'AP-LPD prévoyait à l'art. 16 al. 3 AP-LPD une notification au PFPDT des résultats de la DPA dans tous les cas. Conformément à la réglementation actuelle, le PFPDT devait communiquer ses objections au responsable du traitement dans un délai déterminé. L'obligation d'informer dans tous les cas le PFPDT des résultats d'une DSFA a été fortement critiquée lors de la consultation publique. Le Conseil fédéral a alors atténué cette obligation en introduisant l'art. 21 al. 1 P-LPD. Cette norme atténuée a été reprise dans la réglementation actuelle de l'art. 23 al. 1 en ce sens que le PFPDT ne doit être consulté que si, malgré les mesures prises, des risques élevés pour la personnalité ou pour les droits fondamentaux de la personne concernée subsistent. 4

C. But de la norme

Selon le message, l'obligation de consulter a été introduite dans le cadre de la révision totale en 2020 "parce qu'elle permet au préposé d'agir à titre préventif et de conseiller". Selon lui, c'est la solution la plus efficace pour le responsable, car les problèmes potentiels liés à la protection des données peuvent être identifiés et adressés à un stade précoce. La consultation permet 5

au PFPDT d'obtenir et d'évaluer les informations nécessaires pour évaluer un traitement de données prévu présentant un risque élevé. Cela favorise également le processus démocratique.

6 Le but de l'art. 23 est en outre de développer des solutions avant la mise en œuvre d'un projet prévoyant des traitements de données correspondants. Cela permet d'assurer d'emblée un niveau élevé de protection des données et de garantir la sécurité des informations. Le législateur vise ainsi à adopter un comportement proactif afin de réduire au minimum, voire d'exclure, dès le départ, les éventuelles violations de la loi. En outre, il sert à protéger le responsable a posteriori - lorsqu'un traitement de données a déjà commencé - contre des efforts et des coûts supplémentaires. Cela semble également judicieux compte tenu du fait qu'il est souvent difficile d'éliminer les dommages et les blessures après coup. Dans l'ensemble, cet article s'inscrit donc dans l'approche basée sur les risques de la LPD totalement révisée.

II. CONTENU

A. Destinataires

7 Les destinataires de l'article 23 sont, comme à l'article 22, les autorités fédérales et les responsables privés. Les sous-traitants n'en font pas partie. En ce qui concerne le rôle de ces sous-traitants, on peut se référer au commentaire correspondant de l'art. 22.

8 Les autorités fédérales et les responsables privés sont donc tenus de consulter le PFPDT lorsqu'un traitement de données prévu entraîne, malgré les mesures mises en œuvre, un risque élevé pour la personnalité et les droits fondamentaux des personnes concernées. Le PFPDT est quant à lui tenu de procéder à la consultation conformément à la LPD et de respecter les délais en vigueur (cf. n. 25).

B. Traitement "planifié

9 Le texte normatif de l'art. 23 prévoit à l'al. 1 que la consultation du PFPDT doit avoir lieu en cas de traitement planifié présentant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Cette disposition ne s'applique que si le responsable a déjà prévu des mesures pour

atténuer les risques qui en découlent et que le traitement des données présente néanmoins un risque élevé.

Alors que le texte laisse supposer qu'il ne peut s'agir que de nouveaux traitements de données planifiés, cette disposition englobe également les modifications de traitements de données ou de procédures déjà existants (voir à ce sujet le commentaire relatif à l'art. 69). Cela signifie que le PFPDT doit être consulté chaque fois qu'il y a des modifications dans le processus de traitement des données ou des changements dans les circonstances de fait ou de droit. Ces changements de circonstances doivent toutefois permettre de conclure ou d'établir clairement qu'il existe un risque élevé au sens de l'article 22. En outre, les mesures prises dans le cadre d'une nouvelle analyse des données personnelles ou d'une analyse répétée ne doivent pas suffire à réduire ce risque élevé. En ce qui concerne la notion de risque élevé, on peut se référer aux explications relatives à l'art. 22 (art. 22, n. 12 ss). Le fait que, dans un environnement aussi disruptif et marqué par des changements rapides, les responsables doivent toujours intégrer les risques dans leurs propres réflexions et planification des traitements de données afin de ne pas mettre en danger ou violer concrètement les droits des personnes concernées (cf. art. 7) plaide en faveur de l'appréciation selon laquelle le PFPDT doit également être consulté en cas de modifications des activités de traitement de données existantes. 10

C. Consultation

1. Introduction

Pour commencer, l'article 23 présuppose que le responsable du traitement a effectué une AIPD concernant un traitement de données prévu ou modifié conformément à l'article 22. Si le responsable arrive à la conclusion que, malgré les mesures prévues, le traitement des données présente un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, il doit consulter le PFPDT. Bien que la loi ne prévoie aucune exigence de forme, cette consultation devrait se faire par écrit, ne serait-ce que pour des raisons de preuve. Si ce risque élevé n'existe pas, le responsable peut néanmoins soumettre volontairement la DSFA au PFPDT. Bien que cela soit utile à la sécurité du droit et de l'information, les responsables privés devraient régulièrement y renoncer (cf. n. 34 ss). 11

12 La consultation doit être effectuée avant le début du traitement de données concerné. Ce n'est qu'une fois la consultation terminée, c'est-à-dire après que le PFPDT a pris position, que l'autorité fédérale ou le responsable privé peut commencer le traitement des données.

13 Trois points relatifs à la consultation doivent être pris en compte au préalable :

- Premièrement, la consultation est payante pour les responsables privés (voir art. 59 al. 1 let. c LPD ; art. 44 OLPD). Les coûts respectifs dépendent des frais de personnel dans le cas particulier. En revanche, il n'y a pas de frais pour les organes fédéraux.
- Deuxièmement, le PFPDT peut à son tour s'adresser au responsable du traitement et demander une évaluation des risques et une consultation s'il a connaissance d'opérations de traitement prévues.
- Troisièmement, le PFPDT peut lier cette demande à l'exécution d'actes d'enquête (cf. n. 23).

2. Informations à fournir

14 La disposition de l'art. 23 détermine les cas dans lesquels le PFPDT doit être consulté. Elle ne définit toutefois pas les informations qui doivent être fournies au PFPDT pour son évaluation. Compte tenu de cette situation initiale, il faut s'attendre, ou il a déjà été annoncé, que le PFPDT lui-même établira, peu de temps après l'entrée en vigueur, des directives correspondantes auxquelles le responsable pourra se référer. Toutefois, le responsable devrait au moins veiller à ce que les documents élaborés dans le cadre de la DSFA soient disponibles dans leur intégralité, afin que le PFPDT puisse émettre un avis sur cette base. Ces documents devraient donc contenir entre autres des informations sur le traitement prévu - y compris, le cas échéant, la finalité du traitement -, sur les risques éventuels pour la personnalité ou les droits fondamentaux de la personne concernée ainsi que sur les mesures techniques et organisationnelles prévues. Il convient également d'expliquer pourquoi le risque est toujours considéré comme élevé malgré les mesures décrites. Cela est important car, dans le cas contraire, aucune consultation ne serait nécessaire.

Le DSGVO peut servir de guide à cet égard, car il contient une liste des informations à fournir (voir N. 39). Il peut également être utile de procéder selon l'approche dite SIPD. Celui-ci prévoit une description aussi précise que possible du projet, y compris une présentation de la situation juridique ainsi que des mesures organisationnelles et techniques. Lors de la description du projet, il est prévu de fournir des informations sur le service responsable et le service traitant les données, la finalité et le type de traitement des données ainsi que les destinataires et les personnes concernées. En revanche, la description des aspects organisationnels et techniques suppose une présentation des applications, des réseaux, des technologies ainsi que des rôles et des concepts d'autorisation. Il convient de noter que dans certains cas, des concepts détaillés ou des plans de mesures peuvent être demandés. 15

En outre, les documents remis doivent être structurés et munis de son propre nom et d'une adresse de contact. Cela permet de communiquer avec le PFPDT si, dans un cas particulier, des questions se posent ou si d'autres clarifications sont nécessaires. 16

3. Procédure du PFPDT

Lorsque les documents correspondants ont été remis dans leur intégralité (cf. n. 15 ss), le PFPDT procède généralement en trois étapes (i)-(iii) : Dans un premier temps, les informations soumises sont examinées et il est vérifié si des informations, documents ou autres données supplémentaires sont nécessaires pour clarifier la situation. Si c'est le cas, ces informations sont demandées au responsable (i). Ensuite, les documents sont soigneusement examinés et analysés afin de déterminer s'ils sont compréhensibles et pertinents (ii). La troisième étape consiste à clôturer la procédure, à communiquer les éventuelles objections et à proposer des mesures à prendre (iii). Dans le cadre de ces trois étapes, le PFPDT évalue si les mesures proposées sont suffisantes pour garantir la protection de la personnalité et des droits fondamentaux de la personne concernée et pour atténuer le risque élevé. 17

Dans la première étape, le PFPDT examine les informations fournies par le responsable du traitement et s'assure qu'il comprend le processus de traitement des données. Il s'agit en particulier de la description factuelle et technique du traitement de données en question. Si le PFPDT a besoin d'informations supplémentaires, il les demande et, le cas échéant, demande à discuter oralement du traitement de données prévu avec le responsable afin 18

de clarifier des questions spécifiques. Il convient de noter que le texte de la loi ne précise pas si le délai imparti au PFPDT pour prendre position ne commence à courir qu'après cette étape ou directement lors du dépôt de la demande de consultation. Selon le point de vue défendu ici, le délai pour prendre position ne commence toutefois à courir qu'après la remise complète de toutes les informations demandées par le PFPDT. Cela signifie que la durée de la consultation peut donc être plus longue que ces deux ou trois mois, selon les informations et documents supplémentaires demandés par le PFPDT.

19 C'est sur cette base que commence l'examen proprement dit du traitement de données en question. Lors de cette deuxième étape, le PFPDT examine en particulier l'évaluation des risques et les mesures proposées par le responsable. Cette évaluation comprend la vérification des conditions légales, dont fait partie en premier lieu le respect des principes de protection des données. Outre la proportionnalité (mots-clés : minimisation et évitement des données), il s'agit notamment des éventuelles bases légales ou contractuelles ou des motifs de justification du traitement des données, de l'externalisation du traitement des données ou de la communication de données à l'étranger, de la sécurité des données ainsi que de la garantie des droits des personnes concernées, notamment le droit d'accès ainsi que le droit de rectification et d'effacement des données. Il convient de prendre en compte aussi bien la sensibilité des données que les parties impliquées et leurs responsabilités. Les mesures techniques et organisationnelles sont également examinées. Cela se fait en relation avec les technologies utilisées et, le cas échéant, avec les fournisseurs qui se trouvent derrière. A l'heure où les cyberattaques et les piratages informatiques se multiplient, cela contribue à la sécurité de l'information.

20 Après avoir examiné ces aspects en profondeur, le PFPDT rédige en principe, dans une troisième étape, une prise de position à l'attention du responsable. Dans cet avis, il énumère ses observations concernant le traitement de données prévu et propose une évaluation tant du point de vue juridique que du point de vue technique et organisationnel. S'il conclut que le traitement des données est conforme à la protection des données, il n'y a pas d'autres conditions à remplir par le responsable. Dans ce cas, le PFPDT n'émet pas non plus de recommandations. Dans un tel cas, il peut même s'abstenir d'envoyer un avis au responsable. Lorsque le PFPDT émet des objections, il

les accompagne de propositions de mesures concrètes (cf. art. 22 n. 26.). Ces mesures visent à garantir à la fois le respect de la protection des données et la sécurité de l'information. En règle générale, le PFPDT fixera un délai au responsable pour la mise en œuvre de ces mesures.

Dans ce cadre, il convient de tenir compte d'un cas particulier : Si, suite au traitement de données effectué, le PFPDT arrive à la conclusion que les mesures n'étaient pas suffisantes ou qu'il n'existe aucune mesure pour réduire les risques identifiés, il est habilité à mener une enquête (art. 49). Le PFPDT dispose à cet effet de toutes les mesures administratives prévues à l'art. 51. L'enquête peut donc avoir pour conséquence, entre autres, une suspension, voire une interdiction du traitement des données. Bien que l'on puisse partir du principe que le PFPDT ne prendra en règle générale des décisions formelles que dans des cas isolés, la loi lui laisse explicitement cette possibilité lorsque les responsables ne gèrent pas les risques de manière appropriée. 21

Il convient en outre de souligner que l'avis du PFPDT est une recommandation non contraignante. Il n'a pas le caractère d'une décision et ne peut donc en aucun cas être considéré comme une approbation ou une autorisation d'effectuer le traitement de données prévu. 22

4. Délai

Dans la mesure où le PFPDT est consulté, il doit, conformément à l'art. 23 al. 2, communiquer son avis au responsable du traitement dans un délai de deux mois à compter de la remise du dossier complet au PFPDT. Le PFPDT peut prolonger ce délai d'un mois au maximum s'il s'agit d'un traitement de données complexe. Si le responsable ne reçoit pas de communication du PFPDT dans ce délai, il faut partir du principe que le PFPDT ne s'opposera pas au traitement de données prévu. 23

D. Exceptions

L'art. 23 prévoit quelques exceptions à l'obligation de principe de consulter. Ces exceptions sont régies par l'al. 4 et ne s'appliquent qu'aux responsables privés. Les autorités fédérales ne sont donc pas concernées par ces exceptions. 24

25 L'al. 4 stipule qu'une consultation n'est pas nécessaire si le responsable consulte un conseiller à la protection des données en ce qui concerne le traitement de données prévu. Il ressort du message que le conseiller à la protection des données doit effectivement être activement impliqué dans la DSFA. Il doit donc avoir été en mesure de se prononcer de manière exhaustive sur les mesures et les risques. Dans ce contexte, il semble judicieux de régler de manière exhaustive le déroulement d'une DSFA ainsi que les compétences et l'intervention du conseiller à la protection des données dans des directives ou instructions internes.

26 Selon le message, l'exception vise à réduire la charge administrative du côté des responsables privés. D'un point de vue économique, cette exception est à saluer. En effet, du point de vue des responsables privés, elle permet d'éviter les retards, les coûts supplémentaires et les conséquences potentiellement négatives de la consultation du PFPDT. Le PFPDT s'était certes prononcé contre cette exception dans le cadre de la consultation, mais elle a finalement été intégrée dans le texte de loi.

27 L'exception doit en outre être interprétée comme une incitation pour les responsables privés. Ainsi, la réglementation leur offre une raison très spécifique de désigner un conseiller à la protection des données. Cette incitation est importante, car contrairement à l'article 37 du RGPD, la nomination d'un conseiller à la protection des données est toujours facultative selon la LPD.

28 L'exception ne s'applique toutefois que si les conditions de l'art. 10 al. 3 sont remplies. En conséquence, le conseiller à la protection des données doit être indépendant sur le plan professionnel, ne pas être lié par des instructions, être libre de tout conflit d'intérêts et disposer des connaissances techniques nécessaires (voir le commentaire relatif à l'art. 10 pour plus de détails sur ces conditions). En revanche, le responsable doit publier les coordonnées du conseiller à la protection des données et les communiquer au PFPDT. Cette exception rappelle celle en vigueur sous l'art. 11a al. 5 let. e aDSG concernant l'obligation de déclarer les fichiers, qui a été supprimée de la LPD sans être remplacée. Les responsables privés sont donc déjà parfaitement familiarisés avec ces conditions.

29 Les responsables privés qui développent ou utilisent des modèles commerciaux ou des technologies susceptibles d'entraîner des risques élevés

pour les personnes concernées désigneront, selon l'expérience, un conseiller à la protection des données et feront usage de cette exception. Cela leur permettra d'éviter de consulter le PFPDT. On peut d'autant plus le supposer que les responsables privés actifs au niveau international dans de tels secteurs sont de toute façon déjà tenus de nommer un responsable de la protection des données en vertu du DSGVO.

III. VIOLATION DE L'OBLIGATION DE CONSULTER LE PFPDT

Dans le cas où un responsable ne consulte pas préalablement le PFPDT malgré l'obligation prévue à l'art. 23, l'art. 51 al. 3 let. e prévoit que le PFPDT peut ordonner, sous peine de sanction, que le responsable le consulte préalablement. En revanche, les personnes concernées n'ont pas le droit d'intenter une action en justice pour obtenir la consultation du PFPDT. 30

Si le PFPDT constate, dans le cadre d'une enquête, qu'un traitement de données entraîne un risque élevé, il peut décider d'adapter, de suspendre ou d'interrompre complètement le traitement des données. Ceci est valable jusqu'à ce qu'une DSFA ait été effectuée et que le PFPDT ait été consulté (art. 51 al. 1 en relation avec l'art. 49 f). Cette étape peut entraîner des retards considérables et donc des coûts élevés et des efforts supplémentaires pour le responsable. Comme les résultats d'une enquête peuvent en outre être publiés par le PFPDT (art. 57 al. 2), des risques de réputation sont en outre à prévoir dans de tels cas. 31

La violation de l'obligation de consulter le PFPDT n'est toutefois pas soumise à une amende en soi. Cela semble logique, d'autant plus qu'il s'agit d'un devoir de diligence et que le PFPDT a les compétences correspondantes (voir à ce sujet les explications à l'art. 22, n. 37). Dans l'UE, une amende est prévue dans ces cas. 32

IV. DÉFIS ET PERTINENCE PRATIQUE

La pertinence pratique de l'article 23 reste à voir. Ainsi, les responsables privés au moins tenteront de se soustraire dans une large mesure à l'obligation en adaptant le traitement de données prévu jusqu'à ce qu'il n'entraîne plus de risque élevé pour les personnes concernées dans le cadre des mesures prises. Il faut donc partir du principe que le PFPDT ne sera consulté que dans des 33

cas exceptionnels. Il y a d'autres raisons à cela : D'une part, les responsables privés ne voudront pas attendre jusqu'à trois mois avant de recevoir une évaluation de leur traitement de données et de pouvoir poursuivre leur projet. D'autant plus que l'on peut supposer que ce délai ne commence à courir que lorsque le PFPDT a reçu du responsable toutes les informations qu'il juge nécessaires. Dans certains cas, cela pourrait avoir pour conséquence que les projets doivent être interrompus beaucoup plus longtemps. Les projets peuvent alors aussi concerner des processus et des faits importants pour les affaires qui, dès qu'ils sont soumis au PFPDT, pourraient être rendus publics. Cela peut être le cas lorsque le PFPDT doit rendre compte de la DSFA dans son rapport d'activité ou lorsqu'il est obligé de divulguer certaines informations en vertu de la LTrans. On ne peut pas toujours répondre à cela par le fait que le PFPDT s'engage à garder le secret. Enfin, conformément à l'art. 59 al. 1 let. c LPD, la consultation du PFPDT est payante pour les responsables privés, selon un tarif horaire de 150 à 250 CHF (art. 44 al. 2 OLPD), ce qui, dans le cadre de processus de traitement de données complexes, devrait représenter un coût non négligeable. Les frais peuvent être multipliés par deux si la consultation du PFPDT peut être réutilisée à des fins commerciales (art. 44 al. 3 et 4 OLPD). Ces coûts s'ajoutent aux coûts propres qu'une AIPD engendre de toute façon chez un responsable privé.

34 Dans les cas où un traitement de données fait l'objet d'une publicité et que le PFPDT, en raison de cette publicité ou de la pression politique qui en découle, adresse par exemple une demande au responsable ou mène une enquête, les responsables privés devraient, comme par le passé, être obligés de procéder à une AIPD par voie d'ordonnance (cf. art. 51, al. 2, let. d et art. 49). De telles ordonnances prévoient probablement aussi une obligation de consulter le PFPDT pour ce processus de traitement de données particulier.

V. COMPARAISON AVEC LE DROIT DE L'UE

35 Le RGPD prévoit à l'art. 36 al. 1 l'obligation de consulter l'autorité de contrôle compétente dans la mesure où un traitement de données pourrait, malgré les mesures prises, entraîner des risques élevés pour les personnes concernées. A cet égard, la réglementation est identique à l'art. 23 al. 1 LPD.

36 Comme à l'art. 23 al. 2 LPD, l'autorité de surveillance compétente doit, conformément à l'art. 36 al. 2 RGPD, communiquer dans un délai de huit semaines au responsable du traitement ainsi que, le cas échéant, aux sous-

traitants impliqués, les objections au traitement de données prévu. De telles objections peuvent résulter du fait que l'autorité de contrôle arrive à la conclusion que le responsable "n'a pas suffisamment identifié le risque ou ne l'a pas suffisamment circonscrit". En revanche, le délai peut être prolongé de six semaines et non d'un mois seulement à compter de la réception de la demande. Une telle prolongation de délai doit être communiquée au responsable dans un délai d'un mois et doit en outre être motivée. L'autorité de contrôle peut suspendre ces délais jusqu'à ce qu'elle ait reçu les informations nécessaires conformément à l'art. 36 al. 3 DSGVO. Les dispositions de l'UE sont donc plus détaillées que celles de la Suisse et semblent judicieuses, d'autant plus qu'elles règlent de manière plus détaillée le processus et les obligations des autorités de surveillance en matière de délais.

Si l'autorité de contrôle a des objections, elle doit transmettre des recommandations écrites au responsable du traitement et, le cas échéant, aux sous-traitants impliqués, ce qui ressemble beaucoup à la réglementation suisse, bien qu'en Suisse, le destinataire de l'avis soit en principe le responsable du traitement. L'autorité de surveillance a en outre expressément le droit d'exercer les autres compétences que lui confère l'article 58 du RGPD. La LPD ne le mentionne pas explicitement. 37

Alors que l'art. 23 LPD ne contient pas de dispositions détaillées sur les informations que les responsables doivent fournir au PFPDT dans le cadre de la consultation, l'art. 36 al. 3 RGPD contient une liste des informations à fournir : Informations sur les responsabilités du responsable, des responsables conjoints et, le cas échéant, des sous-traitants, les finalités et les moyens du traitement de données envisagé, les mesures et les garanties prévues pour la protection des droits et libertés des personnes concernées [conformément au RGPD], le cas échéant les coordonnées du délégué à la protection des données, l'analyse d'impact relative à la protection des données en tant que telle et toute autre information demandée par l'autorité de contrôle. 38

L'art. 36 al. 4 et 5 RGPD régit ensuite certains droits et obligations des États membres ainsi que des exigences supplémentaires que les États membres peuvent prévoir dans leur droit local. 39

Le non-respect de l'obligation de consulter l'autorité de contrôle, tout comme l'obligation d'effectuer une DSFA, est sanctionné par le RGPD. Ainsi, le RGPD 40

prévoit des amendes allant jusqu'à 10 millions d'euros ou jusqu'à 2% du chiffre d'affaires annuel total réalisé dans le monde au cours de l'exercice précédent en cas de violation de l'obligation de consultation (art. 83 al. 4 let. a RGPD). Ceci est contraire à la LPD qui ne prévoit pas d'amende pour ces cas (cf. N. 33).

BIBLIOGRAPHIE

Blonski Dominika, Kommentierung zu Art. 23 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Aufl., Zürich/Basel, 2023.

Kasper Gabriel, People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, Zürich 2021.

Lobsiger Adrian, Hohes Risiko – kein Killerargument gegen Vorhaben der digitalen Transformation, SJZ 2023, S. 311–319.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16. November 2020.

Kühling Jürgen/Buchner Benedikt, Datenschutz-Grundverordnung BDSG, Kommentar, 3. Aufl., München, 2020.

MATÉRIAUX

Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017, S. 6941 ff., abrufbar unter: https://fedlex.data.admin.ch/eli/fga/2017/2057, besucht am 5.6.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 25 LPD

Un commentaire de Martin Steiger

PROPOSITION DE CITATION

Martin Steiger, Kommentierung zu Art. 25 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Steiger, N. XXX zu Art. 25 DSG.

Chapitre 4 Droits de la personne concernée

Art. 25 Droit d'accès

[1] Toute personne peut demander au responsable du traitement si des données personnelles la concernant sont traitées.

[2] La personne concernée reçoit les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la présente loi et pour que la transparence du traitement soit garantie. Dans tous les cas, elle reçoit les informations suivantes:

a. l'identité et les coordonnées du responsable du traitement;

b. les données personnelles traitées en tant que telles;

c. la finalité du traitement;

d. la durée de conservation des données personnelles ou, si cela n'est pas possible, les critères pour fixer cette dernière;

e. les informations disponibles sur l'origine des données personnelles, dans la mesure où ces données n'ont pas été collectées auprès de la personne concernée;

f. le cas échéant, l'existence d'une décision individuelle automatisée ainsi que la logique sur laquelle se base la décision;

g. le cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles sont communiquées, ainsi que les informations prévues à l'art. 19, al. 4.

[3] Des données personnelles sur la santé de la personne concernée peuvent lui être communiquées, moyennant son consentement, par l'intermédiaire d'un professionnel de la santé qu'elle aura désigné.

[4] Le responsable du traitement qui fait traiter des données personnelles par un sous-traitant demeure tenu de fournir les renseignements demandés.

[5] Nul ne peut renoncer par avance au droit d'accès.

[6] Le responsable du traitement fournit gratuitement les renseignements demandés. Le Conseil fédéral peut prévoir des exceptions, notamment si la communication de l'information exige des efforts disproportionnés.

[7] En règle générale, les renseignements sont fournis dans un délai de 30 jours.

TABLE DES MATIÈRES

En bref ... 376
I. Généralités ... 376
A. Objectif ... 376
B. Historique ... 377
II. Droit d'accès (al. 1) ... 378
III. Contenu des renseignements (al. 2) ... 380
IV. Cas particuliers ... 383
A. Renseignement par un professionnel de la santé (al. 3) ... 383
B. Traitement par des personnes travaillant sur mandat (al. 4) ... 383
V. Modalités ... 384
A. Pas de renonciation au droit d'accès (al. 5) ... 384
B. Gratuité des renseignements (al. 6) ... 384
C. Délai pour l'information (al. 7) ... 385
VI. Application du droit ... 385
Bibliographie ... 386

EN BREF

L'art. 25 LPD régit le droit d'accès des personnes concernées en tant que "pilier du droit de la protection des données". Toute personne concernée peut exiger des responsables qu'ils lui indiquent si des données personnelles la concernant sont traitées. Le droit d'accès est strictement personnel. Les personnes concernées ne peuvent pas renoncer à l'avance à leur droit d'accès. L'information doit comprendre toutes les données nécessaires pour que la personne concernée puisse faire valoir ses droits et comprendre le traitement des données. Le contenu minimal du renseignement est défini par la loi. Les renseignements doivent être fournis sous une forme compréhensible, en principe gratuitement et dans un délai de 30 jours. En cas de traitement par un sous-traitant, le responsable du traitement reste tenu de fournir les informations. Les personnes concernées disposent de différentes possibilités juridiques pour faire valoir leur droit d'accès.

I. GÉNÉRALITÉS

A. Objectif

1 Le chapitre 4 "Droits des personnes concernées" comprend le droit d'accès (art. 25 ss LPD) et le droit à la remise ou à la transmission des données introduit par la LPD (art. 28 s. LPD ; également : droit à la portabilité des données). Le droit d'accès peut être déduit de l'art. 13 Cst. sur la "protection de la sphère privée" ainsi que de l'art. 8 CEDH sur le "droit au respect de la vie privée et familiale" et constitue un "pilier du droit de la protection des données". Le droit d'accès doit donc également figurer expressément dans les clauses de protection des données d'un contrat (art. 16 al. 2 let. b LPD) et dans les garanties spécifiques (art. 16 al. 2 let. c LPD) en cas de communication de données personnelles à l'étranger.

2 Le droit d'accès est un droit essentiel pour les personnes concernées qui leur permet, dans certaines limites, de savoir quelles données les concernant sont traitées, par qui et dans quel but. Le droit d'accès doit notamment permettre aux personnes concernées de vérifier si leurs données sont traitées conformément aux principes de la protection des données (art. 6 ss LPD). Le droit d'accès doit donc avoir une fonction de contrôle et un effet préventif.

Le droit d'accès permet aux personnes concernées d'exercer leur droit à l'autodétermination en matière d'information, si et dans la mesure où un tel droit a été mis en œuvre dans la LPD. Le droit d'accès et les renseignements fournis en conséquence constituent souvent la base de l'exercice d'autres droits juridiques des personnes concernées, tels que la rectification et l'effacement (art. 32 et 41 LPD) ou l'opposition (art. 30 al. 2 let. b LPD), en fin de compte pour faire valoir la protection de la personnalité. 3

Le droit d'accès selon les art. 25 ss. LPD complète le devoir d'information selon les articles 19 et suivants et va plus loin dans son contenu. Les personnes concernées peuvent obtenir des renseignements qui vont au-delà de ce que le responsable est tenu d'informer, ce qui accroît la transparence. 4

Les trois articles relatifs au droit d'accès sont structurés comme suit : L'art. 25 LPD détermine qui peut demander des informations et quelles informations les responsables doivent fournir et dans quel cadre. L'art. 26 LPD précise les conditions dans lesquelles le droit d'accès peut être limité. L'art. 27 LPD définit les conditions dans lesquelles le droit d'accès peut être encore limité dans le contexte des médias. Dans le règlement sur la protection des données, les articles 16 à 19 de l'OLPD concrétisent le droit d'accès. 5

B. Historique

L'article 25 se fonde sur l'ancien article 8 aDSG. Par rapport à l'art. 8 aLPD, les personnes peuvent demander des renseignements à tous les responsables (art. 5 let. j LPD) et non plus seulement au "maître d'un fichier" (art. 3 let. i en relation avec l'art. 8 al. 1 aLPD). Dans l'ensemble, les dispositions actuelles relatives au droit d'accès selon les articles 8 aDSG et suivants ont été conservées et complétées par endroits. 6

L'obligation de renseigner - qui, du point de vue du responsable, est la contrepartie du droit d'accès des personnes concernées - n'est plus limitée à certaines informations (c'est notamment le cas de l'art. 8, al. 2, aDSG), mais les informations nécessaires pour que la personne concernée puisse faire valoir ses droits conformément à la LPD et pour garantir un traitement transparent des données doivent être communiquées (art. 25, al. 2, LPD). Parallèlement, on tente de limiter l'utilisation abusive du droit d'accès à des fins de recherche de preuves, qui était "courante sous l'aDSG". Lors des débats parlementaires, il a en outre été ajouté en particulier que les renseignements doivent être 7

fournis sur "les données personnelles traitées en tant que telles" (art. 25 al. 2 let. b LPD).

II. DROIT D'ACCÈS (AL. 1)

8 L'art. 25 al. 1 LPD statue sur le droit d'accès de manière générale. Toute personne physique peut exiger qu'un responsable lui indique si des données personnelles (art. 5 let. a LPD) la concernant sont traitées. Les personnes privées responsables et les organes fédéraux responsables sont tenus de fournir des renseignements (art. 5 let. j LPD). Il n'est en principe pas nécessaire de motiver les renseignements demandés ou de justifier d'un intérêt à les obtenir par voie juridique. Pour les organes fédéraux, la communication de renseignements est une décision au sens de l'art. 5 PA, ce qui implique une motivation et l'indication des voies de recours conformément à l'art. 35 PA.

9 Le droit d'accès est de nature strictement personnelle et se limite à l'accès à ses propres données. Le droit d'accès n'est pas transmissible et n'est pas héréditaire. Pour les personnes incapables de discernement, c'est le représentant légal qui agit (art. 19c al. 2 CC).

10 La personne concernée qui demande des informations doit se faire identifier par le responsable du traitement par des mesures appropriées et collaborer à la preuve de son identité (art. 16 al. 5 RGPD). Il convient d'évaluer au cas par cas si l'identification par la copie d'une pièce d'identité officielle est appropriée. L'obligation prévue à l'art. 1 al. 1 aLPD, selon laquelle la personne concernée doit justifier de son identité, n'existe plus. Selon les données disponibles sur une personne, les indications figurant sur une pièce d'identité officielle ne sont pas appropriées pour l'identification. Dans le cas des plateformes Internet, par exemple, les responsables ne connaissent souvent que l'adresse électronique ou un numéro de téléphone mobile. Dans ce cas, l'identification peut se faire par ce biais. La demande générale d'une copie de pièce d'identité, éventuellement même certifiée conforme, violerait les principes de nécessité, de proportionnalité et de finalité de la protection des données (art. 6 al. 2, 3 et 4 LPD).

11 La demande d'une personne concernée visant à savoir si des données la concernant sont traitées doit en principe être faite par écrit (art. 16 al. 1 phrase 1 RGPD). Le ou la responsable peut également permettre des demandes

d'accès orales (art. 16, al. 1, 2e phrase, RGPD). Le droit d'accès est ainsi potentiellement aménagé de manière un peu plus accessible. La voie électronique est assimilée à la voie écrite (art. 16 al. 3 RGPD). La forme écrite comprend toute forme qui permet d'en apporter la preuve par un texte.

L'information sur les données traitées se fait par écrit ou sous la forme sous laquelle les données sont disponibles (art. 16 al. 2 phrase 1 RGPD). La voie électronique est assimilée à la voie écrite (art. 16 al. 3 RGPD). Le ou la responsable peut proposer une consultation sur place, à laquelle la personne concernée ne doit toutefois pas consentir (art. 16, al. 2, 2e phrase, RGPD). Avec l'accord de la personne concernée, le ou la responsable peut également fournir l'information oralement (art. 16, al. 2, 3e phrase, RGPD). En cas de consultation sur place, il existe un droit à des copies. Lors de la communication des renseignements, les données personnelles de la personne concernée doivent être protégées contre l'accès de tiers non autorisés (art. 8 LPD). Le ou la responsable peut répondre sous la même forme que la personne concernée a demandé des renseignements, par exemple au moyen d'un courriel non crypté de bout en bout. Le cryptage des e-mails est souvent étranger à la pratique et n'est pas approprié. Une alternative au courrier électronique peut être la messagerie instantanée avec un cryptage standard de bout en bout, par exemple avec Signal, Threema ou WhatsApp, pour autant que la personne concernée qui demande des renseignements utilise un tel service de messagerie instantanée. 12

En ce qui concerne la voie électronique, comme en particulier l'utilisation du courrier électronique, il convient de noter qu'une demande de renseignements ou des renseignements fournis par voie électronique sans accusé de réception peuvent, le cas échéant, ne pas être considérés comme notifiés. La charge de la preuve incombe à l'expéditeur. Dans le cas des plateformes Internet, il peut être proposé de traiter les demandes de renseignements et la communication de renseignements par le biais de la plateforme. Les personnes concernées sont toutefois libres de demander des renseignements par écrit. 13

Les informations doivent être fournies sous une forme compréhensible pour la personne concernée (art. 16 al. 4 RGPD). L'intelligibilité, par exemple en cas de format inhabituel ou difficilement lisible des données, peut être garantie par des explications appropriées. Selon le texte, l'intelligibilité concerne la forme et non le contenu des informations. 14

III. CONTENU DES RENSEIGNEMENTS (AL. 2)

15 Le renseignement doit contenir, au sens d'une clause générale selon l'art. 25 al. 2 LPD, les informations nécessaires pour que la personne concernée puisse faire valoir ses droits conformément à la LPD et pour garantir un traitement transparent des données. Si aucune donnée personnelle n'est disponible, un renseignement négatif doit être fourni.

16 Indépendamment de cela, l'art. 25 al. 2 LPD définit une liste minimale d'informations qui doivent être communiquées aux personnes concernées : Identité et coordonnées du ou de la responsable (let. a, par analogie avec l'art. 19 al. 2 let. a LPD), données personnelles traitées en tant que telles (let. b), finalité du traitement (let. c, par analogie avec l'art. 19 al. 2 let. b LPD), durée de conservation ou, si cela n'est pas possible, critères de détermination de la durée de conservation (let. d), informations disponibles sur l'origine des données personnelles (source), si elles n'ont pas été collectées auprès de la personne concernée, car dans ce cas, la personne concernée a déjà été informée conformément à l'art. 19 f. LPD (let. e), l'existence et la logique d'une éventuelle décision individuelle automatisée selon l'art. 21 LPD (let. f) et les éventuels destinataires (let. f, par analogie avec l'art. 19 al. 2 let. c LPD). La question de savoir dans quelle mesure les informations non énumérées ne doivent être communiquées par le ou la responsable que sur demande ou si une mention de telles informations doit être faite dès le début est controversée.

17 En ce qui concerne le ou la responsable selon l'art. 25 al. 2 let. a, il peut arriver que l'on ne sache pas qui est responsable, le cas échéant avec d'autres (art. 5 let. j LPD). L'identité et les coordonnées doivent être mentionnées ou, si elles sont déjà connues, confirmées. Celui qui reçoit une demande d'accès devra - également au regard de la clause générale - informer la personne concernée s'il n'y a pas de responsabilité exclusive ou si aucun renseignement ne peut être fourni en l'absence de responsabilité. En cas de responsabilité commune, la communication des informations doit être coordonnée entre les responsables, les personnes concernées devant toujours pouvoir demander des informations à un ou plusieurs responsables en Suisse, ce qui est particulièrement important dans le cas d'éventuels autres responsables à l'étranger. En cas de pluralité de responsables, chacun d'entre eux est tenu de fournir des informations (art. 17, al. 1, RGPD). S'il n'y a pas de responsabilité, notamment en cas de traitement par des sous-traitants (art. 8 LPD), la

demande de renseignements doit être transmise au responsable ou au moins mentionner le responsable. La charge de la preuve qu'un renseignement qualifié d'exhaustif l'est effectivement incombe au ou à la responsable. Les responsables ne voudront normalement pas donner l'impression que l'information fournie est complète et ne sont pas non plus tenus d'en donner confirmation.

Conformément à l'art. 25 al. 2 let. b, seules les données personnelles traitées doivent être fournies en tant que telles, c'est-à-dire, par exemple, pas les documents individuels, les e-mails, les notes ou les contrats dans leur ensemble, mais uniquement les données personnelles qu'ils contiennent. Les documents dans leur ensemble peuvent être fournis volontairement, ce qui, dans la pratique, peut être plus simple pour le ou la responsable en fonction des données. Le droit d'accès ne peut porter que sur des données personnelles traitées qui sont couvertes par la LPD (art. 2 al. 2 LPD), donc par exemple pas sur des données personnelles traitées par des personnes physiques exclusivement pour leur usage personnel (art. 2 al. 2 let. a LPD e contrario). En cas de traitement d'une grande quantité de données, le ou la responsable peut demander des précisions à la personne concernée. 18

Seules les "données écrites ou "physiquement" disponibles, et donc objectivement consultables à long terme [...], et non pas simplement accessibles de mémoire", peuvent être communiquées. "Le mode de stockage ou la désignation des données ne sont pas pertinents". 19

Le droit d'accès aux données concernant des personnes décédées, prévu à l'article 1, al. 7 aLPD, n'a pas été repris dans la LPD ou dans l'OLPD. Cette disposition a été qualifiée en dernier lieu de contraire au droit fédéral par la jurisprudence. 20

Ce qui est considéré comme une donnée personnelle au sens du droit d'accès doit être évalué au cas par cas, notamment en ce qui concerne le critère de déterminabilité (art. 5 let. a LPD). La clause générale est à la fois un critère et une restriction : "En matière de droit de la protection des données, il s'agit uniquement d'aider une personne concernée à pouvoir faire valoir ses droits en matière de protection des données (au moins les droits qui peuvent être invoqués en justice) et de garantir une transparence du traitement des données (motivée par le droit de la protection des données)". Le droit d'accès 21

ne doit notamment pas être un moyen d'obtenir des preuves (cf. n. 7 ci-dessus).

22 Le but du traitement (art. 25 al. 2 let. c) correspond à celui prévu par le devoir d'information (art. 18 al. 2 let. b LPD).

23 La durée de conservation ou, si la communication d'une durée n'est pas possible, les critères de détermination de cette durée (art. 25 al. 2 let. d LPD) peuvent être tirés par les responsables d'un éventuel registre des activités de traitement existant (art. 12 al. 2 let. e LPD). Comme critère, il faudra au moins se référer au principe de nécessité (art. 6 al. 4 LPD).

24 En ce qui concerne l'origine selon l'art. 25 al. 2 let. e LPD, il n'est pas possible d'exiger du ou de la responsable des éclaircissements sur l'origine des données.

25 En présence d'une décision individuelle automatisée, l'art. 25 al. 1 let. f LPD exige d'une part des renseignements sur ce fait et d'autre part sur la logique sur laquelle repose la décision. L'existence en soi devrait en principe déjà être connue de la personne concernée en raison du devoir d'information en cas de décision individuelle automatisée (art. 21 al. 1 LPD ; exceptions selon l'art. 21 al. 3 LPD). La logique, c'est-à-dire les critères et les données sous-jacentes, doit être réclamée par la personne concernée en faisant référence à son droit d'accès. Les algorithmes peuvent être protégés en tant que secrets commerciaux, mais les hypothèses de base de la logique de l'algorithme doivent être mentionnées. Dans le cas de l'"intelligence artificielle", le droit d'accès se heurte à des limites à cet égard, car le ou la responsable ne sait souvent pas (et ne peut pas non plus savoir) quelles données personnelles ont conduit au résultat visible et pourquoi.

26 Pour les éventuels destinataires selon l'art. 25 al. 2 let. g, il suffit de communiquer les catégories. Les catégories sont par exemple les autorités ou les sociétés du groupe, alors que les noms ne doivent pas être mentionnés. S'y ajoute l'information sur la communication à l'étranger selon l'art. 19 al. 4 LPD.

IV. CAS PARTICULIERS

A. Renseignement par un professionnel de la santé (al. 3)

Pour les données personnelles relatives à la santé, l'art. 25 al. 3 LPD prévoit qu'elles peuvent être communiquées, avec le consentement de la personne concernée, par un professionnel de la santé désigné par elle. Les données relatives à la santé sont des données personnelles sensibles au sens de l'art. 5 let. c ch. 2 LPD. 27

Cette disposition correspond dans une large mesure à l'art. 8 al. 3 aDSG. Le consentement requis a été complété afin de permettre à la personne concernée de choisir librement. Les renseignements ne peuvent plus être fournis uniquement par des médecins, mais par tous les professionnels de la santé qualifiés pour le cas en question. Doivent notamment être considérées comme des professionnels de la santé les personnes médicales inscrites au registre des professions médicales (MedReg). 28

B. Traitement par des personnes travaillant sur mandat (al. 4)

En cas de traitement de données personnelles par des sous-traitants (art. 9 LPD), le responsable du traitement reste soumis à l'obligation de renseigner. Cette disposition correspond à la première phrase de l'actuel art. 8 al. 4 aDSG, dont la deuxième phrase a été supprimée sans être remplacée. 29

Un sous-traitant qui reçoit une demande d'information sans être responsable doit transmettre la demande d'information au responsable ou au moins indiquer le responsable. Conformément à l'art. 17 al. 2 OLPD, les personnes chargées du traitement des commandes doivent aider le ou la responsable à fournir les renseignements, dans la mesure où elles n'ont pas été mandatées pour le faire. Le ou la responsable devra régler la communication des renseignements dans le contrat conclu avec le ou la sous-traitant(e) (contrat de sous-traitance) (art. 9 al. 1 let. a LPD). 30

V. MODALITÉS

A. Pas de renonciation au droit d'accès (al. 5)

31 Conformément à l'art. 25 al. 5 LPD, il n'est pas possible de renoncer à l'avance au droit d'accès. Cette disposition correspond à l'art. 8 al. 6 aDSG.

B. Gratuité des renseignements (al. 6)

32 Conformément à l'art. 25 al. 6 LPD, les renseignements doivent en principe être fournis gratuitement. La disposition partielle correspondante de l'art. 8, al. 5 aDSG ("en règle générale [...] gratuitement") a ainsi été reprise. Le droit d'accès part du principe que la communication de renseignements est en règle générale possible sans grand effort lorsque le traitement des données est conforme à la loi et à l'ordonnance.

33 Le Conseil fédéral reçoit la compétence de prévoir des exceptions à la gratuité, "notamment lorsque les coûts sont disproportionnés". Le Conseil fédéral a fait usage de cette compétence avec l'article 19 OLPD.

34 En cas de charge de travail disproportionnée, la communication des renseignements peut exceptionnellement être subordonnée à une participation aux frais appropriée pouvant aller jusqu'à 300 francs (art. 19 al. 1 et 2 OLPD).

35 Il n'y a pas de charge de travail disproportionnée lorsque des renseignements doivent être fournis sur un grand nombre de données personnelles parce que le ou la responsable collecte (autant que possible) un grand nombre de données dans son propre intérêt. Il en va de même lorsque la charge de travail disproportionnée résulte d'un manque d'organisation du ou de la responsable. En ce qui concerne les demandes de renseignements adressées à la fondation mesvaccins après l'arrêt de la plateforme Internet mesvaccins.ch, le PFPDT a recommandé aux personnes concernées qui avaient demandé des renseignements de rembourser les frais de copies certifiées conformes de pièces d'identité que la fondation avait exigés.

36 Le ou la responsable doit informer la personne concernée qui a demandé des renseignements du montant de la participation aux frais avant de fournir les renseignements (art. 19 al. 3 phrase 1 OLPD). Dans la mesure où la personne concernée ne maintient pas l'information demandée dans un délai de dix

jours, la demande d'information est considérée comme retirée sans conséquences financières (art. 19 al. 2 RGPD). Le premier délai pour fournir les renseignements conformément à l'art. 18 al. 1 OLPD est ainsi prolongé de ce délai de réflexion de dix jours (art. 19 al. 3 phrase 2 OLPD).

Dans la pratique, une participation aux frais de la personne concernée n'a que peu d'importance. Dans le cas d'un calcul des coûts complets, les dépenses du ou de la responsable en rapport avec la participation aux frais atteignent souvent le maximum possible de 300 francs. Cette charge augmente encore si la personne concernée adapte sa demande de renseignements en raison de la participation aux frais exigée, afin que le ou la responsable ne puisse plus prétendre à une charge disproportionnée. Il est habituellement plus facile pour le responsable de demander une précision sur les renseignements demandés (cf. n. 18 ci-dessus). 37

C. Délai pour l'information (al. 7)

Un premier délai de 30 jours à compter de la réception par le responsable s'applique à la communication des renseignements (art. 18 al. 1 RGPD). Le ou la responsable peut prolonger ce délai si les renseignements ne peuvent pas être fournis dans les 30 jours et doit dans ce cas informer la personne concernée du nouveau délai (art. 18 al. 2 RGPD). L'information doit avoir lieu avant l'expiration du premier délai de 30 jours, tout comme l'information sur l'ajournement, la limitation ou le refus de l'accès (art. 18 al. 3 RGPD ; cf. art. 26 f. LPD sur les restrictions du droit d'accès). 38

VI. APPLICATION DU DROIT

Le droit d'accès doit être mis en œuvre par une action civile contre les personnes privées responsables, le non-respect ne constituant en principe pas une atteinte directe à la personnalité. Le non-respect ne peut pas être justifié conformément à l'article 31 LPD. Le for pour les actions civiles est au siège ou au domicile de l'une des parties (art. 20 let. d CPC), aucune avance de frais n'étant requise (art. 99 al. 3 let. d CPC) et aucun frais de justice n'étant alloué (art. 113 al. 2 let. g et 114 let. g CPC). La procédure simplifiée s'applique aux actions visant à faire valoir le droit d'accès (art. 243 al. 2 let. d CPC). 39

40 Le droit d'accès contre les organes fédéraux responsables doit être mis en œuvre par voie de recours. La personne concernée qui demande des renseignements a droit à une décision susceptible de recours.

41 Le PFPDT peut, dans le cadre de la procédure administrative, conformément aux art. 49 ss. LPD, ordonner la communication de renseignements et assortir la décision d'une menace de sanction (art. 51 al. 3 let. g et 63 LPD). La personne concernée n'a pas la qualité de partie dans cette procédure (art. 52 al. 2 LPD e contrario).

42 La communication intentionnelle d'un renseignement faux ou incomplet est punie, sur plainte de la personne concernée, d'une amende de 250'000 francs au plus (art. 60 al. 1 let. a LPD). La personne concernée a le droit de porter plainte (art. 30 CP, en particulier art. 30 al. 1 CP). Contrairement au RGPD, la LPD ne connaît en principe pas d'amendes administratives (art. 83 RGPD), une amende étant toutefois possible à titre exceptionnel pour les entreprises (cf. N. 44).

43 Le responsable qui ne répond pas à une demande d'information ou qui prétend à tort ne pas être tenu de fournir des informations n'est pas punissable. Cette lacune de punissabilité existait déjà selon l'art. 34 al. 1 let. aDSG, l'amende maximale possible étant de 10'000 francs (art. 106 al. 1 CP).

44 La disposition pénale est en principe limitée aux personnes physiques pour les personnes privées responsables. Le risque d'amende est essentiellement supporté par les personnes physiques individuelles qui fournissent des renseignements, ce qui peut également être une personne subalterne. Les entreprises ne peuvent être punies qu'exceptionnellement ; dans ce cas, l'amende maximale possible est de 50'000 francs (art. 64 LPD). La punissabilité pour la fourniture intentionnelle d'un renseignement incomplet est supprimée si l'on ne donne pas l'impression que le renseignement est complet. Il n'y a pas d'obligation de fournir une déclaration d'exhaustivité. Pour les collaborateurs de l'administration fédérale et d'autres organes fédéraux, seuls des moyens disciplinaires sont à disposition.

BIBLIOGRAPHIE

Baeriswyl Bruno, Vorbemerkung zu Art. 25-29 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar,

Datenschutzgesetz, 2. Aufl., Bern 2023 (zit. SHK-Baeriswyl, Vorb. zu Art. 25-29 DSG).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBI 2017 S. 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 30.3.2023.

Bundesamt für Justiz: Verordnung über den Datenschutz (Datenschutzverordnung, DSV), Erläuternder Bericht vom 31.8.2022 (zit. BJ, Bericht).

Bauer Stefan, Beweisführung der Zustellung im E-Mail-Verkehr, 1.5.2022, https://www.cubewerk.de/wp-content/uploads/2022/06/Stefan_Bauer_Beweisfuehrung_E-Mail_Fiktion_Zugangsfiktion_Zustellnachweise_E-Mail.pdf, besucht am 30.3.2023 (zit. Bauer, E-Mail-Zustellung).

Pärli Kurt/Flück Nathalie, Kommentierung zu Art. 25 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023 (zit. SHK-Pärli/Flück, Art. 25 DSG).

Rosenthal David, Das neue Datenschutzgesetz, Jusletter vom 16.11.2020 (zit. Rosenthal, Jusletter).

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz und weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. Rosenthal/Jöhri Art. 8 aDSG).

Schlussbericht und Empfehlungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EBÖB) betreffend die Plattform «meineimpfungen.ch», 31.8.21 (zit. Schlussbericht EDÖB).

Suter-Sieber Irène/Stutz Christoph/Wirz Chiara, Datenschutzzweckwidrige Auskunftsbegehren im Arbeitsverhältnis, AJP 5 (2021), S. 593-605 (zit. Suter-Sieber/Stutz/Wirz, Auskunftsbegehren).

Thouvenin Florent, Recht auf informationelle Selbstbestimmung?!, Vortrag am Datenschutz-Festival der Digitalen Gesellschaft am 2.12.2022 in Zürich, https://www.digitale-gesellschaft.ch/2022/12/15/erstes-datenschutz-festival-der-schweiz-zusammenfassung-rueck-und-ausblick/ und https://

www.digitale-gesellschaft.ch/uploads/2022/12/Datenschutz-Festival-Informationelle-Selbstbestimmung.pdf, besucht am 30.3.2023.

Vasella David, 4A_125/2020 (amtl. Publ.): Gegenstand des Auskunftsrechts, insb. betr. Herkunftsangaben; keine Auskunft über Daten im Gedächtnis, in: datenrecht.ch, 12.1.2021, https://datenrecht.ch/4a_125-2020-amtl-publ-gegenstand-des-auskunftsrechts-insb-betr-herkunftsangaben-keine-auskunft-auf-daten-im-gedaechtnis/, besucht am 30.3.2023 (zit. Vasella, Gedächtnis).

Vasella David, 4A_277/2020: Rechtsmissbrauch eines Auskunftsbegehrens bejaht (Fishing Expedition), in: datenrecht.ch, 8.12.2020, https://datenrecht.ch/4a_277-2020-rechtsmissbrauch-eines-auskunftsbegehrens-bejaht-fishing-expedition/, besucht am 30.3.2023 (zit. Vasella, Fishing Expedition).

Vasella David, EuGH (Österreichische Post): Auskunftsrecht umfasst wenn möglich die einzelnen Empfänger (nicht nur Kategorien), in: datenrecht.ch, 14.1.2023, https://datenrecht.ch/eugh-oesterreichische-post-auskunftsrecht-umfasst-die-einzelnen-empfaenger-nicht-nur-kategorien/, besucht am 30.3.2023 (zit. Vasella, Österreichische Post).

Vasella David, OGer ZH: kein Auskunftsrecht betr. Daten einer verstorbenen Person, Art. 1 Abs. 7 VDSG bundesrechtswidrig; Dispositionsmaxime bei Klagen auf Auskunftserteilung, in: datenrecht.ch, 4.4.2017, https://datenrecht.ch/oger-zh-kein-auskunftsrecht-betr-daten-einer-verstorbenen-person-art-7-abs-1-vdsg-bundesrechtswidrig-dispositionsmaxime-bei-klagen-auf-auskunftserteilung/, besucht am 30.3.2023 (zit. Vasella, Tod).

Waldvogel Marcel, Machine Learning: Künstliche Faultier-Intelligenz, in: dnip.ch, 16.8.2022, https://dnip.ch/2022/08/16/machine-learning-kuenstliche-faultier-intelligenz/, besucht am 30.3.2023 (zit. Waldvogel, Machine Learning).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 26 LPD

Un commentaire de Martin Steiger

PROPOSITION DE CITATION

Martin Steiger, Kommentierung zu Art. 26 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Steiger, N. XXX zu Art. 26 DSG.

Art. 26 Restrictions au droit d'accès

[1] Le responsable du traitement peut refuser, restreindre ou différer la communication des renseignements dans les cas suivants:

a. une loi au sens formel le prévoit, notamment pour protéger un secret professionnel;

b. les intérêts prépondérants d'un tiers l'exigent;

c. la demande d'accès est manifestement infondée notamment parce qu'elle poursuit un but contraire à la protection des données ou est manifestement procédurière.

[2] Il est au surplus possible de refuser, de restreindre ou de différer la communication des renseignements dans les cas suivants:

a. lorsque le responsable du traitement est une personne privée et que les conditions suivantes sont remplies:

ses intérêts prépondérants l'exigent,
il ne communique pas les données à un tiers.

b. lorsque le responsable du traitement est un organe fédéral:

si un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Suisse, l'exige, ou
si la communication des informations est susceptible de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative.

[3] Les entreprises appartenant au même groupe ne sont pas considérées comme des tiers au sens de l'al. 2, let. a, ch. 2[7].

[4] Le responsable du traitement indique le motif pour lequel il refuse, restreint ou diffère la communication des informations.

TABLE DES MATIÈRES

En bref ... 392
I. Généralités ... 392
II. Types de restrictions (al. 1 et 2) ... 392
III. Motifs de limitation (al. 1-3) ... 394
A. Obligations légales, notamment le secret professionnel (al. 1 let. a) ... 394
B. Intérêts prépondérants de tiers (al. 1 let. b) ... 394
C. Manifestation manifestement infondée ou quérulence manifeste (al. 1 let. c) ... 395
D. Intérêts prépondérants des responsables privés (al. 2 let. a et al. 3) ... 396
E. Intérêts prépondérants des organes fédéraux (al. 2 let. b) ... 397
IV. Obligation de motiver (al. 4) ... 398
Bibliographie ... 398

EN BREF

L'article 26 LPD régit les restrictions possibles au droit d'accès des personnes concernées. Le ou la responsable peut différer, limiter ou refuser l'accès pour différents motifs. Les motifs de limitation sont notamment les obligations légales telles que le secret professionnel, les intérêts prépondérants de tiers et le caractère manifestement infondé ou manifestement quérulent. Les responsables privés peuvent invoquer leurs propres intérêts prépondérants, les organes fédéraux des intérêts publics prépondérants. Les restrictions doivent être proportionnées, examinées au cas par cas et justifiées auprès de la personne concernée.

I. GÉNÉRALITÉS

1 Le droit d'accès des personnes concernées selon l'art. 25 LPD existe dans les limites des art. 26 f. LPD. L'accès peut être différé, limité ou refusé par le responsable du traitement pour différents motifs de restriction (art. 26 LPD). Les médias peuvent invoquer d'autres motifs pour restreindre l'accès (art. 27 LPD).

2 La disposition "peut" donne l'impression que les responsables peuvent décider librement de restreindre ou non l'accès. Or, ce n'est pas le cas, car les responsables peuvent souvent être tenus de restreindre l'accès. L'art. 26 al. 1 LPD cite comme motifs les obligations légales (let. a), les intérêts prépondérants de tiers (let. b) et le caractère manifestement infondé (let. c). L'art. 26 al. 2 LPD mentionne d'autres motifs selon que le ou la responsable est une personne privée (let. a) ou un organe fédéral (let. b) (cf. n. 8 ss. ci-dessous).

II. TYPES DE RESTRICTIONS (AL. 1 ET 2)

3 Les renseignements peuvent être différés, limités ou refusés (art. 26 al. 1 et 2 LPD). La restriction doit être proportionnée, également selon l'art. 6 al. 2 LPD et l'art. 36 al. 3 Cst., c'est-à-dire nécessaire, appropriée et adéquate ou proportionnée au sens strict. La restriction doit notamment être apte à atteindre l'objectif visé dans sa forme et son étendue ainsi que dans le temps.

En cas de refus, aucun renseignement n'est fourni. La personne concernée qui demande des informations ne reçoit aucune information pour une durée illimitée. Le responsable du traitement n'indique pas à la personne concernée si des données personnelles la concernant sont traitées (art. 25 al. 1 LPD). Si le refus est limité dans le temps, il s'agit d'un ajournement (cf. n. 6 ci-dessous). 4

Dans le cas d'une restriction, les informations ne sont fournies que partiellement, par exemple en noircissant certaines données. La restriction peut également signifier que les renseignements sont fournis en tout ou en partie, mais qu'ils sont assortis de conditions. Une telle condition peut consister à ne pas rendre les informations communiquées accessibles à des tiers et à ne pas les publier. Le ou la responsable peut exiger de la personne concernée qui demande des informations la confirmation préalable du respect des conditions, également sous la forme d'un accord de confidentialité. Une garantie plus étendue, par exemple par la convention d'une peine contractuelle dans le cas d'une personne privée responsable ou par une menace de peine selon l'art. 292 CP dans le cas d'un organe fédéral responsable, ne devrait être admise qu'exceptionnellement eu égard au principe de proportionnalité (cf. n. 3 ci-dessus). La communication restreinte de renseignements, y compris d'éventuelles conditions, peut être limitée dans le temps. Dans ce cas, il s'agit d'un ajournement (cf. n. 6). 5

En cas d'ajournement, les renseignements ne sont pas fournis en tout ou en partie dans le délai imparti (art. 25 al. 7 LPD), mais seulement à une date ultérieure. Dans le cas d'un organe fédéral responsable, par exemple, la communication des renseignements peut être différée afin de ne pas entraver la libre formation de l'opinion et de la volonté. 6

Contrairement à l'art. 9 al. 3 aDSG, l'art. 26 LPD ne règle pas la manière de procéder lorsque les motifs de restriction disparaissent. Selon l'art. 9 al. 3 aDSG, un organe fédéral devait dans ce cas fournir l'information, à moins que la communication de l'information ne soit impossible ou n'exige un effort disproportionné. Pour les organes fédéraux responsables, il faut partir du principe que cette obligation de principe de reconsidération reste valable. En revanche, pour les responsables privés, l'obligation de répondre a posteriori ne doit être admise qu'avec retenue, à savoir logiquement en cas de report. 7

III. MOTIFS DE LIMITATION (AL. 1-3)

8 L'art. 26 al. 1-3 LPD énumère de manière exhaustive les motifs de limitation possibles. S'il n'existe aucun motif de limitation, les informations ne peuvent être limitées d'aucune manière (cf. n. 3 ss. ci-dessus). S'il existe plus d'un motif de restriction, les responsables peuvent invoquer tous les motifs de restriction existants. Tous les responsables peuvent invoquer les motifs de limitation prévus à l'art. 26 al. 1 LPD. Les motifs de limitation selon l'art. 26 al. 2 LPD font la distinction entre les personnes privées responsables et les organes fédéraux. L'art. 26 al. 3 LPD ne concerne que les personnes privées. C'est l'art. 5 let. i LPD qui détermine si une personne responsable est considérée comme un organe fédéral.

A. Obligations légales, notamment le secret professionnel (al. 1 let. a)

9 Selon le libellé, ce motif de restriction s'applique exclusivement aux obligations prévues par une loi au sens formel. Ce motif de restriction a été repris de l'art. 9 al. 1 let. aDSG, à l'exception de la mention désormais explicite des secrets professionnels. Les obligations légales conformément à une ordonnance ne suffisent pas, a contrario. Il convient d'examiner au cas par cas si l'information peut être limitée en se référant au secret de fonction général.

10 Par ailleurs, l'obligation doit porter sur la limitation des renseignements vis-à-vis des personnes concernées. Les dispositions légales qui excluent de manière générale l'accès aux données personnelles ne sont pas pertinentes. Un avocat, par exemple, peut invoquer le secret professionnel à l'égard de tiers, notamment en vertu de l'art. 13 LLCA, mais pas à l'égard d'un client en tant que personne concernée.

B. Intérêts prépondérants de tiers (al. 1 let. b)

11 Les données ou informations ne doivent pas se rapporter uniquement à une personne concernée qui demande des renseignements. Un lien peut également exister avec d'autres personnes concernées (art. 5 let. b LPD), mais aussi avec d'autres tiers, par exemple des personnes morales. Sont par exemple considérés comme des tiers les employés du responsable du traitement. Un tel lien, et donc éventuellement des intérêts de tiers, est même possible sans que des données personnelles concernant de tels tiers soient

concernées. Ainsi, un tiers sur lequel le responsable ne traite pas de données personnelles pourrait tout de même avoir un intérêt à ce que l'information soit limitée par rapport à une personne qui demande des informations.

Si les intérêts de tiers sont concernés, le responsable doit vérifier s'il existe des intérêts prépondérants et, dans l'affirmative, si ces intérêts prépondérants exigent une limitation des renseignements. L'examen, y compris la pesée des intérêts, doit être effectué au cas par cas. La nécessité d'intérêts prépondérants montre que les intérêts de la personne concernée qui demande des informations ne prévalent pas en soi. Inversement, les intérêts des tiers concernés par les informations restreintes doivent prévaloir, c'est-à-dire qu'il doit être possible de "présumer une certaine importance de l'atteinte à la position du ou des tiers". Le motif de restriction a été repris tel quel de l'art. 9 al. 1 let. b aDSG. L'exception existe de la même manière pour le devoir d'information selon l'art. 20 al. 3 let. a LPD. 12

C. Manifestation manifestement infondée ou quérulence manifeste (al. 1 let. c)

Conformément à l'art. 26 al. 1 let. c LPD, l'information peut être limitée si la demande d'information est manifestement infondée, notamment si elle poursuit un but contraire à la protection des données, ou si elle est manifestement quérulente. Ces motifs de limitation constituent une nouveauté par rapport aux motifs de limitation prévus à l'article 9 aDSG et ont été complétés dans le cadre des débats parlementaires, notamment sur la base de la jurisprudence. Il s'agit ici aussi d'éviter les demandes de renseignements abusives. 13

Ces motifs de limitation doivent être interprétés de manière stricte. Le ou la responsable ne peut pas supposer sans autre qu'une demande de renseignements est manifestement infondée ou manifestement quérulente. Sont notamment considérées comme manifestement abusives les demandes d'informations qui ont manifestement pour but de "harceler ou d'exercer un responsable (par exemple en répétant les informations ou en sachant qu'elles sont inutiles)". Une demande d'information est considérée comme manifestement infondée lorsqu'elle ne cherche pas à faire valoir des droits en matière de protection des données ou à créer une transparence motivée par la protection des données. 14

15 Si une demande de renseignements est effectivement manifestement infondée ou manifestement quérulente, la solution la plus favorable à la personne concernée doit être choisie. La solution choisie, notamment l'ajournement ou la limitation plutôt que le refus, doit être proportionnée (voir n. 3 ci-dessus).

D. Intérêts prépondérants des responsables privés (al. 2 let. a et al. 3)

16 Les responsables privés peuvent limiter l'accès au-delà des motifs de l'art. 26 al. 1 LPD si leurs propres intérêts l'emportent sur ceux de la personne concernée qui demande l'accès (ch. 1) et si les données en question ne sont pas communiquées à des tiers (ch. 2). Ces conditions sont cumulatives. L'examen, y compris une éventuelle pesée des intérêts, doit être effectué au cas par cas (cf. également n. 12 ci-dessus). Cette disposition correspond à l'art. 9, al. 4, aDSG et constitue également une exception à l'obligation d'informer (art. 20, al. 3, let. c, LPD).

17 Les intérêts personnels prépondérants peuvent être, par exemple, des données servant à la protection contre le vol dans un grand magasin, la protection de secrets de fabrication et d'affaires ou une charge financière élevée, une participation aux frais devant être examinée dans ce dernier cas conformément à l'art. 26 al. 6 LPD.

18 Les données qui ne sont pas communiquées à des tiers ou à de "vrais" tiers, c'est-à-dire les données internes, sont en principe des données qui ne sont communiquées qu'à des personnes appartenant à la même structure d'organisation ou d'entreprise, donc pas à une autre structure d'organisation ou d'entreprise, et qui poursuivent éventuellement avec le traitement des données d'autres buts que le responsable. Dans le cadre des débats parlementaires, l'art. 26 al. 3 LPD a créé un privilège de groupe selon lequel les entreprises appartenant au même groupe ne sont pas considérées comme des tiers au sens de l'art. 26 al. 2 let. a ch. 2 LPD (il en va de même pour le devoir d'information ; art. 20 al. 3 let. c ch. 2 en relation avec l'art. 4 LPD). al. 4 LPD). L'aDSG ne connaissait pas encore un tel privilège et les sociétés du groupe étaient considérées comme des tiers.

19 L'exception s'applique également aux entreprises situées à l'étranger et appartenant au même groupe. Par ailleurs, la communication de données à des sociétés du groupe à l'étranger est soumise aux obligations applicables en

matière de protection des données, par exemple pour la communication de données personnelles à l'étranger (art. 16 s. LPD).

Les personnes qui traitent les données sur mandat conformément à l'art. 5 let. k LPD ne sont pas considérées comme des tiers (cf. également art. 9 et 24 al. 4 LPD). 20

E. Intérêts prépondérants des organes fédéraux (al. 2 let. b)

En tant que responsables, les organes fédéraux peuvent limiter les renseignements au-delà des motifs de l'art. 26 al. 1 LPD si les intérêts publics l'emportent sur les intérêts de la personne concernée qui demande les renseignements (ch. 1) ou si les renseignements compromettent une enquête, une instruction ou une procédure judiciaire (ch. 2). Cette disposition correspond pour l'essentiel à l'art. 9, al. 2, aDSG et constitue également une exception à l'obligation d'informer (art. 20, al. 3, let. d, LPD). 21

Chiffre 1 cite notamment la sécurité intérieure ou extérieure de la Confédération comme un éventuel intérêt public prépondérant dont la sauvegarde peut exiger une restriction des informations. La mention est faite à titre d'exemple, ce qui signifie que tous les intérêts publics peuvent entrer en ligne de compte comme motif de restriction, pour autant qu'ils soient prépondérants et que la restriction soit nécessaire pour la sauvegarde correspondante des intérêts. D'autres intérêts publics entrant en ligne de compte sont par exemple - en s'inspirant également de l'art. 7, al. 1, LTrans - la libre formation de l'opinion et de la volonté des autorités, des instances judiciaires et d'autres organes publics, l'exécution conforme aux objectifs de mesures concrètes prises par les autorités, les intérêts de politique extérieure ou les relations internationales de la Suisse, les relations entre la Confédération et les cantons ou les intérêts de la Suisse en matière de politique économique, monétaire et monétaire. 22

Chiffre 2 mentionne un autre motif de restriction, à savoir la mise en danger possible d'une enquête, d'une instruction ou d'une procédure administrative ou judiciaire. Cette restriction n'est valable que si et dans la mesure où la LPD est applicable à de telles enquêtes et procédures (art. 2 al. 3 LPD). Dans la littérature, certains estiment que les enquêtes internes, qui précèdent par exemple une procédure disciplinaire, pourraient tomber sous le coup de cette disposition. 23

24 Les deux motifs de restriction doivent être examinés au cas par cas, y compris une éventuelle pesée des intérêts (cf. également n. 12 et 16 ci-dessus).

IV. OBLIGATION DE MOTIVER (AL. 4)

25 Le ou la responsable doit motiver la limitation de l'accès à la personne concernée, comme le prévoit déjà l'art. 9 al. 5 aDSG. La motivation doit permettre à la personne concernée de comprendre le ou les motifs de la limitation et d'en vérifier la légitimité. Dans le cas des organes fédéraux responsables, la limitation doit être prononcée au moins sur demande de la personne concernée sous la forme d'une décision sujette à recours (art. 5 PA). Il n'y a pas d'obligation de conserver la justification donnée, mais il est évident que la ou les personnes responsables doivent conserver les communications correspondantes avec la personne concernée pour des raisons de preuve.

26 La charge de la preuve du ou des motifs de restriction incombe au responsable, y compris en ce qui concerne la proportionnalité. En cas de demande de renseignements abusive au sens de l'article 26 al. 1 let. c LPD, il suffit de montrer qu'une demande de renseignements "sert manifestement de manière pertinente une finalité qui ne concerne pas la protection des données", ce qui constitue un allégement de la preuve.

BIBLIOGRAPHIE

Bundesamt für Justiz: Verordnung über den Datenschutz (Datenschutzverordnung, DSV), Erläuternder Bericht vom 31.8.2022 (zit. BJ, Bericht).

Husi-Stämpfli Sandra, Kommentierung zu Art. 26 DSG in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern, 2023 (zit. SHK-Husi-Stämpfli, Art. 26 DSG).

Rosenthal David, Das neue Datenschutzgesetz, Jusletter vom 16.11.2020 (zit. Rosenthal, Jusletter).

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz und weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. Rosenthal/Jöhri, Art. 9 aDSG).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 27 LPD

Un commentaire de Martin Steiger

PROPOSITION DE CITATION

Martin Steiger, Kommentierung zu Art. 27 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Steiger, N. XXX zu Art. 27 DSG.

Art. 27 Restrictions au droit d'accès applicables aux médias

[1] Lorsque les données personnelles sont traitées exclusivement pour la publication dans la partie rédactionnelle d'un média à caractère périodique, le responsable du traitement peut refuser, restreindre ou différer la communication des renseignements dans l'un des cas suivants:

a. les données fournissent des indications sur les sources d'information;

b. un droit de regard sur des projets de publication en résulterait;

c. la libre formation de l'opinion publique serait compromise.

[2] Les journalistes peuvent en outre refuser, restreindre ou différer la communication des renseignements lorsque les données personnelles servent exclusivement d'instrument de travail personnel.

TABLE DES MATIÈRES

En bref 402
I. Généralités 402
II. Conditions pour le privilège des médias 402
III. Motifs de limitation 404
A. Protection des sources (al. 1 let. a) 404
B. Protection des projets (al. 1 let. b) 404
C. Protection de la libre formation de l'opinion du public (al. 1 let. c) 404
D. Instrument de travail personnel des journalistes (al. 2) 404
Bibliographie 405

EN BREF

L'art. 27 LPD régit le privilège des médias. Les médias et les professionnels des médias peuvent, sous certaines conditions, restreindre le droit d'accès des personnes concernées au-delà des motifs généraux de restriction. Le privilège des médias n'est applicable qu'aux données personnelles destinées à des publications rédactionnelles dans des médias à parution périodique. Le privilège des médias sert à protéger la liberté des médias.

I. GÉNÉRALITÉS

1 Il est incontestable que la LPD est également applicable aux médias. En raison du rôle particulier des médias, notamment dans le cadre de la liberté des médias, y compris le secret de rédaction (art. 17 Cst.), l'art. 10 aDSG connaissait déjà un privilège des médias (restrictions du droit d'accès pour les professionnels des médias). Ce privilège des médias a été repris pour l'essentiel sans modification, tout comme le motif justificatif correspondant (art. 31 al. 2 let. d LPD, même si des adaptations ont été apportées par rapport à l'art. 13 al. 2 let. d aDSG). Le titre mentionne désormais les médias et non plus les professionnels des médias, bien que la disposition continue de concerner les médias et les professionnels des médias.

2 Les types généraux de restrictions (art. 26 al. 1 et 2 LPD) et la même obligation de motivation (art. 26 al. 4 LPD) s'appliquent au privilège des médias. De même, les restrictions doivent être proportionnées et faire l'objet d'un examen au cas par cas.

II. CONDITIONS POUR LE PRIVILÈGE DES MÉDIAS

3 Les responsables qui souhaitent restreindre l'accès en se référant au privilège des médias doivent remplir les conditions cumulatives suivantes : Les données personnelles concernées doivent être traitées exclusivement en vue de leur publication dans la partie rédactionnelle d'un média à caractère périodique (al. 1).

4 Traitement exclusif : les données personnelles concernées ne doivent pas être traitées dans un but autre que la publication dans la partie rédactionnelle d'un média à caractère périodique. Toute autre finalité non contraignante d'un

point de vue légal, comme par exemple un secret professionnel (cf. art. 26 n. 9 s.), signifie que le renseignement ne peut pas être limité en se référant au privilège des médias. Les données personnelles contenues dans les archives des médias, qui sont accessibles au public, ne tombent pas sous le coup du privilège des médias.

Utilisation rédactionnelle : Les articles, rapports, séries de photos, interviews, commentaires et contributions d'opinion sont considérés comme rédactionnels. Les commentaires des lecteurs, traditionnellement sous forme de lettres de lecteur, sont également considérés comme rédactionnels. Ne sont pas considérés comme rédactionnels les objectifs internes et autres objectifs non rédactionnels, notamment le marketing des lecteurs et la publicité ou les possibilités de communication avec le public sans lien avec la rédaction, comme les salons de discussion. Ne sont pas non plus considérés comme rédactionnels les commentaires de lecteurs qui ne sont pas visionnés avant la publication. 5

Publication : les données personnelles concernées doivent être traitées dans le but de publier ces données personnelles ou au moins de contribuer à une publication. L'expression "traitées en vue de la publication [...]" signifie que l'information restreinte n'est pas limitée au traitement avant la publication, mais qu'elle dépend de la finalité du traitement, indépendamment du moment. 6

Média à parution périodique : par média au sens de l'art. 27 al. 1 LPD, il faut entendre tous les moyens de diffusion d'informations, y compris les moyens numériques tels que les bulletins d'information par e-mail, les canaux de médias sociaux et les newsletters. Le terme "média" est volontairement formulé de manière ouverte et neutre sur le plan technique. La parution doit être périodique, c'est-à-dire qu'elle doit être répétée sans que l'intervalle ou la période soit toujours le même. Un site web publié une seule fois avec des contributions rédactionnelles ou un magazine publié une seule fois avec des contenus journalistiques n'est donc pas considéré comme un média à parution périodique. 7

III. MOTIFS DE LIMITATION

A. Protection des sources (al. 1 let. a)

8 Toute déduction à partir des données personnelles concernées sur des sources d'information de toute nature est considérée comme un motif de restriction. Le motif de restriction va au-delà de la protection des sources au sens de l'article 28a CP, mais exige en même temps que les données "renseignent" effectivement et qu'il n'y ait pas seulement une possibilité correspondante. Dans le cas de la seule protection des sources, il faudrait tenir compte du fait que celle-ci ne garantit pas la protection des sources, mais permet aux médias et aux professionnels des médias de protéger leurs sources sous certaines conditions.

B. Protection des projets (al. 1 let. b)

9 Ce motif de restriction vise à empêcher la censure préalable, même si la protection des sources (al. 1 let. a) est garantie. On parle également de protection de la publication : la possibilité d'un tri préalable via le droit d'accès pourrait conduire les médias et les professionnels des médias à ne pas publier un contenu comme prévu, voire à ne pas le publier du tout. Le motif de restriction peut donc également empêcher un "chilling effect".

C. Protection de la libre formation de l'opinion du public (al. 1 let. c)

10 La liberté d'opinion et d'information comprend, entre autres, le droit de toute personne de former librement son opinion (art. 16 al. 2 Cst.), notamment sur la base du contenu des médias et des professionnels des médias (art. 16 al. 3 Cst.). Le motif justificatif correspondant vise à protéger un paysage médiatique qui fonctionne bien.

D. Instrument de travail personnel des journalistes (al. 2)

11 Ce motif de restriction concerne les données personnelles qui ne sont pas déjà exclues du champ d'application de la LPD en tant que données personnelles traitées par une personne physique pour son usage personnel exclusivement (art. 2, al. 2, let. a LPD) et qui sont traitées par des professionnels des médias.

Les collectes d'informations ou les notes personnelles ne tomberaient pas sous le coup de l'exception de l'art. 2 al. 2 let. a LPD si elles sont communiquées à des tiers par des journalistes. Les journalistes peuvent souvent en avoir besoin, par exemple lors de contacts avec des sources ou de recherches. 12

Les professionnels des médias sont toutes les personnes physiques qui exercent une activité journalistique, artistique ou rédactionnelle pour les médias au sens de l'al. 1, qu'elles soient employées à titre permanent ou indépendant ou qu'elles travaillent à leur compte, contre rémunération ou non. En 2008, Rosenthal/Jöhri exigeaient encore une certaine activité professionnelle et excluaient les "journalistes amateurs", ce qui ne peut plus être valable au vu du paysage médiatique actuel. 13

BIBLIOGRAPHIE

Glasl Daniel, Anonyme Kommentare auf News-Portalen und Quellenschutz, Medialex 08 (2022), 7.10.2022 (zit. Glasl, Quellenschutz).

Husi-Stämpfli Sandra, Kommentierung zu Art. 27 DSG in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023 (zit. SHK-Husi-Stämpfli, Art. 27 DSG).

Rosenthal David, Das neue Datenschutzgesetz, in: Jusletter vom 16.11.2020 (zit. Rosenthal, Jusletter).

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz und weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. Rosenthal/Jöhri, Art. 10 aDSG).

Schweizer Michael, Chilling Effect im Schweizer Medienkontext, Medialex 10/202, 3.12.2020 (zit. Schweizer, Chilling Effect).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 28 LPD

Un commentaire de Samuel Mätzler

PROPOSITION DE CITATION

Samuel Mätzler, Commentaire de l'art. 28 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Mätzler, art. 28 LPD N. XXX.

Art. 28 Droit à la remise ou à la transmission des données personnelles

[1] La personne concernée peut demander au responsable du traitement qu'il lui remette sous un format électronique couramment utilisé les données personnelles la concernant qu'elle lui a communiquées lorsque les conditions suivantes sont réunies:

a. le responsable du traitement traite les données personnelles de manière automatisée;

b. les données personnelles sont traitées avec le consentement de la personne concernée ou en relation directe avec la conclusion ou l'exécution d'un contrat entre elle et le responsable du traitement.

[2] La personne concernée peut en outre demander au responsable du traitement qu'il transmette les données personnelles la concernant à un

autre responsable du traitement, pour autant que les conditions de l'al. 1 soient remplies et que cela n'exige pas des efforts disproportionnés.

[3] Le responsable du traitement remet ou transmet gratuitement les données personnelles. Le Conseil fédéral peut prévoir des exceptions, notamment si la remise ou la transmission des données personnelles exige des efforts disproportionnés.

TABLE DES MATIÈRES

En bref 410
I. Remarques préliminaires 410
II. Généralités 411
A. Objectif de la norme 411
B. Genèse 413
C. Remarques de droit comparé 414
III. Conditions 414
A. Données personnelles des personnes concernées 414
B. Données communiquées 416
C. Traitement automatisé 417
D. Consentement ou lien direct avec un contrat 418
IV. Conséquence juridique : le transfert 419
A. À la personne concernée (remise des données ; al. 1) 420
B. À un responsable du traitement (transfert de données ; al. 2) 420
C. Format des données 421
1. Courant 421
2. Format électronique 422
3. Absence d'exigence d'interopérabilité 423
V. Modalités (al. 3 et OPDDo) 424
A. Forme et délai 424
B. Compétence 425
C. Gratuité 426
Bibliographie 426
Matériaux 429

EN BREF

Le droit à la communication ou au transfert des données est, avec le droit d'accès, le deuxième droit des personnes concernées en matière de protection des données. Il est souvent désigné sous le nom de « droit à la portabilité des données ». Ce droit permet à une personne concernée d'exiger que certaines données, qu'elle a activement mises à la disposition du responsable du traitement ou que celui-ci a collectées, lui soient communiquées ou soient transférées directement à des tiers. Les données doivent être transférées dans un format électronique courant. Cela doit permettre une réutilisation directe par la personne concernée ou par un autre prestataire. Ce nouveau droit à la portabilité des données a été repris du RGPD et se situe à la croisée du droit de la protection des données et du droit de la concurrence. Il vise à donner à la personne concernée, dans le cadre de l'économie des données, la possibilité de disposer de « ses » données en toute autonomie.

I. REMARQUES PRÉLIMINAIRES

1 L'article 28 de la LPD prévoit le droit de la personne concernée à la remise (al. 1) ou au transfert (al. 2) de certaines données la concernant. Également désigné sous le nom de **droit à la portabilité des données**, il constitue – aux côtés du droit d'accès – le deuxième droit de la personne concernée dans le cadre de la LPD. L'article 29 LPD, qui suit, doit être lu conjointement avec l'article 28 LPD et énonce les motifs de restriction possibles.

2 Pour exercer le droit prévu à l'article 28 de la LPD, la **personne physique requérante**, dont les données sont traitées par un responsable du traitement, est **legitimée activement**. Est **legitimé passivement** le responsable du traitement qui traite lui-même les données de la personne requérante visées par le droit à la portabilité ou qui les fait traiter par un sous-traitant. Peuvent être concernés à cet égard des personnes privées et, dans de rares cas, des organes fédéraux.

II. GÉNÉRALITÉS

A. Objectif de la norme

L'objectif de l'art. 28 LPD reste controversé à ce jour. Alors que le Conseil fédéral, par exemple, voit dans le droit à la portabilité des données la réalisation d'objectifs relevant du droit de la concurrence (cf. N. 10), d'autres voix dans la doctrine mettent en avant des objectifs liés à la protection des consommateurs ou à la protection des données. La détermination de l'objectif normatif est d'autant plus compliquée que, lors de l'élaboration de la réglementation, les Chambres fédérales se sont certes concentrées sur les réseaux sociaux, mais n'ont pas prévu, dans le droit à la portabilité des données, de restriction correspondante aux réseaux sociaux. L'art. 28 LPD peut donc **s'appliquer à de nombreux contextes et secteurs** – par exemple dans le secteur de la mobilité, dans le domaine de la santé, sur les plateformes Internet, pour les services cloud ou dans la gestion des ressources humaines. Le seul point commun entre tous ces cas d'application est qu'ils découlent des changements fondamentaux intervenus dans le traitement moderne des données (voir également N. 23 et suivants). C'est l'émergence récente de l'**économie des données** qui a rendu nécessaire le droit à la portabilité des données. Cet aspect doit être pris en compte dans l'objectif de la norme. 3

Du point de vue du droit de la protection des données, le droit à la portabilité de la personne concernée doit permettre une **gestion autonome des données**. Il vise à mettre fin à la possibilité d'exclusion de fait dont bénéficierait le responsable du traitement en l'absence de droit à la portabilité, et à faire passer la personne, jusqu'alors reléguée au rang d'objet des données, au statut de sujet des données, en lui permettant d'avoir son mot à dire sur l'utilisation de ses données. Cela permet de remédier aux déséquilibres entre les acteurs engendrés par l'économie des données. La personne concernée dispose pour la première fois d'un moyen juridique pour intervenir de manière autonome dans l'économie des données et pouvoir participer au potentiel de celles-ci. 4

Toutefois, **des considérations relevant du droit de la concurrence** y sont étroitement liées. À cet égard, le droit à la portabilité vise à promouvoir la concurrence de manière générale et à favoriser la libre circulation des données. D'autres objectifs souvent cités dans la littérature, tels que la 5

réduction des coûts de changement ou des barrières à l'entrée sur le marché et la prévention des effets de verrouillage, ne peuvent en revanche, selon le point de vue défendu ici, jouer qu'un rôle secondaire : l'article 28 de la LPD ne se limite pas aux cas dans lesquels un effet de verrouillage existe ou pourrait simplement exister, et il n'est pas nécessaire de prouver l'existence de barrières à l'entrée sur le marché ni de démontrer que celles-ci sont réduites. De plus, le responsable du traitement n'est pas tenu d'occuper une position particulière sur le marché ni même d'être actif sur un marché.

6 Ainsi, les objectifs relevant du droit de la concurrence s'éloignent d'une conception classique du droit des ententes et se rapprochent d'un « droit de la réglementation » qui agit *ex ante*. Ces objectifs reposent en outre sur l'idéalisme de ce qu'on appelle l'**Open Web**. Ce mouvement, apparu à la fin des années 2000, est ancré dans le milieu informatique américain et repose sur l'idée que seules la liberté de créer des liens vers des contenus sur Internet (et en particulier sur le World Wide Web) ainsi que l'accès à ceux-ci ont permis l'innovation et ont pu donner naissance aux offres existantes aujourd'hui. Cet « Open Web » est toutefois menacé par les monopoles et les silos de données (appelés « walled gardens »), car les grandes plateformes Internet, notamment, s'isolent de plus en plus les unes des autres. Le droit à la portabilité des données doit donc être considéré, à un niveau bien plus fondamental, comme une réponse à un Internet composé de « walled gardens ». L'économie des données – telle qu'elle se manifeste principalement sur le World Wide Web – doit être libérée des silos de données propriétaires, et les personnes concernées doivent pouvoir changer de fournisseur sans se heurter à des obstacles faussant la concurrence.

7 En raison de la diversité des cas d'application possibles, les objectifs mentionnés, parfois très différents, ne sont pas toujours faciles à concilier. Cela dit, le droit à la portabilité des données poursuit à la fois des objectifs relevant du droit de la protection des données et du droit de la concurrence. Il convient toutefois de **le considérer avant tout comme un instrument relevant du droit de la protection des données**, qui poursuit *également* des objectifs relevant du droit de la concurrence. Cela découle systématiquement du fait que le droit à la portabilité ne s'applique qu'aux données à caractère personnel et ne peut être exercé que par les personnes concernées (au sens du droit de la protection des données). En conséquence, un lien avec la personnalité de la personne concernée et son

autodétermination informationnelle s'impose naturellement. À l'inverse, aucune condition relevant du droit de la concurrence ne doit être remplie pour que ce droit puisse être exercé. Il n'est même pas nécessaire que le responsable du traitement opère sur un marché ou de manière pertinente au regard de la concurrence.

Par conséquent, le droit à la portabilité des données n'est **pas** (comme certains le soutiennent) **étranger au système du droit de la protection des données, mais « créateur de système »**. Il est l'expression d'une décision de principe du législateur, selon laquelle la personne concernée doit avoir la possibilité d'exercer un droit de regard sur les données la concernant. En l'ancrant dans la LPD, le législateur a clairement indiqué que l'accent devait désormais être mis sur la personne concernée. 8

Compte tenu notamment de l'histoire peu linéaire de son émergence en Suisse (nous y reviendrons aussitôt), le droit à la portabilité des données doit également être compris dans un contexte plus large : il s'agit d'un instrument de la **politique suisse en matière de données** par excellence et non « simplement » d'un instrument relevant du droit de la protection des données. Le droit à la portabilité découle de considérations fondamentales en matière de politique des données et vise à permettre une libre circulation des données à l'ère de l'économie des données. En ce sens, s'il peut certes – comme c'est désormais le cas – s'inscrire dans le cadre du droit de la protection des données, il ne doit pas nécessairement entretenir un lien étroit avec la LPD. Dès le début des délibérations sur la révision de la LPD, la porte-parole de la commission compétente l'avait d'ailleurs très justement souligné : « Il ne s'agit pas simplement de la protection des données, mais aussi d'autres questions de politique des données telles que la portabilité, etc., auxquelles nous devons [...] nous confronter. » 9

B. Genèse

L'article 28 de la LPD n'a pas d'équivalent dans l'aDSG. Il s'agit d'une véritable innovation de la révision, reprise de la DSGVO (cf. N. 12) . Son **introduction était toutefois incertaine jusqu'au dernier moment** : le Conseil fédéral considérait une telle réglementation comme « problématique » et avait renoncé à inclure un droit à la portabilité des données dans l'avant-projet. Il justifiait cette décision en arguant qu'un tel droit visait davantage à permettre aux personnes concernées de réutiliser leurs données afin de favoriser la 10

concurrence qu'à protéger leur vie privée. Il craignait en outre des coûts élevés et doutait du succès de la mise en œuvre, car celle-ci nécessiterait un accord entre les responsables sur les supports de données et les normes informatiques. Le Conseil fédéral souhaitait plutôt examiner l'introduction de droits de portabilité spécifiques à certains secteurs.

11 Lors des **débats parlementaires**, la CIP-N a toutefois intégré un droit général à la portabilité des données dans le projet. Cette mesure visait à ouvrir de nouveaux espaces économiques et à modifier l'équilibre des pouvoirs entre les petites et les grandes plateformes. Une minorité a par ailleurs demandé d'élargir encore la portée de ce droit et de soumettre à la portabilité toutes les données se rapportant à une personne. La majorité du Conseil national, ainsi que le Conseil fédéral, ont toutefois estimé qu'un tel droit irait trop loin au regard des problèmes potentiels liés aux secrets d'affaires. Finalement, les Chambres ont décidé d'ancrer le droit à la portabilité dans sa forme actuelle, « en gardant toujours à l'esprit ce qui porte atteinte au caractère approprié et ce qui n'y porte pas atteinte ».

C. Remarques de droit comparé

12 Le droit à la portabilité des données a été **repris** pratiquement sans modification de la DSGVO, raison pour laquelle la disposition figurant à l'art. 20 de la DSGVO peut servir de référence pour l'interprétation suisse. Il existe toutefois des différences ponctuelles dans la formulation, qui seront abordées – dans la mesure où elles sont pertinentes – dans le cadre des différentes conditions.

III. CONDITIONS

A. Données personnelles des personnes concernées

13 L'art. 28, al. 1, de la LPD prévoit tout d'abord que la personne concernée peut exiger du responsable du traitement la remise de « ses données personnelles ». Il en résulte que seules les données se rapportant à une **personne physique** sont portables (art. 2, al. 1, et art. 5, let. a, de la LPD). Ainsi, les données sans lien avec la personne concernée ne sont pas visées, dans la mesure où le responsable du traitement ne peut pas les associer à celle-ci. On peut citer, par exemple, les indicateurs de performance anonymes dans le cadre de logiciels, tels que les informations relatives à l'utilisation du processeur ou à la

consommation de mémoire sur l'appareil d'une utilisatrice. Il est donc exigé que les données aient un lien étroit avec la personnalité de la personne concernée.

Par conséquent, les données se rapportant à des personnes morales ne sont pas soumises au droit à la portabilité. Ne sont pas non plus concernées les données qu'un responsable du traitement **anonymise a posteriori**. S'il s'agit de données pseudonymisées, celles-ci doivent être considérées comme des données à caractère personnel si le responsable du traitement peut les relier à la personne concernée. 14

Comme le précisent clairement les versions latines, les données doivent se rapporter à la personne qui en fait la demande. En revanche, rien ne peut être déduit de la formulation ambiguë de la version allemande (« ses données à caractère personnel »), qui permettrait également une interprétation différente et plus large. Il en résulte que les **données purement relatives à des tiers**, c'est-à-dire les données qui se rapportent exclusivement à des tiers, ne sont pas soumises au droit à la portabilité. 15

La question de savoir comment il en va des données qui se rapportent *également* à des tiers, par exemple des photos sur lesquelles plusieurs personnes apparaissent, fait toutefois l'objet d'une controverse. Étant donné que les motifs de restriction du droit à la portabilité des données prévus à l'art. 29, al. 1, en liaison avec l'art. 26, al. 1, let. b, de la LPD, font référence à des intérêts prépondérants de tiers, il y a lieu de considérer que les données personnelles qui se rapportent également à des tiers peuvent être soumises au droit à la portabilité. Sont donc également concernées les **données présentant un « double lien »**, qui présentent un certain lien avec la personne concernée, même si ces données ne se rapportent pas (uniquement) à celle-ci. C'est le cas, par exemple, des historiques complets de discussions en ligne ou d'e-mails, ou encore des transactions bancaires archivées (y compris les informations relatives aux débiteurs ou aux bénéficiaires). Ce n'est que s'il existe des intérêts prépondérants de tiers (ou s'il s'agit de données relevant exclusivement de tiers) que les données ne sont pas soumises au droit à la portabilité des données. S'il en allait autrement, l'art. 28 LPD resterait sans effet précisément dans de nombreux cas visés par l'objectif de la norme. 16

Il convient donc de procéder comme suit pour déterminer si certaines données sont soumises au droit à la portabilité : dans un premier temps, le 17

responsable du traitement doit vérifier si, d'une manière générale, les conditions prévues à l'article 28 de la LPD sont remplies, en particulier si les données à caractère personnel en question ont été communiquées par la personne concernée. Si les données concernent *également* des tiers (mais pas *uniquement* des tiers) et présentent un double lien, il convient, dans un deuxième temps, d'évaluer, au sens d'une « mesure restrictive », si des intérêts prépondérants de tiers justifient une restriction. En l'absence d'intérêts prépondérants du tiers, les données peuvent être transférées.

B. Données communiquées

18 Le droit à la portabilité des données est limité aux données que la personne concernée a « communiquées » au responsable du traitement. La notion de communication ne doit **pas être comprise au sens de la définition légale de l'art. 5, let. e, LPD**. Cela n'est d'ailleurs pas nécessaire pour son interprétation : dès la procédure législative, il a été précisé dans les documents de travail quelles données étaient visées. Le Conseil fédéral a ensuite précisé la portée de cette caractéristique dans l'OPDo. De plus, l'OFJ s'est exprimé sur cette portée dans ses commentaires. C'est pourquoi la condition de la communication en Suisse (contrairement à ce qui est le cas dans la DSGVO) est, du moins en théorie, largement incontestée. Dans la pratique, des questions de délimitation délicates peuvent néanmoins se poser.

19 Conformément à l'art. 20, al. 1, let. a, de l'OPDo, sont d'abord considérées comme communiquées les données qu'une personne concernée met sciemment et volontairement à la disposition du responsable du traitement (**ce que l'on appelle les « données de base » ; également « provided data** »). Sont concernées toutes les données communiquées directement et en toute connaissance de cause, par exemple les coordonnées saisies dans le cadre d'une commande en ligne ou les données à fournir lors d'une inscription sur une plateforme ou sur un formulaire d'anamnèse à l'hôpital. Les mots de passe ou les clés privées n'entrent pas dans cette catégorie, dans la mesure où ils sont – ce qui devrait être le cas en règle générale – cryptés et ne peuvent pas être associés à la personne concernée par le responsable du traitement.

20 Par ailleurs, les données sont considérées comme communiquées lorsqu'un responsable du traitement les a collectées au sujet de la personne concernée et de son comportement dans le cadre de l'utilisation d'un service ou d'un

appareil (art. 20, al. 1, let. b, OPDo) . Ces **données observées (ou « observed data »)** sont générées indirectement – sciemment ou non – par la personne concernée lors de l'utilisation d'un service ou d'un appareil. Cela inclut, par exemple, les valeurs d'une application de fitness sur une montre connectée, générées sur la base des performances sportives, les titres musicaux écoutés sur un service de streaming ou les données de consommation et de localisation d'un véhicule connecté.

Ne sont pas concernées les **données dérivées (également appelées « derived data »)**, c'est-à-dire les données que le responsable du traitement génère par sa propre analyse des données (art. 20, al. 2, OPDo). Comme celles-ci constituent une prestation autonome du responsable du traitement, elles sont exclues du portage. Dans ce cas, le législateur a accordé une plus grande importance à la protection de la prestation propre et des investissements propres du responsable du traitement qu'au droit de la personne concernée de permettre une réutilisation de « ses » données à caractère personnel. 21

La distinction entre données observées et données dérivées doit être établie au cas par cas et ne devrait pas toujours être aisée. Ainsi, dans le domaine de la santé, par exemple, observer revient le plus souvent à mesurer, et une simple mesure repose souvent sur une technologie complexe qui s'appuie sur des méthodes scientifiques. Dans ces cas, la transition entre la simple observation et la dérivation peut être floue et difficile à déterminer. 22

C. Traitement automatisé

Une autre restriction réside dans le fait que seules les données que le responsable du traitement traite de manière automatisée sont soumises au droit à la portabilité des données (art. 28, al. 1, let. a, LPD). Cela vise principalement à exclure les données qui sont **conservées sous forme papier**. On peut penser, par exemple, aux formulaires d'anamnèse physiques dans un cabinet médical, tant qu'ils ne sont pas transférés a posteriori dans un dossier médical électronique. 23

Seules les **données traitées par voie électronique** sont concernées. En effet, malgré la neutralité technologique intrinsèque de la LPD, le droit à la portabilité des données vise les échanges numériques et est destiné à s'appliquer en particulier aux échanges de données sur Internet. Toutefois, 24

cette condition ne constitue aujourd'hui **pratiquement plus une restriction**, car la plupart des traitements de données sont vraisemblablement automatisés.

25 Le responsable du traitement n'est pas tenu de numériser les données conservées sous forme papier ou sous toute autre forme analogique. Toutefois, si les données ne sont traitées **que partiellement de manière automatisée**, le responsable du traitement peut, dans certains cas, être tenu de transférer ces données, car la restriction ne fait pas référence à un traitement exclusivement automatisé. Étant donné qu'il doit, dans ce cas, fournir ou transférer les données dans un format électronique courant, des obligations supplémentaires peuvent alors lui incomber.

D. Consentement ou lien direct avec un contrat

26 L'art. 28 LPD prévoit une autre condition : la restriction s'applique aux données traitées avec le consentement de la personne concernée ou en lien direct avec la conclusion ou l'exécution d'un contrat entre le responsable du traitement et la personne concernée (al. 1, let. b). Cette condition se réfère aux **motifs justifiant un traitement de données prévus à l'art. 31 LPD** et a été reprise *tel quel* de la DSGVO.

27 Toutefois, la DSGVO repose sur le principe de l'interdiction avec réserve d'autorisation. En Suisse, en revanche, le traitement de données par des particuliers est en principe autorisé tant que la personnalité de la personne concernée n'est pas lésée de manière illicite (autorisation avec réserve d'interdiction). En conséquence, la LPD n'exige pas dans tous les cas un motif de justification au sens de l'article 31 LPD pour un traitement de données par des particuliers. Au contraire, un traitement de données ne peut **pas porter atteinte de manière illicite à la personnalité de la personne concernée**, par exemple parce qu'il est effectué conformément aux principes de protection des données (art. 30, al. 1 et al. 2, let. a, LPD *a contrario*). Cela méconnaît toutefois la condition prévue à l'art. 28, al. 1, let. b, LPD.

28 Une interprétation littérale signifierait donc que seuls les traitements de données sont soumis au droit à la portabilité s'ils peuvent s'appuyer sur les motifs justificatifs que sont le consentement (art. 31, al. 1, variante 1, LPD) ou l'intérêt prépondérant découlant d'un lien direct avec un contrat (art. 31, al. 2, let. a, LPD). Cela garantirait certes que les traitements de données fondés sur

une obligation légale ne soient pas couverts par le droit à la portabilité des données. Toutefois, aucune raison n'apparaît pour laquelle **les traitements de données ne nécessitant aucun motif de justification** devraient être exclus de la portabilité.

La doctrine part donc du principe d'une négligence législative et plaide, au regard de l'objectif de la norme, en faveur d'une interprétation plus large. Il convient donc de se fonder sur le **caractère volontaire du traitement des données**. Par conséquent, l'initiative du traitement concret des données doit au moins (également) émaner de la personne concernée. Le traitement des données ne doit pas être totalement dissocié de la volonté des personnes concernées. Si tel est le cas, la condition prévue à l'art. 28, al. 1, let. b, LPD est remplie, indépendamment du fait qu'un motif justificatif au sens de l'art. 31 LPD soit invoqué ou non. 29

À l'inverse, cela signifie que les traitements de données qui se fondent sur un autre motif justificatif ne sont pas soumis au droit à la portabilité des données. Cela est notamment pertinent lorsqu'il existe une base légale pour le traitement des données (art. 31, al. 1, variante 3, LPD). Alors que la DSGVO prévoit une exclusion expresse des traitements effectués dans le cadre de l'exercice de missions de service public (art. 20, al. 3, 2e phrase, DSGVO), ce n'est pas le cas en vertu de la LPD. Néanmoins, la restriction prévue à l'art. 28, al. 1, let. b, LPD montre clairement que les traitements de données qui reposent sur une **base légale** sont en principe exclus. Par conséquent, les traitements de données effectués par des organes fédéraux, qui sont liés par le principe de légalité, ne relèvent généralement pas du droit à la portabilité des données. 30

IV. CONSÉQUENCE JURIDIQUE : LE TRANSFERT

Si les conditions énoncées au point III sont remplies de manière cumulative, la personne concernée peut exiger que les données lui soient remises (al. 1) ou qu'elles soient transférées à un autre responsable du traitement (al. 2). Tant la remise que le transfert des données doivent s'effectuer dans un format électronique couramment utilisé (cf. N. 38 et suivantes). 31

L'exercice du droit à la portabilité ne modifie pas la **relation juridique** entre la personne concernée et le responsable du traitement. Un consentement donné une fois n'est pas réputé révoqué, et cela ne change rien à une 32

éventuelle relation contractuelle entre les parties. Le responsable du traitement peut continuer à invoquer des motifs de justification. Par conséquent, il n'est pas tenu de supprimer les données transférées.

A. À la personne concernée (remise des données ; al. 1)

33 En vertu de l'hypothèse de base de l'art. 28, al. 1, LPD, le responsable du traitement remet les données **à la personne concernée**. Celle-ci peut ensuite utiliser les données à des fins purement personnelles (par exemple, enregistrer désormais localement sur son ordinateur une collection de photos) ou les transmettre de son propre chef à un tiers de son choix. Cette dernière opération ne repose toutefois pas sur l'article 28 de la LPD.

B. À un responsable du traitement (transfert de données ; al. 2)

34 Conformément à l'article 28, al. 2, de la LPD, un **transfert direct à des tiers** (désignés à l'article 28 comme un « autre responsable du traitement ») est également possible à la demande de la personne concernée. Pour cela, toutes les conditions prévues à l'al. 1 doivent d'abord être remplies. En outre, le transfert ne doit pas nécessiter un effort disproportionné. L'al. 2 est respecté lorsque le tiers peut obtenir les données directement auprès du responsable ayant la légitimation passive, par exemple parce que celui-ci lui en accorde l'accès via une interface de programmation (API). Il n'existe toutefois aucun droit à cela.

35 L'art. 21, al. 3, de l'OPDo précise qu'il y a charge disproportionnée lorsque le **transfert n'est techniquement pas possible**. Une telle impossibilité ne devrait toutefois pratiquement jamais se présenter, car la remise des données à la personne concernée n'est, d'un point de vue technique, ni plus simple ni plus complexe que le transfert de données à un autre responsable du traitement. Étant donné que le responsable du traitement est légalement tenu de remettre les données en vertu de l'al. 1, un transfert de données au sens de l'al. 2 devrait également être possible en règle générale (sans effort disproportionné). Cela vaut d'autant plus que le responsable du traitement doit, dès le départ, concevoir ses systèmes de manière à pouvoir remplir ses obligations légales (art. 7 LPD).

36 Il est vrai qu'un tiers n'est pas tenu d'accepter les données ni de veiller à la faisabilité technique du transfert. Il ne joue **aucun rôle au regard de la**

protection des données tant qu'il n'a pas reçu de données à caractère personnel et qu'il ne les traite donc pas. À cet égard, la désignation d'« autre responsable du traitement » dans la loi prête à confusion, d'autant plus que l'art. 28 LPD – contrairement à l'art. 20 de la DSGVO – ne prévoit pas d'interdiction d'entrave qui imposerait une obligation à l'« autre responsable du traitement » dans le cadre du droit à la portabilité des données. En vertu de la réglementation de l'UE, on postule donc que la faisabilité technique doit se rapporter à la relation entre le responsable du traitement et le tiers. Un transfert est toujours considéré comme disproportionné lorsque les systèmes de traitement des données du responsable du traitement et du tiers ne sont pas compatibles. Cette condition se rapporte donc à une caractéristique du tiers, sans pour autant lui imposer d'obligation.

Les coûts supportés par le responsable du traitement ne permettent pas de conclure à une charge disproportionnée. Le droit à la portabilité des données est un droit de la personne concernée qui doit être garanti indépendamment des éventuels coûts de mise en œuvre. Les coûts liés au transfert à un tiers ne peuvent donc pas être invoqués, d'autant plus qu'il est difficile de voir en quoi un tel transfert devrait entraîner des coûts plus élevés que la remise des données à la personne concernée. 37

C. Format des données

L'art. 28 LPD prévoit la communication ou le transfert dans un **format électronique courant**. Il doit s'agir de formats de données permettant, avec un effort proportionné, de transférer les données et de les réutiliser par la personne concernée ou par un autre responsable du traitement (cf. art. 21, al. 1, OPDo). 38

Cette précision n'étant guère utile, **il convient de se référer à la disposition de l'art. 20 de la DSGVO**, même si le libellé suisse s'est plutôt inspiré de celui du droit d'accès prévu à l'art. 15, al. 3, de la DSGVO. L'art. 20 de la DSGVO parle d'un « format structuré, couramment utilisé et lisible par machine ». 39

1. Courant

Un format est considéré comme courant lorsqu'il est largement utilisé dans le secteur concerné pour le type de données en question et dans la zone 40

géographique pertinente. Toutefois, il ne faut pas accorder une importance excessive à la zone géographique. Dans l'économie mondialisée des données, la Suisse n'est pas un îlot technologique et l'exigence de caractère courant serait ainsi fixée à un niveau inutilement élevé. Le caractère courant ne correspond pas non plus à l'état de la technique. Ce qui importe, ce n'est pas de savoir quel format semble le « meilleur », mais quel est **le plus répandu** et qui a ainsi fait ses preuves dans la pratique. Par conséquent, un format est considéré comme courant lorsqu'il s'est imposé comme norme. Il convient donc de se baser en premier lieu sur les normes et les usages du secteur.

41 Il convient toutefois d'en exclure les **formats propriétaires**, qui sont certes peut-être répandus, mais dont la licence n'est accessible qu'à un coût élevé. Ils ne doivent pas être considérés comme courants, pas plus que les formats utilisés uniquement en interne. À l'inverse, **les formats ouverts ne sont pas courants en soi**, mais doivent être d'usage courant et répandus. S'il n'existe pas (encore) de formats courants dans un secteur donné, le responsable doit recourir à des formats ouverts d'usage courant, tels que XML, JSON ou CSV.

42 Le caractère courant doit être évalué du **point de vue du responsable jouissant de la légitimation passive** : un fichier DICOM (pour Digital Imaging and Communications in Medicine, avec l'extension .dcm) peut être inhabituel pour une patiente, mais il est courant en radiologie. Cela vaut également lorsque le responsable du traitement exerce son activité dans un secteur différent de celui du tiers auquel les données doivent être transférées. Cela peut toutefois constituer un obstacle réel à un transfert intersectoriel.

2. Format électronique

43 Un format électronique correspond en substance à la lisibilité par machine au sens de la DSGVO. Dans ce cadre, la lisibilité par machine est considérée comme une véritable « exigence de forme » pour la société numérique, car c'est elle seule qui permet le traitement automatisé des informations par des ordinateurs. Étant donné que le droit à la portabilité des données vise l'économie des données, le format doit garantir l'importation automatique des données dans un système informatique sous une forme structurée. Les données doivent donc être **traitables électroniquement** et pouvoir faire l'objet d'un traitement automatisé.

Dans certains cas précis, la réglementation suisse peut toutefois être plus restrictive que la lisibilité par machine. Alors que l'on débat parfois, dans le cadre de la DSGVO, de la question de savoir si les impressions informatiques doivent être considérées comme lisibles par machine en raison de la possibilité technique de reconnaissance optique de caractères (OCR), celles-ci ne doivent manifestement pas être classées comme un format électronique au regard de la LPD. 44

3. Absence d'exigence d'interopérabilité

Les exigences relatives au format des données n'impliquent aucune obligation d'interopérabilité. L'interopérabilité ne concerne d'ailleurs pas les données (ou leurs formats), mais les systèmes qui entretiennent un échange bidirectionnel. Cela nécessiterait donc non seulement l'échange de données, mais aussi l'**interaction entre différents systèmes**. Ainsi, un réseau social pourrait par exemple permettre à une utilisatrice de transférer ses photos vers un autre fournisseur. En revanche, l'interopérabilité entre deux réseaux sociaux ne serait atteinte que si, par exemple, un commentaire publié sous une photo pouvait s'afficher sur un autre réseau social et faire l'objet d'une interaction avec celui-ci (notamment par le biais d'un nouveau commentaire). Les différents systèmes doivent donc non seulement être capables d'échanger des données, mais aussi s'accorder sur les conditions applicables à ces données. 45

L'article 21, al. 2, de l'OPDo précise en ce sens que le droit à la portabilité n'implique **aucune obligation** pour le responsable du traitement d'adopter ou de maintenir des systèmes de traitement de données techniquement compatibles. Cette obligation n'existe bien entendu pas non plus pour les tiers, qui ne sont pas tenus de reprendre les données transférées. Les dispositions de la LPD et de l'OPDo n'imposent pas non plus d'obligation d'assurer l'interopérabilité entre les systèmes. 46

Dans ses commentaires, l'OFJ suggère en outre que les informations transmises soient décrites avec précision dans des formats interopérables, accompagnées de métadonnées appropriées et compréhensibles, afin qu'elles puissent être intégrées de manière pertinente dans un nouveau système. Les métadonnées doivent être suffisamment détaillées pour permettre l'utilisation et la réutilisation des données sans divulguer de secrets d'affaires. Cela suggère une obligation de traitement de (nouvelles) métadonnées, à laquelle il 47

ne faut pas se conformer. L'art. 28 LPD établit simplement, notamment au regard de l'art. 21, al. 2, OPD, un **droit à obtenir les données** *« telles quelles »*. Cela inclut également les éventuelles métadonnées qui permettent, par exemple, de structurer un ensemble de données plus volumineux. On ne peut toutefois en déduire une obligation de compléter les métadonnées (parfois par des données dont le responsable du traitement n'a peut-être même pas besoin dans son système). Cela d'autant plus que la réglementation suisse, contrairement à l'article 20 de la DSGVO, ne mentionne justement pas expressément l'exigence d'une structure. De plus, les métadonnées qui peuvent techniquement être contenues dans un format donné peuvent varier en fonction du format (courant) utilisé. Il convient donc de ne remettre aux personnes concernées que les métadonnées qui sont contenues dans un format électronique courant au sens de l'art. 28 LPD.

V. MODALITÉS (AL. 3 ET OPDDO)

48 L'article 28, al. 3, de la LPD prévoit que le responsable du traitement doit en principe transférer les données à caractère personnel gratuitement. En outre, l'article 22 de l'OPDo précise le délai, la compétence et d'autres modalités. L'article 22 de l'OPDo se limite toutefois à renvoyer, par analogie, aux **modalités du droit d'accès**, sans aborder le fond du droit à la portabilité des données. En principe, il est donc possible de se référer aux considérations relatives au droit d'accès.

A. Forme et délai

49 L'article 22, en liaison avec l'article 16, al. 1, de l'OPDo, exige de la personne concernée une **demande écrite**. Dans celle-ci, la personne doit s'identifier (art. 22, en liaison avec l'article 16, al. 5, de l'OPDo). Elle peut le faire, par exemple, en joignant une copie de sa pièce d'identité à sa demande. Le plus souvent, toutefois, l'identification devrait s'effectuer par le fait que la personne concernée dépose la demande **directement depuis son compte (connecté)** auprès du responsable du traitement. Dans ces cas, le responsable du traitement devrait toutefois prendre des précautions particulières au regard des exigences en matière de sécurité des données (par exemple en mettant en place des mécanismes de détection des tentatives de connexion inhabituelles provenant d'adresses IP étrangères). Avec l'accord du

responsable du traitement, la demande peut également être formulée oralement, ce qui devrait toutefois être rare.

Le transfert doit avoir lieu **dans un délai de 30 jours à compter de la réception de la demande** (art. 22 en liaison avec l'art. 18, al. 1, OPDo). Si le transfert ne peut avoir lieu dans ce délai, le responsable du traitement doit en informer la personne concernée et lui indiquer dans quel délai le transfert pourra être effectué (art. 22 en liaison avec l'art. 18, al. 2, OPDo). Toute restriction éventuelle doit également être communiquée dans le même délai (art. 22 en liaison avec l'art. 18, al. 3, OPDo). 50

Il n'y a pas d'obligation de fournir un flux de données continu ou périodique. Le responsable du traitement n'est pas non plus tenu d'accorder un accès illimité aux données à la personne concernée ou à l'autre responsable du traitement (par exemple via l'accès à une interface). Le droit à la portabilité des données est conçu comme un **mécanisme de transfert statique** et ne fournit donc qu'un « instantané ». 51

À l'instar du droit d'accès, le droit à la portabilité des données peut ainsi en principe être accordé **sous n'importe quelle forme**. Il est par exemple possible d'envoyer une clé USB par la poste ou de procéder à un envoi électronique par e-mail. Il est également possible, notamment pour les ensembles de données volumineux, que le responsable du traitement propose une connexion à une API ou la possibilité de télécharger directement depuis ses serveurs (par exemple depuis un serveur SFTP, une interface web sécurisée ou un portail web). 52

B. Compétence

Le droit à la portabilité des données s'adresse **au responsable du traitement**, même si les données sont stockées chez un sous-traitant. S'il existe plusieurs responsables du traitement, la personne concernée peut faire valoir son droit auprès de chacun d'entre eux individuellement (art. 22 en liaison avec l'art. 17, al. 1, de l'OPDo). Les responsables du traitement sont tenus, dans chaque cas, de traiter la demande et non pas simplement de la transmettre. Les sous-traitants doivent aider le responsable du traitement à répondre à la demande ou y répondre eux-mêmes, pour le compte du responsable du traitement (art. 22 en liaison avec l'art. 17, al. 2, de l'OPDo). Le 53

sous-traitant doit donc fournir au responsable du traitement les données pertinentes pour la portabilité si ce dernier n'en dispose pas lui-même.

C. Gratuité

54 Le responsable du traitement doit remettre ou transférer les données **gratuitement** (art. 28, al. 3, LPD). À titre exceptionnel, une **participation financière pouvant aller jusqu'à 300 CHF est autorisée** si le transfert de données implique un effort disproportionné (art. 22 en liaison avec l'art. 19, al. 1 et 2, de l'OPDo). Cela peut par exemple être le cas (rarement) lorsqu'un tri fastidieux entre les données de tiers et celles de la personne concernée s'avère nécessaire. Le responsable du traitement doit communiquer au préalable le montant de la participation à la personne concernée (art. 22 en liaison avec l'art. 19, al. 3, de l'OPDo).

Remarque :

La structure et le contenu du présent commentaire s'inspirent de la thèse de doctorat de l'auteur consacrée au droit à la portabilité des données. Les notes de bas de page n'y font spécifiquement référence que lorsqu'elles contiennent des explications plus approfondies.

BIBLIOGRAPHIE

Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz (DSG), 2. Aufl., Bern 2023 (zit.: SHK-Autor/in, Art. ... DSG N. ...).

Benhamou Yaniv/Cottier Bertil (Hrsg.), Petit commentaire LPD, Loi sur la protection des données, Basel 2023 (zit.: PC-Autor/in, Art. ... DSG N. ...).

Berners-Lee Tim, Long Live the Web, Scientific American 2010, 80–85.

Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023 (zit.: OFK-Autor/in, Art. ... DSG N. ...).

Bieri Adrian/Powell Julian, Die Totalrevision des Bundesgesetzes über den Datenschutz, Jusletter 16.11.2020.

Brorsen Hans/Falk Richard, Die «Maschinenlesbarkeit» von Informationen, Unter der Haube der EU-Digitalregulierung, MMR 2025, 7–12.

Cattaneo Gianni, Legge federale sulla protezione dei dati (nLPD) e Ordinanza sulla protezione dei dati (nOPDa): struttura, principi e obblighi nel settore privato, in: Bernasconi Giorgio A./Pasucci Paola (Hrsg.), Protezione dei dati personali: orizzonte 2023, Introduzione alle nuove norme di livello federale e cantonale, Basel 2024, 3–67.

Drepper Johannes/Schlünder Irene/Buckow Karoline, Praktische Umsetzbarkeit der Datenportabilität im Bereich der medizinischen Forschung, in: Stiftung Datenschutz, Praktische Umsetzung des Rechts auf Datenübertragbarkeit, Rechtliche, technische und verbraucherbezogene Implikationen, 3. Aufl., Leipzig 2018, 178–196.

Ehmann Eugen/Selmayr Martin (Hrsg.), Beck'scher Kurz-Kommentar zur Datenschutz-Grundverordnung, 3. Aufl., München 2024 (zit.: KUKO-Autor/in, Art. ... DSGVO N. ...).

Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J. (Hrsg.), St. Galler Kommentar zur schweizerischen Bundesverfassung, 4. Aufl., Zürich et al. 2023 (zit.: SGK-Autor/in, Art. 13 BV N. ...).

Engels Barbara, Data portability among online platforms, Internet Policy Review 2/2016, 1–17.

Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit, Bericht vom 17.8.2018, <https://perma.cc/YB65-ECG9> (zit.: Expertengruppe Zukunft).

Fix Alexander Daniel, Das Recht auf Datenportabilität, Art. 20 DSGVO als Schnittstelle zwischen Wettbewerbsförderung und Datenschutz, Berlin 2022.

Götzinger Lena/Vasella David, Datenportabilität und ihre Umsetzung, SZW 2021, 40–51.

Kratz Alexander, Datenportabilität und «Walled Gardens», InTeR 2019, 26–31.

Krause Peter, Datenportabilität, Pflichten für Verantwortliche im Rahmen des Rechts auf Datenübertragbarkeit (Teil 2), PinG 2019, 13–20.

Landolt Robin, Datenkooperationen, Der unternehmensübergreifende Zugang zu Daten im Spannungsfeld zwischen Datenschutz und Wettbewerbsförderung, Zürich 2024.

Laux Christian, Das Recht auf Datenportabilität, digma 2019, 166–170.

Mahon Pascal, Le droit à l'intégrité numérique : réelle innovation ou simple évolution du droit ? Le point de vue du droit constitutionnel, in: Guillaume Florence/Mahon Pascal (Hrsg.), Le droit à l'intégrité numérique, Basel 2021, 43–63.

Mätzler Samuel, Das Recht auf Datenportabilität, Eine rechtsvergleichende Untersuchung von Art. 28 DSG anhand dreier Datenökosysteme, Zürich 2026.

Meier Philippe/Métille Sylvain (Hrsg.), Loi fédérale sur la protection des données, Commentaire Romand, Basel 2023 (zit.: CR-Autor/in, Art. … DSG N. …).

Métille Sylvain, Loi fédérale sur la protection des données révisée : principes généraux et nouveautés, in: Défago Valérie/Dunand Jean-Philippe/Mahon Pascal/Posse-Ousmane Samah/Raedler David (Hrsg.), La protection des données dans les relations de travail à la lumière de la nouvelle loi fédérale sur la protection des données, Genf et al. 2024, 3–47.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16.11.2020.

Schweitzer Heike, Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, GRUR 2019, 569–579.

Sperlich Tim, Informationelle Selbstbestimmung zwischen Wettbewerbs- und Datenschutzrecht, Eine Analyse und Beurteilung der Wechselwirkungen zwischen dem Wettbewerbs- und Datenschutzrecht, Berlin 2021.

Steiner Thomas, Zwischen Autonomie und Angleichung, Eine Analyse zur Anwendung des neuen DSG im Lichte der DSGVO, in: Widmer Michael (Hrsg.), Datenschutz, Rechtliche Schnittstellen, Zürich 2023, 51–138.

Steiner Thomas/Morand Anne-Sophie/Hürlimann Daniel (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz, Version vom 31.7.2023 (zit.: OK-Autor/in, Art. … DSG N. …).

Swire Peter P./Lagos Yianni, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, Maryland Law Review 2013, 335–380.

Swiss Data Alliance, Leitlinie zur Umsetzung der Datenübertragbarkeit in der Schweiz, Version 1.0 vom 20.8.2020.

Thouvenin Florent, Informationelle Selbstbestimmung: Intuition, Illusion, Implosion, ZSR Beiheft 2023.

Thouvenin Florent/Weber Rolf H./Früh Alfred, Elemente einer Datenpolitik, Zürich et al. 2019.

Vasella David/Blechta Gabor-Paul (Hrsg.), Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 4. Aufl., Basel 2024 (zit.: BSK-Autor/in, Art. ... DSG N. ...).

Weber Rolf H./Thouvenin Florent, Gutachten zur Möglichkeit der Einführung eines Datenportabilitätsrechts im schweizerischen Recht und zur Rechtslage bei Personal Information Management Systems (PIMS) vom 22.12.2017.

Wolff Heinrich Amadeus/Brink Stefan/von Ungern-Sternberg Antje (Hrsg.), BeckOK Datenschutzrecht, 53. Aufl., München 2025 (zit.: BeckOK DSR-Autor/in, Art. ... DSGVO N. ...).

Ziegler Noémi/Vasella David, Informationelle Selbstbestimmung, Was leistet das Datenschutzrecht für die Selbstbestimmung der Betroffenen?, digma 2019, 158–164.

MATÉRIAUX

Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, zuletzt überarbeitet und angenommen am 5.4.2017.

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 6941 ff. (zit.: Botschaft DSG 2017).

Bundesamt für Justiz, Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016 (zit.: BJ, Erläuternder Bericht VE-DSG).

Bundesamt für Justiz, Erläuternder Bericht Verordnung über den Datenschutz (Datenschutzverordnung, DSV) vom 31.8.2022 (zit.: BJ, Erläuternder Bericht DSV).

Bundesamt für Kommunikation, «Massnahmen für eine zukunftsorientierte Datenpolitik der Schweiz», Medienmitteilung vom 9.5.2018, <https://perma.cc/VJE24KLZ> (zit.: BAKOM, Medienmitteilung vom 9.5.2018).

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Das neue Datenschutzgesetz aus Sicht des EDÖB vom 9.2.2021 (zit.: EDÖB).

Fahne 17.059, Datenschutzgesetz, Teilrevision und Änderung weiterer Erlasse zum Datenschutz, Entwurf 3 Herbstsession 2019, Beschluss Nationalrat, <https://perma.cc/JQL2-XP5J> (zit.: Fahne 17.059, Beschluss Nationalrat).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 29 LPD

Un commentaire de Samuel Mätzler

PROPOSITION DE CITATION

Samuel Mätzler, Commentaire de l'art. 29 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Mätzler, art. 29 LPD N. XXX.

Art. 29 Restrictions du droit à la remise ou à la transmission des données personnelles

[1] Le responsable du traitement peut refuser, restreindre ou différer la remise ou la transmission de données personnelles pour les mêmes motifs que ceux prévus à l'art. 26, al. 1 et 2.

[2] Le responsable du traitement indique le motif pour lequel il refuse, restreint ou diffère la remise ou la transmission des données personnelles.

TABLE DES MATIÈRES

En bref 433
I. Généralités 433
A. Objectif de la norme et contexte 433
B. Remarques de droit comparé 434
II. Motifs de limitation (al. 1 en liaison avec l'article 26) 434
A. Base légale, notamment le secret professionnel (article 26, al. 1, let. a)) 434
B. Intérêts prépondérants de tiers (art. 26, al. 1, let. b) 435
C. Caractère manifestement infondé (art. 26, al. 1, let. c) 436
D. Autres motifs de restriction (art. 26, al. 2) 436
III. Conséquence juridique 437
IV. Obligation de motivation (al. 2) 437
Bibliographie 438
Matériaux 439

EN BREF

L'article 29 de la LPD énonce les motifs pouvant justifier une restriction du droit à la communication ou au transfert des données prévu à l'article 28 de la LPD. Il renvoie à cet égard aux motifs de restriction du droit d'accès. Cette disposition vise à empêcher que la personne concernée puisse, en invoquant le droit à la portabilité des données, obtenir des données qui ne relèvent pas du droit d'accès. Toutefois, le renvoi général au droit d'accès ne tient pas suffisamment compte des spécificités du droit à la portabilité des données, ce qui peut entraîner des incohérences dans divers cas.

I. GÉNÉRALITÉS

A. Objectif de la norme et contexte

L'article 29 de la LPD définit les motifs pour lesquels un responsable du traitement peut limiter la communication ou le transfert de données au sens de l'article 28 de la LPD (également appelé « droit à la portabilité des données »). Cette disposition n'énumère toutefois pas ces motifs de manière autonome, mais renvoie aux **motifs de limitation du droit d'accès** prévus à l'art. 26, al. 1 et 2, de la LPD. C'est pourquoi les considérations qui y figurent peuvent, pour l'essentiel, être transposées au droit à la portabilité. 1

Le renvoi général aux motifs de limitation du droit d'accès n'est pas sans susciter de controverses, car ces deux droits des personnes concernées **poursuivent des objectifs différents** et les motifs de limitation ne s'appliquent pas toujours aux **différents cas d'application**. Ce renvoi permet toutefois d'empêcher que les limitations du droit d'accès puissent être contournées au moyen du droit à la portabilité des données. 2

Tout comme le droit à la portabilité des données, l'article 29 LPD n'a été introduit qu'au cours des **débats parlementaires**, à l'occasion de la révision de la LPD. Cette disposition n'a pas fait l'objet d'un examen distinct et n'a pas suscité de controverse. 3

B. Remarques de droit comparé

4 L'article 29 LPD a été repris **par analogie de la DSGVO**. Toutefois, la DSGVO ne prévoit pas de disposition distincte. Au contraire, la DSGVO restreint le droit à la portabilité des données à plusieurs endroits. Conformément à l'article 12, al. 5, let. 1 de la DSGVO, le responsable du traitement peut subordonner le transfert de données à une rémunération raisonnable en cas de demandes manifestement infondées ou excessives (let. a) ou le refuser purement et simplement (let. b). Il lui incombe alors d'apporter la preuve du caractère abusif de la demande (art. 12, al. 5, sous-paragraphe 2, de la DSGVO).

5 Conformément à l'art. 20, al. 4, de la DSGVO, le droit à la portabilité ne doit pas porter atteinte aux **droits et libertés d'autrui**. Selon une opinion largement dominante, cela s'applique également au responsable du traitement. Ainsi, le droit à la portabilité prévu par la DSGVO peut être limité par des secrets d'entreprise et d'affaires ou par la propriété intellectuelle, tels que les droits d'auteur.

6 En outre, la DSGVO prévoit, à l'article 20, al. 3, deuxième phrase, une **exclusion expresse** pour les traitements qui sont dans l'intérêt public ou qui sont effectués dans l'exercice de l'autorité publique. En outre, d'autres restrictions peuvent être prévues en droit de l'Union ou en droit d'un État membre, sous réserve des conditions prévues à l'article 23 de la DSGVO. Conformément à l'article 85, al. 2, et à l'article 89, al. 3, de la DSGVO, d'autres dérogations sont également possibles, susceptibles de limiter le droit à la portabilité des données dans certaines situations.

II. MOTIFS DE LIMITATION (AL. 1 EN LIAISON AVEC L'ARTICLE 26)

A. Base légale, notamment le secret professionnel (article 26, al. 1, let. a))

7 Une restriction du droit à la portabilité est admissible si elle est prévue par une loi au sens formel (art. 29, al. 1, en liaison avec l'art. 26, al. 1, let. a, LPD). Une telle base légale doit se rapporter au droit à la portabilité des données et

devrait **être examinée au cas par cas**. À ce jour, il n'existe toutefois aucune base légale correspondante.

La disposition relative au droit d'accès cite à titre d'exemple la protection du secret professionnel. Il apparaît ainsi que la référence au droit d'accès **n'est guère convaincante**, car le droit à la portabilité ne concerne que les données qui se rapportent à la personne concernée et qui ont également été communiquées par celle-ci au responsable du traitement. Les secrets professionnels visent en revanche principalement à protéger cette personne concernée. Étant donné que la personne concernée exerce toujours son droit à la portabilité de sa propre initiative et qu'il y a donc consentement, le secret professionnel n'est pas violé (voir art. 321, ch. 2, CP). 8

B. Intérêts prépondérants de tiers (art. 26, al. 1, let. b)

Le responsable du traitement peut restreindre le droit à la portabilité si cela s'avère nécessaire en raison d'intérêts prépondérants de tiers (art. 29, al. 1, en liaison avec l'art. 26, al. 1, let. b, LPD). Dans ce contexte, l'accent est mis sur le **transfert des données à un tiers ou à un double destinataire**, mais les secrets d'affaires ou les droits de propriété intellectuelle de tiers peuvent également entrer en ligne de compte. En revanche, les restrictions fondées sur les intérêts du responsable du traitement doivent être prises en compte en vertu de l'art. 26, al. 2, LPD. 9

En ce qui concerne les intérêts de tiers, il convient de procéder à une **mise en balance des intérêts**. Il ne faut pas présumer à la légère que les intérêts de tiers prévalent : les données en question sont toujours celles qui se rapportent (au moins en partie) à la personne concernée et qui ont de toute façon été communiquées par celle-ci au responsable du traitement. Compte tenu de la décision du législateur de permettre à la personne concernée de disposer de « ses » données grâce au droit à la portabilité des données, le motif de restriction ne doit donc **pas être interprété de manière trop large**. Toutefois, il est également vrai qu'en cas de doute, le responsable du traitement devrait plutôt accepter une éventuelle violation du droit à la portabilité des données – qui n'est pas passible de sanctions en vertu de la LPD – plutôt que la violation des droits de tiers. 10

C. Caractère manifestement infondé (art. 26, al. 1, let. c)

11 Si une demande est manifestement infondée, le responsable du traitement peut également restreindre le droit à la portabilité des données (art. 29, al. 1, en liaison avec l'art. 26, al. 1, let. c, LPD). À titre d'exemple, l'article 26 de la LPD, qui porte spécifiquement sur le droit d'accès, cite les cas dans lesquels une demande poursuit une **finalité contraire à la protection des données** ou est **manifestement vexatoire**. La possibilité de restreindre la portabilité en cas de finalité contraire à la protection des données est toutefois difficilement compatible avec le droit à la portabilité, compte tenu des objectifs en matière de protection des données et de droit de la concurrence. Le droit à la portabilité des données vise notamment à garantir la libre circulation des données, raison pour laquelle une demande ne devrait **pas être considérée à la légère comme manifestement infondée**. Cette référence au droit d'accès est donc elle aussi insatisfaisante. Le droit à la portabilité vise à permettre le transfert de données entre différents acteurs de la manière la plus standardisée possible et sans tenir compte de l'équité au cas par cas. En conséquence, on ne sait pas clairement dans quels cas le responsable du traitement peut refuser une demande au titre de ce droit.

12 On peut toutefois présumer qu'une demande est non fondée lorsque le droit à la portabilité est exercé de **manière abusive**. Il est également fait mention du cas d'une **obtention de preuves** à l'encontre du responsable dans le cadre d'une procédure civile.

D. Autres motifs de restriction (art. 26, al. 2)

13 L'art. 29, al. 1, LPD renvoie en outre à l'art. 26, al. 2, LPD. Ce dernier prévoit d'autres motifs de restriction pour les personnes privées (let. a) et pour les organes fédéraux (let. b). Étant donné que ces derniers ne sont que rarement légitimés à être partie défenderesse en matière de droit à la portabilité des données, les motifs de restriction **applicables aux organes fédéraux** ne peuvent guère revêtir d'importance d'emblée.

14 Il est en revanche concevable qu'un **responsable du traitement privé** souhaite limiter le portage parce que ses intérêts prépondérants l'exigent (let. a, ch. 1). Un responsable du traitement peut ainsi, en vertu de l'art. 29, al. 1, en liaison avec l'art. 26, al. 2, let. a, LPD, invoquer ses **propres secrets d'affaires et droits de propriété intellectuelle** comme motif de restriction. Dans

l'ensemble, cela ne devrait toutefois être que rarement le cas, car seules les données communiquées par la personne concernée relèvent du droit à la portabilité des données, tandis que les données dérivées, c'est-à-dire celles qui reposent sur une prestation du responsable du traitement, sont exclues du champ d'application. Le législateur a, en principe, déjà subordonné les intérêts du responsable du traitement à ceux de la personne concernée et de la concurrence lors de l'introduction du droit à la portabilité des données, raison pour laquelle ce dernier ne devrait que rarement pouvoir invoquer des secrets d'affaires.

Si le responsable du traitement souhaite limiter le portage en invoquant ses intérêts prépondérants, l'art. 26, al. 2, let. a, de la LPD énonce une condition supplémentaire qui doit être remplie. Le responsable du traitement ne doit pas être autorisé à **communiquer les données à caractère personnel à des tiers** (let. a, ch. 2). Cette condition n'est toutefois pas compatible avec le droit au transfert des données prévu à l'art. 28, al. 2, LPD et est donc, selon le présent avis, **sans importance** en tant que condition de restriction. On peut également en conclure que le responsable du traitement ne peut pas du tout se fonder sur l'art. 26, al. 2, let. a, LPD lorsque la personne concernée demande un transfert de données. 15

III. CONSÉQUENCE JURIDIQUE

En présence d'un motif de restriction admissible, le responsable du traitement peut **refuser, restreindre ou reporter** la portabilité. Ce faisant, il doit respecter le principe de proportionnalité et garantir le droit à la portabilité des données de la manière la plus **complète possible**. Il convient donc de toujours examiner la possibilité d'un report ou d'une restriction avant d'envisager un refus. 16

IV. OBLIGATION DE MOTIVATION (AL. 2)

Conformément à l'art. 29, al. 2, LPD, le responsable du traitement doit indiquer les raisons pour lesquelles il refuse, limite ou reporte la portabilité. Cela correspond à l'obligation à laquelle un responsable du traitement doit également se conformer dans le cadre du droit d'accès (voir art. 26, al. 4, LPD). Le responsable du traitement doit **informer** la personne concernée *du fait que* la portabilité est refusée, restreinte ou reportée et en **motiver** les 17

raisons en conséquence. Un **délai de 30 jours** à compter de la réception de la demande s'applique également dans ce cas (art. 22 en liaison avec l'art. 18, al. 3, OPDo). Pour plus de détails, il convient de se reporter au commentaire de l'art. 25 LPD.

Remarque :

La structure et le contenu du présent commentaire s'inspirent de la thèse de doctorat de l'auteur consacrée au droit à la portabilité des données. Les notes de bas de page n'y font spécifiquement référence que lorsqu'elles contiennent des explications plus approfondies.

BIBLIOGRAPHIE

Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz (DSG), 2. Aufl., Bern 2023 (zit.: SHK-Autor/in, Art. ... DSG N. ...).

Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023 (zit.: OFK-Autor/in, Art. ... DSG N. ...).

Erard Frédéric/di Tria Livio, Consentement aux traitements de données en cabinet médical, Ni libre, ni éclairé, ni nécessaire ?, Jusletter 23.9.2024.

Gola Peter/Heckmann Dirk (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Kommentar, 3. Aufl., München 2022 (zit.: GK-Autor/in, Art. ... DSGVO N. ...).

Landolt Robin, Datenkooperationen, Der unternehmensübergreifende Zugang zu Daten im Spannungsfeld zwischen Datenschutz und Wettbewerbsförderung, Zürich 2024.

Mätzler Samuel, Das Recht auf Datenportabilität, Eine rechtsvergleichende Untersuchung von Art. 28 DSG anhand dreier Datenökosysteme, Zürich 2026.

Meier Philippe/Métille Sylvain (Hrsg.), Loi fédérale sur la protection des données, Commentaire Romand, Basel 2023 (zit.: CR-Autor/in, Art. ... DSG N ...).

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16.11.2020.

Steiner Thomas/Morand Anne-Sophie/Hürlimann Daniel (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz, Version vom 31.7.2023 (zit.: OK-Autor/in, Art. ... DSG N. ...).

Taeger Jürgen/Gabel Detlev (Hrsg.), Kommunikation & Recht Kommentar zu DSGVO/BDSG/TDDDG, 4. Aufl., Frankfurt am Main 2022 (zit.: KRKomm-Autor/in, Art. ... DSGVO N. ...).

Vasella David/Blechta Gabor-Paul (Hrsg.), Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, 4. Aufl., Basel 2024 (zit.: BSK-Autor/in, Art. ... DSG N. ...).

MATÉRIAUX

Artikel 29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, zuletzt überarbeitet und angenommen am 5.4.2017.

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 6941 ff. (zit.: Botschaft DSG 2017).

Fahne 17.059, Datenschutzgesetz, Teilrevision und Änderung weiterer Erlasse zum Datenschutz, Entwurf 3 Herbstsession 2019, Beschluss Nationalrat, <https://perma.cc/JQL2-XP5J> (zit.: Fahne 17.059, Beschluss Nationalrat).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 31 al. 2 let. e LPD

Un commentaire de Philipp do Canto

PROPOSITION DE CITATION

Philipp do Canto, Commentaire de l'art. 31 al. 2 let. e LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-do Canto, art. 31 al. 2 let. e LPD N. XXX.

Art. 31 Motifs justificatifs

[1] [...]

[2] Les intérêts prépondérants du responsable du traitement entrent notamment en considération dans les cas suivants:

a. [...]

b. [...]

c. [...]

d. [...]

e. les données personnelles sont traitées à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, si les conditions suivantes sont réunies:

le responsable du traitement anonymise les données dès que la finalité du traitement le permet; si une anonymisation est impossible ou exige des efforts disproportionnés, il prend des mesures appropriées afin que les personnes concernées ne puissent pas être identifiées,
s'il s'agit de données sensibles, le responsable du traitement ne les communique à des tiers que sous une forme ne permettant pas d'identifier la personne concernée; si cela n'est pas possible, des mesures doivent être prises qui garantissent que les tiers ne traitent les données qu'à des fins ne se rapportant pas à des personnes,
les résultats sont publiés sous une forme ne permettant pas d'identifier les personnes concernées;

f. [...]

TABLE DES MATIÈRES

En bref ... 444
I. Généralités ... 444
II. al. 1, consentement, intérêt prépondérant, justifications légales. ... 444
III. al. 2 ... 444
A. Généralités / étapes de contrôle ... 444
B. Liste des cas légaux ... 444
1. let. a - d. ... 444
2. let. e, traitement à des fins non personnelles ... 444
a) Finalité non personnelle en tant qu'élément constitutif de base ... 445
b) Chiffre 1, Anonymisation ou pseudonymisation (cryptage) ... 447
c) Chiffre 2, Communication à des tiers ... 448
d) Chiffre 3, Publication des résultats ... 449
Bibliographie ... 449
Matériaux ... 450

EN BREF

[Dans l'introduction à l'article 31, par un autre rédacteur]

I. GÉNÉRALITÉS

[Généralités sur l'art. 31 ; préambule et contexte, par d'autres rédacteurs]

II. AL. 1, CONSENTEMENT, INTÉRÊT PRÉPONDÉRANT, JUSTIFICATIONS LÉGALES.

[ad art. 31 al. 1 ; par d'autres personnes].

III. AL. 2

A. Généralités / étapes de contrôle

[Généralités sur l'al. 2 ; par un autre responsable du traitement].

B. Liste des cas légaux

1. let. a - d.

[par un autre responsable du traitement].

2. let. e, traitement à des fins non personnelles

1 Le traitement à des fins non personnelles est la disposition relative aux intérêts prépondérants qui a été la plus étendue par rapport à la disposition précédente de l'art. 13 al. 2 let. e aDSG. A côté de l'ancienne réglementation sur la publication des résultats (désormais au ch. 3 de la disposition, cf. ci-dessous n. 15), s'ajoutent une obligation d'anonymisation ou de pseudonymisation le plus tôt possible (ch. 1) ainsi que, en tant qu'élément constitutif d'une infraction qualifiée, une obligation de communiquer des données personnelles sensibles à des tiers (ch. 2). Le régulateur n'intervient donc plus seulement au moment de la publication des résultats, mais directement dans la gestion interne des processus pendant le traitement. La densité accrue de la réglementation est, d'une part, la conséquence d'une

concrétisation légale de principes existants et, d'autre part, elle implique pour les responsables un renforcement des conditions lors du traitement à des fins non personnelles.

a) Finalité non personnelle en tant qu'élément constitutif de base

L'élément central de la disposition est le traitement à des fins non liées aux personnes. Les finalités non personnelles sont celles pour lesquelles l'identité de la personne concernée n'est pas pertinente. En d'autres termes, la finalité de l'activité est également remplie si des données anonymes ou codées étaient traitées. Il existe un vaste champ de finalités possibles de traitement pouvant relever de ce motif justificatif. Il ne s'agit pas seulement d'un grand nombre de personnes, mais le traitement des données d'une seule personne ou d'un groupe peut également servir à des fins non personnelles, tant qu'il ne s'agit que des caractéristiques et non de l'identité. L'identité de la personne concernée peut toutefois revêtir une importance pratique pour les responsables eux-mêmes, par exemple dans le domaine des études longitudinales, dans lesquelles des informations sont collectées à intervalles réguliers auprès des personnes concernées. 2

La loi elle-même ne définit pas la notion de finalité non personnelle, mais cite comme exemples la recherche privée, la statistique et la planification. La réglementation est donc également qualifiée de "privilège de la recherche" en matière de droit des données. Les exemples de planification cités dans la doctrine sont la planification démographique ainsi que la planification du territoire et des transports. Le privilège accordé à ces domaines est justifié par le fait qu'ils ne fournissent pas seulement des bases de décision importantes pour l'économie, mais qu'ils répondent également à de multiples besoins sociaux et publics. La mention des domaines n'est pas exhaustive. On peut notamment penser à l'exploitation des données d'utilisation d'Internet et d'applications ou à l'utilisation de modèles d'IA dans le contexte d'analyses de données volumineuses, où tout intérêt pour l'individu disparaît d'emblée. D'autre part, la mention explicite dans la loi ne signifie pas que le traitement des données dans les domaines de la recherche, des statistiques et de la planification sert toujours des finalités non personnelles. Comme exemple de finalités personnelles, on peut citer la médecine de précision, dans laquelle les résultats positifs des études doivent également profiter aux personnes concernées. D'autres activités à d'autres fins sont la recherche historique et 3

généalogique, qui ne sont pas couvertes par le privilège lorsqu'elles concernent des personnes ou des groupes spécifiques.

4 La disposition règle le traitement des données par des personnes privées. Sont donc concernées la recherche pharmaceutique privée, les études cliniques privées ou menées par des organisations privées, les études de marché et la planification dans les entreprises. En vertu de l'article 40 LPD, les activités de droit privé des organes fédéraux tombent également sous le coup de cette disposition. Les activités étatiques sont régies par l'article 39 LPD, qui contient une disposition analogue concernant le traitement de données à des fins non personnelles par des organes fédéraux.

5 Il existe également des traitements qui comportent à la fois des données à caractère personnel et des données non personnelles, notamment dans le domaine de la recherche. Dans de telles activités, on peut se demander dans quelle mesure le motif justificatif peut être invoqué. Pour les organes fédéraux, l'art. 35 OLPD stipule que les exceptions prévues à l'art. 39, al. 2, LPD ne s'appliquent qu'au traitement à des fins ne se rapportant pas à des personnes. Une réglementation analogue pour les responsables privés est donc compréhensible ; elle conduit à une considération séparée du droit des données pour différents aspects d'une activité spécifique.

6 Pour les trois domaines mentionnés dans la loi et d'autres, il convient de tenir compte de la législation spéciale qui, selon l'acte législatif, va de la norme de renvoi globale à la réglementation détaillée. Il s'agit en particulier du droit de la recherche sur l'être humain (en cours de révision) avec la LRH et les actes législatifs apparentés, comme la loi sur l'enregistrement du cancer, qui contiennent leurs propres prescriptions sur la pseudonymisation ainsi que des dispositions de triage concernant l'application de la LRH et de la LPD (p. ex. art. 28 LEMO). Dans le domaine de l'approvisionnement en électricité, l'art. 17c al. 1 LApEl renvoie à la LPD en ce qui concerne les compteurs intelligents. Dans le domaine de la statistique, la législation spéciale selon la LSF s'applique dans la mesure où elle couvre des institutions privées (art. 2 al. 3 LSF, cf. également les principes selon l'art. 4 LSF).

7 En cas de traitement à des fins ne se rapportant pas à des personnes, les différentes dispositions des chiffres 1 à 3 s'appliquent. Détails des dispositions :

b) Chiffre 1, Anonymisation ou pseudonymisation (cryptage)

Les responsables doivent en principe anonymiser les données dès que la finalité du traitement le permet. La disposition reprend ainsi le principe de l'art. 6 al. 4 LPD tout en le relativisant par une exception. Selon cette disposition, les responsables peuvent prendre d'autres mesures appropriées pour empêcher l'identification de la personne si l'anonymisation est techniquement impossible ou implique des efforts disproportionnés. Grâce au développement de logiciels de reconnaissance biométrique, il est aujourd'hui impossible d'anonymiser des portraits de personnes, alors qu'il suffisait auparavant de placer une barre noire sur le contour des yeux. Compte tenu de l'objectif de la norme, l'exception doit être appliquée avec discernement, malgré ses conséquences techniques et financières, et nécessite une pesée des intérêts au cas par cas, qui équilibre les intérêts des personnes concernées avec le privilège voulu pour les activités en question. 8

Les mesures appropriées sont notamment la pseudonymisation, le cryptage ou la codification. La pseudonymisation joue un rôle important dans la pratique et représente en même temps un défi technique. Les exigences techniques en matière de pseudonymisation ont augmenté, notamment en ce qui concerne les données obtenues à partir de matériel biologique (bio-échantillons), c'est-à-dire de parties du corps humain telles que des tissus ou des échantillons de sang. La technologie de laboratoire, en particulier l'analyse de l'ADN, facilite l'identification, le cas échéant en combinaison avec des caractéristiques d'autres échantillons. Le droit relatif à la recherche sur l'être humain prévoit des dispositions correspondantes pour le traitement du matériel biologique et des données génétiques (art. 32 ss LRH). 9

En ce qui concerne les mesures visant à empêcher l'identification, il convient de mentionner le vaste catalogue de mesures techniques et organisationnelles figurant à l'art. 3 OLPD, notamment les règles relatives à la confidentialité et à l'intégrité. Il existe en outre différentes directives sur le cryptage, comme les directives scientifiques contraignantes de l'Office fédéral de la statistique ou les directives intersectorielles de l'Agence européenne pour la cybersécurité (Enisa). Ces directives contiennent entre autres des conditions relatives à la manipulation des codes et à la dé-pseudonymisation. 10

c) Chiffre 2, Communication à des tiers

11 La deuxième édition concerne le traitement de données sensibles (sur cette notion, voir le commentaire de l'art. 5 let. c LPD). Cette disposition se réfère à l'art. 30 al. 2 let. c LPD, selon lequel la communication de telles données à des tiers constitue une atteinte à la personnalité. Comme au ch. 1, un principe est posé et celui-ci est atténué par une exception. Cette exception ne figurait pas encore dans le projet de loi et a été introduite au Conseil national.

12 Si l'élément constitutif supplémentaire des données sensibles est rempli, le principe est que celles-ci ne peuvent être transmises à des tiers que de manière à ce que la personne concernée ne soit pas identifiable. Les données ne peuvent donc être transférées que sous forme anonymisée ou cryptée. La transmission de données à des tiers n'est donc pas traitée différemment de la publication (ch. 3). Le ch. 2 veut exclure que la communication de données personnelles sensibles non anonymisées soit justifiée par le fait qu'elle est effectuée à des fins de recherche, de planification ou de statistique.

13 L'exception s'applique lorsqu'il n'est pas possible de prendre des mesures pour empêcher l'identification, ce qui peut par exemple être le cas pour les données génétiques volumineuses d'une personne. Selon le texte, la disproportion de la mesure n'est pas considérée comme un motif justificatif (cf. ch. 1). En cas d'impossibilité, il faut garantir que des tiers ne traitent les données qu'à des fins ne se rapportant pas à des personnes. La disposition n'exige pas que le but du traitement soit le même chez le tiers que chez le responsable, ce qui est compréhensible compte tenu des différents domaines d'activité dans la recherche, la statistique et la planification. L'obligation de garantie incombe en premier lieu au responsable, le ch. 2 ne contenant pas de prescriptions méthodologiques pour garantir (contractuellement) l'affectation à des fins non personnelles vis-à-vis de tiers.

14 Ensuite, le message relatif à l'aDSG fait référence aux prescriptions légales en matière de confidentialité. Lorsque celles-ci interdisent la transmission de données à des tiers, elles priment en tant que réglementation spéciale, par exemple les secrets professionnels protégés par le droit pénal (p. ex. le secret médical). Les services statistiques ou les chercheurs ne peuvent donc pas justifier la transmission de données secrètes sur la base du chiffre 2. Il en va de même pour les obligations de confidentialité contractuelles ou stipulées d'une autre manière.

d) Chiffre 3, Publication des résultats

Le ch. 3 reprend la réglementation actuelle selon laquelle les personnes concernées ne doivent pas être identifiables lors de la publication des résultats (art. 13, al. 2, let. e, aDSG). En d'autres termes, on renonce toujours à exiger une anonymisation lors de la publication. La doctrine fait remarquer que la publication d'études ne portant que sur un petit nombre de personnes peut entraîner un risque de déductions sur la personne, par exemple dans le cas d'études sur des maladies rares ou de planifications pour des zones géographiques restreintes. Lors de la publication de résultats sur la base de données de nombreuses personnes concernées, cela semble toutefois moins problématique dans la mesure où l'identification de la personne par un être humain est plus difficile. En revanche, les systèmes de reconnaissance automatique mentionnés fonctionnent indépendamment des restrictions géographiques ou numériques, de sorte que c'est finalement le progrès technique qui augmente constamment les exigences en matière de publication des résultats. 15

BIBLIOGRAPHIE

Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2022 (zit. SHK DSG-Bearbeiter/-in).

Baeriswyl Bruno, Die Einwilligung hilft (nicht) weiter, digma 2020 S. 62 ff. (zit. Baeriswyl).

Baeriswyl Bruno, "Big Data" ohne Datenschutz-Leitplanken, digma 2013 S. 14 ff. (zit. Baeriswyl, Big Data).

Baeriswyl Bruno/Pärli Kurt (Hrsg.), Datenschutzgesetz (DSG), Stämpflis Handkommentar, Bern 2015 (zit. SHK aDSG-Bearbeiter/-in).

Kasper Gabriel, People Analytics in privatrechtlichen Arbeitsverhältnissen, Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, Zürich/St. Gallen 2021 (zit. Kasper).

Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023 (zit. OFK-Bearbeiter/-in).

Blechta, Gabor-Paul/Vasella, David (Hrsg.), Datenschutzgesetz / Öffentlichkeitsgesetz, DSG/BGÖ. Basler Kommentar, 4. Aufl., Basel 2024 (zit. BSK nDSG-Bearbeiter/-in).

Laux, Christian, Introduction into the legal aspects of big data (part #3: privacy aspects – basics), Swiss Data Analytics Magazine 2015/01, S. 13 ff. (zit. Laux).

Maurer-Lambrou, Urs/Blechta, Gabor-Paul (Hrsg.), Datenschutzgesetz/ Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014 (zit. BSK-Bearbeiter/-in).

Meier Philippe, Protection des données, Fondements, principes généraux et droit privé, Bern 2010 (zit. Meier).

Reudt-Demont Janine, Digitalisierung des Gesundheitswesens 2023, LSR 2023 S. 39 ff. (zit. Reudt-Demont).

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. Rosenthal/ Jöhri (2008)).

Volz Stephanie, KI Sandboxen für die Schweiz?, SZW 2022 S. 51 ff., 56 (zit. Volz).

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 6941 ff., abrufbar https://www.fedlex.admin.ch/eli/fga/2017/2057/de (zit. Botschaft 2017).

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988 II 413 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/ de, (zit. Botschaft 1988).

Erläuterungsbericht Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz, BJ, 23.6.2021 (zit. Erläuterungsbericht).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 33 LPD

Un commentaire de Sandra Husi-Stämpfli

PROPOSITION DE CITATION

Sandra Husi-Stämpfli, Kommentierung zu Art. 33 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Husi-Stämpfli, N. XXX zu Art. 33 DSG.

Chapitre 6
Dispositions particulières pour le traitement de données personnelles par des organes fédéraux

Art. 33 Contrôle et responsabilité en cas de traitements de données personnelles conjoints

Lorsqu'un organe fédéral traite des données personnelles conjointement avec d'autres organes fédéraux, avec des organes cantonaux ou avec des personnes privées, le Conseil fédéral règle les procédures de contrôle et les responsabilités en matière de protection des données.

TABLE DES MATIÈRES

En bref 453
I. Généralités 453
A. Historique 453
B. Objectif de la norme 453
II. Pas de vide en matière de responsabilité 454
III. Responsabilité partagée 454
IV. Procédure de contrôle 454
V. Régime réglementaire 455
VI. Questions de responsabilité 455
Bibliographie 455

EN BREF

Comme le traitement de données personnelles est de plus en plus souvent effectué non seulement en commun par plusieurs services fédéraux, mais aussi en collaboration avec des services cantonaux ou communaux, voire des particuliers, il est nécessaire de définir clairement les responsabilités. L'art. 33 LPD habilite le Conseil fédéral à définir les responsabilités dans ces constellations.

I. GÉNÉRALITÉS

A. Historique

La disposition précédente de l'art. 16 aDSG a été scindée lors de la révision de la protection des données. L'art. 16 al. 1 aDSG, qui régissait la responsabilité générale, a été transféré à l'art. 5 let. j. L'art. 16 al. 2 aLPD, qui régissait la responsabilité en cas de pluralité de personnes traitant des données, a été repris à l'art. 33 LPD. 1

B. Objectif de la norme

L'art. 5 let. j LPD définit qui doit être inclus dans la notion de responsable (cf. OK-Hofmann sur l'art. 5 let. j LPD) : le point de rattachement est la souveraineté de décision sur les finalités et les moyens des opérations de traitement des données. L'organe fédéral auquel revient cette souveraineté décisionnelle est déterminé par les lois spéciales respectives qui servent de base juridique aux traitements de données. 2

Étant donné que le traitement de données personnelles est de plus en plus souvent effectué non seulement en commun par plusieurs services fédéraux, mais que les opérations de traitement de données dépassant le cadre des niveaux fédéraux font partie du quotidien et que même des personnes privées peuvent avoir accès à des bases d'informations communes, une réglementation claire des responsabilités s'impose. Dans le cas contraire, le risque existe que de nombreux services traitent les données personnelles en question, mais que personne ne se sente responsable. 3

II. PAS DE VIDE EN MATIÈRE DE RESPONSABILITÉ

4 L'art. 33 LPD habilite le Conseil fédéral à régler les responsabilités en matière de respect des prescriptions légales de protection des données ainsi que les contrôles qui y sont liés lorsque plusieurs organes fédéraux ou des organes fédéraux et des tiers cantonaux ou privés participent ensemble à des opérations de traitement de données. Cette réglementation ne figure pas dans l'OLPD, mais dans la législation spéciale correspondante ou dans les ordonnances d'exécution y afférentes. Ainsi, l'art. 33 LPD stipule explicitement que le Conseil fédéral règle les procédures de contrôle et la responsabilité en cas de traitement commun de données personnelles.

III. RESPONSABILITÉ PARTAGÉE

5 Trois cas de figure sont envisageables pour le traitement commun de données personnelles :

- Une loi spéciale ou le Conseil fédéral peut, dans une ordonnance, attribuer à un organe fédéral la responsabilité exclusive du traitement commun des données (art. 5 let. j LPD).
- Une loi spéciale ou une ordonnance permet d'établir un rapport de supériorité ou de subordination dans le cadre du traitement commun des données, qui se traduit par une responsabilité principale et une responsabilité secondaire. Le traitement des données de commande (art. 5 let. k LPD) en est un exemple.
- Il peut résulter d'une loi spéciale ou d'une ordonnance une responsabilité parallèle pour le traitement commun des données (art. 33 LPD), qui doit être différenciée par une répartition claire des tâches dans la loi spéciale ou l'ordonnance.

IV. PROCÉDURE DE CONTRÔLE

6 La notion de procédure de contrôle doit être comprise comme la surveillance des traitements de données. Dans la première constellation de la responsabilité unique, comme dans le cas d'une responsabilité principale et secondaire claire, il y a un contrôle unilatéral du responsable unique ou du responsable principal vis-à-vis de ceux qui participent au traitement commun des données. Dans la deuxième constellation de responsabilités parallèles

pour le traitement commun des données, il faut par nature mettre en place des procédures de contrôle réciproques. Les détails concernant l'étendue, la nature et la régularité des procédures de contrôle doivent être réglés dans la loi spéciale ou l'ordonnance.

V. RÉGIME RÉGLEMENTAIRE

Différents régimes de réglementation s'appliquent au traitement commun de données entre des organes fédéraux, des organes cantonaux et des personnes privées. Pour les organes fédéraux, les dispositions particulières relatives au traitement des données selon les articles 33 et suivants de la loi sur la protection des données s'appliquent. LPD, pour les personnes privées, ce sont les dispositions particulières des art. 30 ss. LPD s'appliquent et pour les organes cantonaux, c'est le droit cantonal qui s'applique. Même s'il s'agit d'un traitement commun de données, il faut toujours distinguer clairement quel acteur est lié à quelles obligations. 7

VI. QUESTIONS DE RESPONSABILITÉ

La responsabilité des organes fédéraux, des organes cantonaux et des personnes privées est régie par des normes différentes : Pour les organes fédéraux, selon la loi sur la responsabilité (LRCF), pour les organes cantonaux, selon les lois cantonales sur la responsabilité et pour les personnes privées, selon le droit civil. Il n'est pas clair dans quelle mesure un responsable peut être tenu responsable, dans les relations externes, de l'ensemble du dommage causé par le traitement commun des données (cf. responsabilité solidaire). La question de savoir dans quelle mesure les manquements aux obligations d'autrui peuvent être imputés à un responsable en raison de l'obligation de contrôle est également ouverte. 8

Dans le présent commentaire, l'auteur fait part de son appréciation personnelle.

BIBLIOGRAPHIE

Mund Claudia, Kommentierung zu Art. 33 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Rudin Beat, Kommentierung zu Art. 5 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Ballenberger Sara, Kommentierung zu Art. 16 DSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz / Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 34 LPD

Un commentaire de Esther Zysset

PROPOSITION DE CITATION

Esther Zysset, Kommentierung zu Art. 34 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Zysset, N. XXX zu Art. 34 DSG.

Art. 34 Bases légales

[1] Les organes fédéraux ne sont en droit de traiter des données personnelles que s'il existe une base légale.

[2] La base légale doit être prévue dans une loi au sens formel dans les cas suivants:

a. il s'agit d'un traitement de données sensibles;

b. il s'agit d'un profilage;

c. la finalité ou le mode du traitement de données personnelles est susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée.

[3] Pour les traitements de données personnelles visés à l'al. 2, let. a et b, une base légale prévue dans une loi au sens matériel suffit si les conditions suivantes sont réunies:

a. le traitement est indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel;

b. la finalité du traitement ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée.

[4] En dérogation aux al. 1 à 3, les organes fédéraux peuvent traiter des données personnelles si l'une des conditions suivantes est remplie:

a. le Conseil fédéral a autorisé le traitement, considérant que les droits des personnes concernées ne sont pas menacés;

b. la personne concernée a consenti au traitement en l'espèce ou a rendu ses données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement;

c. le traitement est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable.

TABLE DES MATIÈRES

En bref 460
I. généralités 460
A. Remarques préliminaires 460
B. But de la norme et contexte 461
C. Historique de la création 461
II. Le principe de légalité dans la protection des données 462
A. Rôle et fonctions du principe de légalité en général 462
1. Base légale en tant que condition préalable aux atteintes aux droits fondamentaux et principe d'action de l'État 462
2. Niveau et densité de la norme 463
B. Exigence de la règle de droit selon l'art. 34 LPD 465
1. principe de base al. 1 465
2. forme de la loi pour les cas visés à l'al. 2 467
3. Base légale de droit matériel pour les cas visés à l'al. 3 467
a. Indispensabilité pour une tâche décrite dans la loi (let. a) 468
b. Le but du traitement ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée (let. b) 468
4. al. 4 : Bassin de collecte pour les exceptions aux exigences des al. 1-3 469
a. Autorisation du Conseil fédéral (let. a) 469
b. Consentement (let. b) 470
c. Clause de police en matière de protection des données (let. c) 470
5. Casuistique relative à l'intensité de l'intervention et aux exigences posées à la norme 471
6. digression : le consentement "au cas par cas" (al. 4 let. b) 472
Bibliographie 474
Matériaux 475

EN BREF

En tant que pierre angulaire du traitement des données par les organes de l'Etat, l'exigence d'une règle de droit revêt une importance primordiale.

L'art. 34 LPD illustre, pour le traitement de données par des organes fédéraux, aussi bien l'art. 5 Cst. selon lequel toute action de l'Etat requiert une base légale que l'art. 36 Cst. qui fixe les conditions pour les atteintes aux droits fondamentaux en général ; cette disposition constitue donc du droit constitutionnel concrétisé. Le traitement de données personnelles par des organes publics constitue une atteinte au droit fondamental à la protection de l'autodétermination en matière d'information selon l'art. 13 al. 2 Cst. ; selon le contexte, d'autres droits fondamentaux les plus divers peuvent en outre être concernés. L'art. 34 LPD s'exprime schématiquement sur le niveau de norme requis.

La nouvelle disposition relative à la base légale, qui n'est pas aussi détaillée que la version précédente de la même norme, reflète l'importance accrue que revêt le fondement juridique correct des traitements de données effectués par des organes étatiques à l'ère du traitement numérique de grandes quantités de données.

I. GÉNÉRALITÉS

A. Remarques préliminaires

1 Une base légale est une norme générale et abstraite édictée par un organe étatique compétent. Dans le détail, le droit applicable détermine les exigences auxquelles une base légale doit répondre. Au niveau fédéral, on trouve des prescriptions à ce sujet dans la Constitution fédérale (art. 164 Cst.) ou dans la loi sur le Parlement (p. ex. art. 22 LParl). La norme qui sert de base légale dans un cas particulier peut provenir du droit national ou international.

2 La terminologie relative au principe de légalité présente une certaine hétérogénéité. Dans ce qui suit, le terme général de règle de droit est également utilisé pour désigner l'exigence d'une réglementation générale et abstraite, appelée "base légale" à l'article 34 LPD. En outre, le droit édicté par le pouvoir législatif est décrit par la notion de "forme de la loi" ou de "loi au

sens formel". Les actes législatifs de niveau inférieur sont considérés comme des "lois au sens matériel", comme l'indique également l'art. 34 al. 3 LPD.

B. But de la norme et contexte

L'art. 34 LPD concrétise pour le droit de la protection des données ce qui vaut de toute façon pour l'action de l'Etat : outre le principe général de légalité de l'art. 5 al. 1 Cst. selon lequel le droit constitue le fondement et la limite de l'action de l'Etat, l'art. 36 al. 1 Cst. exige une base légale pour les atteintes aux droits fondamentaux. L'art. 34 LPD donne des indications schématiques sur le niveau de la norme pour différents types de traitement de données - et donc pour différentes atteintes aux droits fondamentaux, à commencer par les atteintes au droit fondamental à l'autodétermination en matière d'information (art. 13 al. 2 Cst.). 3

C. Historique de la création

Le projet du Conseil fédéral pour la première loi fédérale sur la protection des données, datant de 1988, contenait déjà une disposition qui ressemblait dans les grandes lignes à celle commentée ici ; on y faisait notamment déjà la distinction entre le traitement de données personnelles ordinaires et celui de données nécessitant une protection plus élevée, sous la forme de données personnelles sensibles et de profils de la personnalité. La disposition précédente, l'art. 17 aDSG, modifiée dans le cadre d'une révision intermédiaire, prévoyait le principe de base de la base légale et établissait en outre des exceptions dont la portée était peu claire et donnait lieu à des critiques. 4

La nouvelle norme procède à un désenchevêtrement structurel ; elle distingue clairement, outre le principe de base inchangé (al. 1), l'exigence de la forme de la loi (al. 2), les situations où le niveau de la norme est abaissé (al. 3) et les situations dans lesquelles il est possible de déroger entièrement à l'exigence d'une règle de droit (al. 4). 5

II. LE PRINCIPE DE LÉGALITÉ DANS LA PROTECTION DES DONNÉES

A. Rôle et fonctions du principe de légalité en général

1. Base légale en tant que condition préalable aux atteintes aux droits fondamentaux et principe d'action de l'État

6 Lors du traitement de données personnelles par les autorités étatiques, il y a des atteintes aux positions protégées par les droits fondamentaux : Il s'agit en premier lieu de l'art. 13 Cst. et notamment de son al. 2 (droit fondamental à l'"autodétermination en matière d'information") ainsi que de l'art. 8 CEDH et de l'art. 17 du Pacte II de l'ONU. Contrairement à la formulation de l'art. 13 al. 2 Cst., ce n'est pas seulement la protection contre l'emploi abusif de données personnelles qui est protégée, mais la sphère privée, dans la mesure où elle contient également des données sur la personne concernée. En outre, d'autres droits fondamentaux peuvent être touchés, notamment le droit à la liberté personnelle (art. 10 al. 2 Cst.) ou la liberté d'expression (art. 16 Cst.), a fortiori avec la numérisation croissante, où toute activité de l'Etat implique le traitement de données.

7 A l'article 36, al. 1, la Constitution fédérale prévoit que les restrictions des droits fondamentaux nécessitent une base légale ; les restrictions graves doivent être prévues sous forme de loi, sauf en cas de "danger grave, imminent et impossible à détourner autrement". En outre, les restrictions des droits fondamentaux doivent servir à la réalisation d'un intérêt public et être proportionnées ; l'essence du droit fondamental doit être préservée (cf. critères de l'art. 36 Cst.).

8 Dans son rôle de principe de l'action étatique, l'art. 5 al. 1 Cst. prévoit que l'action étatique a besoin d'un fondement dans le droit et que c'est en même temps le droit qui fixe des limites à toute action étatique ("Schranken", selon les termes du constituant). L'administration - l'"organe fédéral" selon la terminologie de la LPD - ne peut donc agir que s'il existe une base légale à cet effet et ne peut agir que dans la mesure où cette action est couverte par la base correspondante. Cela vaut indépendamment de la nature juridique de l'action de l'État, même si les exigences du principe de légalité prennent différentes formes selon la situation et les risques.

2. Niveau et densité de la norme

L'art. 36 al. 1 Cst. laisse déjà entendre que la règle de droit requise doit satisfaire à des exigences accrues en cas de restrictions graves des droits fondamentaux. Plus l'atteinte aux droits fondamentaux est grave, plus les exigences relatives au niveau et à la densité de la norme sont élevées. Les restrictions graves doivent être prévues dans la loi elle-même, c'est-à-dire dans une loi au sens formel (niveau de la norme) et tenir suffisamment compte du principe de précision (densité de la norme). Au minimum, les normes juridiques doivent être formulées "de manière suffisamment précise pour permettre aux personnes soumises au droit d'orienter leur comportement et de connaître les conséquences d'un comportement déterminé avec un degré de certitude correspondant aux circonstances". Il n'est souvent pas facile de répondre à la question de savoir dans quel cas telle ou telle qualité de la norme juridique est suffisante et cela dépend fortement du cas particulier. Pour reprendre les termes de Tschannen/Müller/Kern, le principe de légalité est "d'une absence de rivage désagréable". Pour le droit fédéral, l'art. 164 Cst. donne tout de même une liste exemplaire de thèmes pour lesquels les dispositions fondamentales sont considérées comme des dispositions importantes fixant des règles de droit et doivent donc être réglées dans une loi au sens formel ; il s'agit de : 9

- Exercice des droits politiques ;
- Limitations des droits constitutionnels;
- Droits et obligations des personnes;
- Le cercle des assujettis ainsi que l'objet et le calcul des taxes;
- les tâches et les prestations de la Confédération;
- Obligations des cantons dans la mise en œuvre et l'exécution du droit fédéral;
- Organisation et procédures des autorités fédérales.

10 La doctrine propose pour sa part les critères suivants pour définir l'importance d'un objet de réglementation :

- Intensité de l'intervention;
- Nombre de personnes concernées par une réglementation ou de faits de vie réglementés;
- importance financière;
- importance pour la formation de la volonté politique, l'organisation des institutions étatiques ou la procédure; et
- le caractère explosif ou acceptable de la thématique.

11 En revanche, le besoin de flexibilité et d'adaptation rapide ou des connaissances techniques particulières plaident plutôt en faveur de réglementations à un niveau normatif inférieur.

12 Ces directives générales de la Constitution fédérale doivent être prises en compte lors de l'élaboration de bases légales conformément à l'article 34 LPD. L'art. 34 LPD indique le niveau de norme requis pour certaines situations typiques de la protection des données, mais pas la densité normative (voir infra, n. 18-19, à propos de la densité normative). Dans le contexte de la protection des données qui nous intéresse ici, la limitation des droits constitutionnels ou l'intensité des atteintes aux droits fondamentaux ainsi que les dispositions relatives aux "droits et obligations des personnes" figurent entre autres au premier plan des catalogues cités ci-dessus. Avec la numérisation croissante, le caractère explosif des thèmes joue également un rôle accru en tant que critère pour la forme de la loi, comme le montre actuellement l'utilisation de l'intelligence artificielle ou, plus concrètement, la reconnaissance faciale dans l'espace public.

13 Si des compétences législatives doivent être déléguées par le législatif à l'exécutif, les conditions générales de la délégation législative développées par la jurisprudence et la doctrine s'appliquent également à la protection des données. Ainsi, la délégation législative ne doit pas être exclue par le droit correspondant (cf. à ce sujet l'art. 164 al. 1 Cst.) ; la norme de délégation doit être contenue dans un acte législatif au niveau de la loi ; la délégation doit se limiter à une matière déterminée et les grandes lignes de cette matière doivent déjà être mentionnées dans la loi.

B. Exigence de la règle de droit selon l'art. 34 LPD

1. principe de base al. 1

L'exigence fondamentale d'une règle de droit soumet le traitement de données par des organes fédéraux à une interdiction avec réserve d'autorisation, contrairement au traitement de données par des personnes privées. Cette exigence s'applique quel que soit le type de traitement de données (voir à ce sujet la définition légale du traitement à l'art. 5 let. d LPD ; pour le cas particulier de la communication, voir l'art. 36 LPD). L'art. 34 LPD ne fait qu'énoncer le principe de base ; il ne peut pas lui-même être invoqué comme base légale directe. En outre, l'al. 1 ne précise pas à quel niveau de norme la règle de droit doit se situer ou quelle densité normative elle doit présenter. 14

Il ressort par ailleurs de la systématique de la LPD que les autres prescriptions générales de la loi, notamment les principes de traitement des données de l'article 6 LPD ainsi que les prescriptions relatives à la sécurité selon l'article 8 LPD, s'appliquent de manière cumulative. Ainsi, l'existence d'une base légale ne dispense pas, par exemple, de l'obligation de respecter le principe de proportionnalité et de ne traiter que les données effectivement nécessaires à l'accomplissement de la tâche publique. 15

Le texte de loi de l'article 34 LPD se réfère au traitement de données personnelles par des organes fédéraux. En ce qui concerne la définition de l'organe fédéral, l'art. 5 let. i LPD exprime qu'elle couvre non seulement les unités de l'administration et des établissements publics de la Confédération qui lui sont rattachés sur le plan organisationnel, mais aussi les personnes privées, dans la mesure où elles sont chargées de l'exécution de tâches publiques de la Confédération (voir à ce sujet). 16

Nonobstant les indications relatives au niveau de la norme aux al. 2-4, la pratique législative n'est souvent pas tout à fait claire quant à la densité normative de la base légale. Ce problème se manifeste par exemple lorsqu'il s'agit de savoir si une base légale générale ("indirecte") suffit ("L'office X exécute la tâche légale Y") ou s'il faut une base légale spécifique et adaptée à un traitement de données particulier ("Pour traiter les demandes de subventions, l'office X traite les données personnelles suivantes : ...", etc.). 17

18 En ce qui concerne la nature de la base légale, l'Office fédéral de la justice a rédigé un guide législatif qui contient des prescriptions spécifiques pour les bases légales dans le domaine de la protection des données. Compte tenu des fonctions du principe de légalité (voir à ce sujet infra N. 43 ss.) et du postulat selon lequel le citoyen doit pouvoir orienter son comportement en fonction de la norme correspondante, les éléments suivants doivent être réglementés :

- Quelle autorité (qui)
- traite quelles catégories de données personnelles (quoi),
- dans quel but (pourquoi) et
- de quelle manière (comment) ?
- A qui les données personnelles sont éventuellement communiquées (à qui) et (comment) ?
- de quelle manière (comment) ?

19 Il convient notamment d'indiquer sous "quoi" si des données sensibles sont également traitées et, dans l'affirmative, quelles catégories (cf. art. 5 let. c LPD), alors que les attributs précis peuvent être précisés dans une ordonnance si la densité normative est suffisante au niveau de la loi. Plus l'atteinte aux droits fondamentaux est importante, plus la base légale doit être formulée de manière détaillée et précise, même si, compte tenu de l'évolution rapide des technologies de l'information et de la communication, il faut parfois s'accommoder d'une certaine flexibilité dans la formulation et du caractère vague qui en découle. Les indications relatives à la durée de conservation et à l'effacement des données personnelles font également partie du traitement.

20 Dans la mesure où la règle de droit établit ainsi la transparence exigée par la loi à l'égard des personnes concernées, le devoir d'information selon l'art. 19 LPD est supprimé (cf. art. 20 al. 1 let. b LPD).

21 Les lois sectorielles respectives peuvent prévoir des règles spéciales qui priment les prescriptions de la LPD en tant que lex specialis et peuvent, du moins en théorie, s'en écarter vers le bas. Le Tribunal fédéral et la doctrine partent du principe que les principes généraux de la protection des données doivent être respectés dans de tels cas.

2. forme de la loi pour les cas visés à l'al. 2

Le deuxième alinéa exige la forme de la loi (loi au sens formel) pour les cas où le traitement des données peut conduire à une atteinte importante aux droits fondamentaux des personnes concernées. Là où le traitement de données personnelles sensibles (let. a) et le profilage (let. b) sont des concepts et des notions définis dans la LPD, l'al. 2 prévoit en outre une clause générale qui s'applique lorsque soit la finalité du traitement, soit la manière dont les données sont traitées peuvent conduire à une atteinte grave aux droits fondamentaux des personnes concernées (let. c). L'exigence de la forme légale pour les traitements de données ayant une grande incidence sur les droits fondamentaux découle toutefois déjà de l'art. 36 al. 1 Cst. indépendamment de la lettre de l'al. 2 à laquelle un état de fait est attribué. 22

Les deux paramètres mentionnés à la let. c, à savoir le but et le mode de traitement, sont les principaux éléments pris en compte pour évaluer l'atteinte au droit fondamental concerné. Compte tenu du contexte des droits fondamentaux, ils ne sont pas exhaustifs. 23

S'il n'est pas possible de fonder le traitement des données sur une base juridique suffisamment précise et détaillée, la jurisprudence confirme qu'une application particulièrement stricte, par exemple du contrôle de la proportionnalité, peut avoir un certain effet compensatoire. 24

3. Base légale de droit matériel pour les cas visés à l'al. 3

L'al. 3 prévoit la possibilité d'un niveau normatif inférieur pour le traitement de données personnelles sensibles et le profilage, pour autant que deux conditions soient remplies de manière cumulative : Le traitement est indispensable à l'accomplissement d'une tâche formellement définie par la loi ; et la finalité du traitement ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée. 25

En raison du cadre constitutionnel, il est à nouveau concevable - même si les exemples devraient être rares - que des dérogations s'imposent, qui ne sont pas concrètement énumérées par l'al. 3 : Par exemple, le caractère socialement explosif d'une thématique pourrait conduire à ce que la forme légale soit exigée pour les traitements de données correspondants ; c'est donc la manière dont les données sont traitées, au lieu de la finalité mentionnée à l'al. 3, qui justifie l'augmentation du niveau de la norme. 26

a. Indispensabilité pour une tâche décrite dans la loi (let. a)

27 En ce qui concerne la formulation de l'al. 3 let. a, il est frappant de constater, par rapport à la version précédente (art. 17 al. 2 let. aDSG), qu'il n'est désormais plus possible de se baser uniquement "à titre exceptionnel" sur le niveau de norme réduit. Dans la version précédente, on pouvait défendre la position selon laquelle il ne s'agissait que de traitements exceptionnels et ponctuels de données dans des situations où un tel traitement n'est normalement pas nécessaire pour l'accomplissement de la tâche légale correspondante. La formulation actuelle s'en écarte nettement en renonçant à la condition de l'existence d'une situation exceptionnelle. Il faut donc partir du principe que le traitement durable de données personnelles sensibles et de profils de la personnalité est également possible sur la base d'une ordonnance si les deux conditions de l'al. 3 sont remplies.

b. Le but du traitement ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée (let. b)

28 L'al. 3 let. b entre en ligne de compte pour les traitements qui relèvent d'une catégorie intermédiaire : Il s'agit certes de types de traitement qui conduiraient typiquement à une atteinte grave aux droits fondamentaux (raison pour laquelle l'al. 2 exige normalement pour eux une base légale formelle), mais dans le cas concret, le but du traitement ne comporte pas de risques particuliers pour les droits fondamentaux des personnes concernées. Selon le message du Conseil fédéral, il s'agit en particulier de données sensibles traitées dans le cadre des affaires du Conseil fédéral, des départements et des offices ; sont mentionnés les décisions sur recours, les cas de responsabilité de l'Etat ou les affaires concernant le personnel fédéral. En outre, la base légale formelle doit concrétiser suffisamment la nature des tâches pour lesquelles le traitement de données personnelles est nécessaire.

29 La formulation de l'al. 3 let. b peut paraître surprenante, car il n'est fait référence qu'au "but du traitement", sans inclure le "mode de traitement des données" mentionné jusqu'ici à l'al. 2 let. c. On peut supposer que le législateur a ainsi voulu rappeler en premier lieu que les traitements de données qui paraissent déjà délicats du point de vue des droits fondamentaux en raison de leur finalité nécessitent dans tous les cas une base sous forme de loi, même si la manière dont le traitement est effectué dans un cas particulier présente peu de risques propres.

4. al. 4 : Bassin de collecte pour les exceptions aux exigences des al. 1-3

al. 4 exclut trois situations idéales (rédigées sous forme d'alternatives) de l'exigence d'une règle de droit : 30

- L'autorisation du traitement par l'exécutif (en l'occurrence le Conseil fédéral), l'autorisation devant ici aussi se fonder sur l'exigence que les droits des personnes concernées ne soient vraisemblablement pas menacés (let. a);
- Le consentement de la personne concernée dans un cas particulier ou la libération sans condition de données personnelles par cette même personne (let. b) ou
- L'intérêt supérieur urgent sous la forme de la protection de la vie ou de l'intégrité physique de la personne concernée ou d'un tiers dans une situation qui ne permet pas de recueillir le consentement (let. c).

Là où l'al. 3 ne fait que réduire les exigences en matière de base légale, l'al. 4 prévoit, dans certains cas, qu'aucune règle de droit, qu'il s'agisse d'une loi ou d'une règle de droit de nature matérielle, n'est nécessaire. Dans la mesure où il est désormais explicitement renoncé à toute exigence d'une règle de droit, cette disposition constitue, d'un point de vue formel, la plus grande nouveauté par rapport aux versions précédentes de la même disposition dans la LPD. Pour les situations mentionnées aux lettres a et b, qui figuraient déjà dans la version précédente, une clarification bienvenue est apportée ; le libellé de la norme précédente ne permettait pas de déterminer avec certitude si l'intention était de renoncer totalement à une base juridique ou non. 31

a. Autorisation du Conseil fédéral (let. a)

Selon la let. a, le Conseil fédéral autorise un traitement parce qu'il "estime que les droits de la personne concernée ne sont pas menacés". Alors que la version précédente mentionnait encore explicitement que cette autorisation était limitée au cas individuel, cet ajout a disparu de la formulation actuelle. Selon le message, la norme ne devrait toutefois pas être modifiée malgré la différence de formulation ; cela ressort également du contexte si l'on y regarde de plus près. L'autorisation en tant que forme de décision doit être considérée par rapport à la réglementation générale et abstraite. Cette dernière prend la forme d'une ordonnance du Conseil fédéral (art. 182 al. 1 32

Cst.), c'est-à-dire d'une base juridique de droit matériel qui peut être soit d'exécution, soit de substitution (et qui, dans le second cas, nécessite une habilitation par une loi). Le cas d'action sans règle de droit visé par l'al. 4 let. a est donc obligatoirement conçu pour le cas particulier.

33 La formulation selon laquelle les "droits de la personne concernée ne doivent pas être menacés" semble tout aussi obscure que dans la version précédente. Cette formulation s'écarte du choix des termes de l'al. 3 let. b, où il est question que le but du traitement "ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée". Néanmoins, étant donné que tout traitement de données par des organes publics constitue une atteinte aux droits fondamentaux, il faut partir du principe que la formule utilisée à l'al. 4 signifie la même chose qu'à l'al. 3 let. b, à savoir qu'il faut partir du principe que l'atteinte aux droits fondamentaux est faible.

b. Consentement (let. b)

34 A la let. b, le consentement se substitue à la base légale. En cas de libération des données sans condition préalable, le consentement est présumé ; dans ce cas, une publication consciente et volontaire par la personne concernée est supposée. Voir à propos du consentement en général l'art. 6 al. 6 et 7 LPD ainsi que la question du consentement en tant que substitut valable d'une base légale ci-après infra N. 42 ss.

c. Clause de police en matière de protection des données (let. c)

35 let. c vise la protection d'intérêts urgents et supérieurs, concrétisée sous la forme de la protection de la vie ou de l'intégrité physique de la personne concernée ou d'un tiers. La condition est qu'il ne soit pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable, ce qui est par exemple le cas lorsque celle-ci n'est pas en état de réagir (coma ou autre) ou qu'elle est introuvable. Cette norme constitue un cas spécifique d'"intérêt policier" du point de vue de la protection des données. En ce sens, elle s'inscrit sans autre dans le schéma de l'art. 36 al. 1 Cst. qui exclut de l'exigence d'une base légale les "cas de danger grave, imminent et impossible à écarter autrement". L'exigence selon laquelle il doit s'agir d'un cas particulier n'est pas explicitement écrite, mais elle est inhérente à la clause de police, ce qui signifie par exemple que le traitement de données par la police ou les services

de renseignement dans le cadre de situations de danger récurrentes ne peut pas se fonder uniquement sur l'al. 4 let. c.

5. Casuistique relative à l'intensité de l'intervention et aux exigences posées à la norme

Conformément à l'art. 17 al. 2 aDSG, le traitement de données d'entraide administrative se rapportant à des relations d'affaires ou à des relations bancaires ne nécessite pas de base sous forme de loi. L'atteinte aux droits constitutionnels en rapport avec les données à collecter dans le cadre de l'entraide administrative n'est en règle générale pas particulièrement grave, de sorte que les exigences en matière de précision de la norme ne sont pas non plus "excessivement élevées" (ATF 148 II 349 consid. 5.3.3-5.3.4). 36

La base légale qui prévoit l'utilisation de compteurs d'eau à radiofréquence par les services communaux de distribution d'eau doit prévoir explicitement que les valeurs horaires relevées sont enregistrées sur le compteur d'eau pendant X jours et envoyées par radio à intervalles réguliers (ATF 147 I 346 consid. 5.4.1). 37

Si, lors de la recherche automatisée d'un véhicule, on obtient, en plus de la plaque de contrôle et donc de l'identité du détenteur, l'heure, l'emplacement, la direction et l'identité des autres occupants du véhicule, ce traitement de données se situe dans le cadre d'une "constatation d'identité conventionnelle", ce qui ne constitue pas encore une atteinte grave aux droits fondamentaux. Mais cela change considérablement avec le regroupement et la comparaison automatique de ces données avec d'autres jeux de données (il est question d'un "traitement en série et simultané de jeux de données importants et complexes en une fraction de seconde") et l'utilisation subséquente par les autorités ; l'intensité de l'atteinte augmente "considérablement", notamment en raison du risque que des personnes soient soupçonnées à tort (ATF 146 I 11 consid. 3.2). 38

L'inscription sur une liste de surveillance gérée par la FINMA, qui sert d'étape préalable à d'éventuelles restrictions de l'activité professionnelle dans le domaine du marché financier et qui aboutit en somme à un véritable profil de la personnalité, constitue une atteinte grave à l'art. 13 al. 2 Cst. et suppose une base sous forme de loi (ATF 143 I 253 consid. 4). 39

40 Si une loi sur la police place la surveillance technique de lieux accessibles à tous sous le slogan de la "sauvegarde de l'ordre et de la sécurité publics", cette indication de but est insuffisante et ne permet notamment pas d'examiner la base légale sous l'angle de la proportionnalité (en particulier le rapport entre le but et les moyens). (ATF 136 I 87 E. 8.3-8.4).

41 Le caractère suffisamment précis d'une norme peut également résulter de l'enchevêtrement des normes applicables : Si l'on objecte que l'art. 91 al. 5 LP dispose d'une densité normative insuffisante pour la communication de données qui contiennent des données personnelles sensibles et/ou des profils de la personnalité, il convient d'objecter que cette disposition ne s'applique que dans le cadre de l'exécution de la saisie. Le but et l'étendue du traitement des données sont ainsi définis de manière suffisamment précise. (ATF 124 III 170 consid. 3a)).

6. digression : le consentement "au cas par cas" (al. 4 let. b)

42 Dans le droit public de la protection des données, il est souvent difficile de savoir dans quelle mesure un consentement peut remplacer la base légale. La question du consentement se pose de manière particulièrement aiguë lorsqu'il s'agit d'atteintes graves à des positions de droits fondamentaux ; la renonciation à des droits fondamentaux ou le consentement à des atteintes particulièrement graves à des droits fondamentaux sont alors au premier plan. A l'autre extrémité de l'éventail des atteintes, il peut toutefois y avoir tout autant de points d'interrogation, par exemple lorsqu'il s'agit de l'envoi d'une newsletter par une autorité publique ou de la demande d'une référence dans une procédure de recrutement. L'art. 34 LPD prévoit à l'al. 4 let. b le consentement comme substitut de la règle de droit, il en va de même pour l'art. 36 al. 2 let. b LPD en ce qui concerne la communication de données personnelles. Dans les deux cas, le consentement est lié au cas particulier, mais n'est pas soumis à la condition qu'il s'agisse d'une situation de danger faible ou inexistant. Contrairement au consentement dans le droit privé de la protection des données (voir à ce sujet l'art. 6, al. 6 et 7 LPD), il ne suffit pas, en droit public, que le consentement soit libre et éclairé. En outre, le consentement doit être approprié dans le cas concret pour assumer les fonctions en jeu du principe de légalité. Au-delà de ces exigences de fond, le consentement en droit public n'est lié à aucune forme.

Le Tribunal fédéral et la doctrine s'accordent à dire que le principe de légalité remplit deux types de fonctions. D'une part, il poursuit des objectifs démocratiques, dont la garantie de la prédominance de la volonté populaire d'une part et la séparation des pouvoirs d'autre part. D'autre part, il remplit des fonctions d'État de droit ; dans ce contexte, il assure la protection de l'individu contre l'arbitraire de l'État, l'égalité de traitement ainsi que la prévisibilité de l'action de l'État. 43

Dans certaines conditions, le consentement peut tout à fait remplacer les fonctions de l'Etat de droit que sont la protection contre l'arbitraire et la prévisibilité de l'action étatique. Pour cela, il faut que la portée du consentement soit reconnaissable au moment où il est donné et qu'il s'agisse d'un contexte dans lequel le caractère volontaire du consentement peut être présumé de bonne foi. 44

Une première restriction découle toutefois de la fonction d'égalité de traitement de l'État de droit : dès qu'il s'agit de l'octroi de droits ou de l'imposition d'obligations, le consentement ne peut être opérationnalisé en tant que substitut d'une règle de droit que si seules des personnes individuelles sont concernées. Lorsque les préoccupations démocratiques sont au premier plan, le consentement n'est plus en mesure d'apporter une compensation fonctionnelle. 45

En conséquence, il convient d'examiner, selon les circonstances, si la renonciation à une base légale et le recours au consentement peuvent être justifiés en se référant au principe de légalité et aux critères de l'exigence de la forme légale (voir à ce sujet N. 9-10 supra). 46

Pour les traitements de données effectués par des organes fédéraux, l'art. 34 al. 4 let. b LPD délimite l'admissibilité en limitant le consentement au cas particulier. Au vu de ce qui précède, il faut partir du principe qu'il doit s'agir d'un nombre très limité de situations, tant du point de vue matériel que temporel, et également du point de vue personnel pour l'introduction de droits et d'obligations. 47

Malgré le caractère schématique de la LPD en ce qui concerne les atteintes aux droits fondamentaux, il n'est donc possible de répondre de manière fiable à cette question que dans le concret, en tenant compte des préoccupations en question. Ainsi, la newsletter susmentionnée d'une autorité pourra être envoyée sur la base d'un consentement même si le nombre de destinataires 48

est très élevé et même si la périodicité est illimitée dans le temps, alors que l'utilisation de systèmes de reconnaissance faciale, même dans un domaine étroitement délimité en termes de lieu, de temps et de personnel, ne devrait pas être autorisée sur la base d'un consentement dans un cas particulier en raison de l'intensité de l'atteinte aux droits fondamentaux des personnes concernées et du caractère socialement explosif de la technologie utilisée.

BIBLIOGRAPHIE

Ballenegger Sarah, Kommentierung zu Art. 17 DSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014.

Dubey Jacques, Kommentierung zu Art. 5 BV, in: Martenet Vincent/Dubey Jacques (Hrsg.), Commentaire romand Constitution fédérale, Basel 2021.

Epiney Astrid/Posse Samah, Kommentierung zu Art. 34 DSG, in: Meier Philippe/Métille Sylvain (Hrsg.), Commentaire romand, Loi sur la protection des données, Basel 2023 (Publikation zum Zeitpunkt der Abgabe der vorliegenden Kommentierung bevorstehend).

Epiney Astrid, Staatliche Überwachung versus Rechtsstaat: Wege aus dem Dilemma?, AJP 2016, S. 1503-1515.

Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl. Zürich/St. Gallen 2020.

Häner Isabelle, Die Einwilligung der betroffenen Person als Surrogat der gesetzlichen Grundlage bei individuell-konkreten Staatshandlungen, ZBl 103 (2002), S. 57-76.

Mund Claudia, Kommentierung zu Art. 34 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Tschannen Pierre, Staatsrecht der Schweizerischen Eidgenossenschaft, 5. Aufl. Bern 2021.

Tschannen Pierre/Müller Markus/Kern Markus, Allgemeines Verwaltungsrecht, 5. Aufl. Bern 2022.

Waldmann Bernhard/Bickel Jürg, Datenbearbeitung durch Bundesorgane, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard (Hrsg.), Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, S. 639-764.

Waldmann Bernhard/Oeschger Magnus, Datenbearbeitung durch kantonale Organe, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard (Hrsg.), Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, S. 765-894.

Wyss Martin Philipp, Öffentliche Interessen – Interessen der Öffentlichkeit?, Bern 2001.

MATÉRIAUX

Bundesamt für Justiz, Gesetzgebungsleitfaden, Leitfaden für die Ausarbeitung von Erlassen des Bundes, 4. Aufl. 2019, abrufbar unter https://www.bj.admin.ch/bj/de/home/staat/legistik/hauptinstrumente.html, besucht am 21.2.2023 (zit. Gesetzgebungsleitfaden).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 S. 6941 ff., abrufbar https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 31.3.2023 (zit. Botschaft 2017).

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988 II S. 413 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/de, besucht am 31.3.2023 (zit. Botschaft 1988).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 35 LPD

Un commentaire de Sandra Husi-Stämpfli

PROPOSITION DE CITATION

Sandra Husi-Stämpfli, Kommentierung zu Art. 35 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Husi-Stämpfli, N XXX zu Art. 35 DSG.

Art. 35 Traitement de données personnelles automatisé dans le cadre d'essais pilotes

[1] Le Conseil fédéral peut autoriser, avant l'entrée en vigueur d'une loi au sens formel, le traitement automatisé de données sensibles ou d'autres traitements au sens de l'art. 34, al. 2, let. b et c, si les conditions suivantes sont réunies:

a. les tâches qui nécessitent ce traitement sont réglées dans une loi au sens formel déjà en vigueur;

b. des mesures appropriées sont prises aux fins de réduire au minimum les atteintes aux droits fondamentaux de la personne concernée;

c. la mise en œuvre du traitement rend indispensable une phase d'essai avant l'entrée en vigueur de la loi au sens formel, en particulier pour des raisons techniques.

[2] Il consulte au préalable le PFPDT.

[3] L'organe fédéral responsable transmet, au plus tard deux ans après la mise en œuvre de l'essai pilote, un rapport d'évaluation au Conseil fédéral. Dans ce rapport, il lui propose la poursuite ou l'interruption du traitement.

[4] Le traitement automatisé de données personnelles doit être interrompu dans tous les cas si aucune loi au sens formel prévoyant la base légale nécessaire n'est entrée en vigueur dans un délai de cinq ans à compter de la mise en œuvre de l'essai pilote.

TABLE DES MATIÈRES

En bref 480
I. Généralités 480
A. Contexte 480
B. Objectif de la norme 480
C. Historique 481
II. conditions pour un essai pilote admissible (al. 1) 481
A. Norme de tâche dans une loi au sens formel (let. a) 481
B. Limitation des atteintes à la personnalité à un minimum (let. b) 482
C. Caractère indispensable de la phase de test (let. c) 482
III. réglementation du projet pilote dans un règlement 483
IV. Obligation de demander l'avis du PFPDT (al. 2) 483
V. Évaluation et limitation dans le temps de la phase pilote (al. 3 et 4) 484
VI. Appréciation 484
Bibliographie 485

EN BREF

La disposition relative à la réalisation d'essais pilotes permet de traiter des données personnelles sensibles, même s'il n'existe pas encore de bases légales formelles. L'objectif de cette disposition est de permettre des traitements de données expérimentaux limités dans le temps, lorsque ceux-ci sont indispensables pour aborder certaines innovations techniques, des questions d'organisation ou d'autres points obscurs.

I. GÉNÉRALITÉS

A. Contexte

1 Le besoin d'applications performantes, non seulement dans les domaines dits "électroniques", c'est-à-dire la cyberadministration ou la cybersanté, mais aussi, de manière plus générale, dans le cadre de l'accomplissement des tâches des autorités, croît avec la numérisation de nos domaines de vie et d'activité.

2 Étant donné que les projets de numérisation impliquent généralement des coûts d'investissement élevés, mais qu'il est souvent impossible d'estimer si les applications en question peuvent être mises en œuvre techniquement comme on l'espère, il faut prévoir la possibilité d'évaluer la conception et notamment la mise en réseau des applications dans le cadre d'essais pilotes. Les essais pilotes doivent être considérés comme des tests permettant d'acquérir des connaissances sur la faisabilité ou l'acceptation d'un projet.

B. Objectif de la norme

3 Les essais pilotes ne doivent pas avoir pour effet de vider de leur substance les principes de l'État de droit. Même si, en raison de la nature expérimentale du traitement des données et de la complexité du processus législatif, il n'est pas encore possible, au moment du projet pilote, de recourir aux bases juridiques prévues par la Constitution (avec un niveau et une densité normatifs appropriés), il convient néanmoins de respecter des prescriptions juridiques minimales.

L'art. 35 LPD permet donc au Conseil fédéral de faire réaliser des essais pilotes limités dans le temps, sur la base d'une simple ordonnance (et non d'une loi au sens formel, comme cela serait nécessaire pour les données personnelles sensibles, art. 34 al. 2 LPD). 4

C. Historique

La motion "Protection accrue des données personnelles dans le cadre des connexions en ligne" a été déposée en 1999 déjà. Elle a constitué la première pierre de ce qui allait devenir l'art. 17a aDSG et la réglementation des traitements de données dans le cadre d'essais pilotes, lors desquels les droits de la personnalité des personnes concernées pourraient être particulièrement menacés. Le contenu de l'art. 35 LPD a été repris dans la nouvelle loi sur la protection des données dans une large mesure sans modification et sans être contesté lors des débats parlementaires. 5

II. CONDITIONS POUR UN ESSAI PILOTE ADMISSIBLE (AL. 1)

Les données personnelles sensibles ou autres traitements de données au sens de l'art. 34 al. 2 let. b et c LPD ne peuvent être traités dans le cadre d'un projet pilote et par exception à l'exigence d'une base légale que si les conditions suivantes sont remplies de manière cumulative : 6

A. Norme de tâche dans une loi au sens formel (let. a)

Les tâches pour l'accomplissement desquelles le projet pilote avec le traitement automatisé des données personnelles sensibles doit être nécessaire doivent déjà être réglées dans une loi au sens formel au moment du projet pilote (voir à ce sujet OK-Zysset ad art. 34 LPD), la loi doit en outre déjà être en vigueur. 7

Il ne suffit pas que la base légale formelle règle uniquement les tâches nécessitant un traitement. L'exigence de densité normative doit être remplie, sinon pour le projet pilote lui-même, du moins pour les tâches qui sont à la base du projet. La base légale doit ainsi décrire l'organe qui a accès aux données, le but concret de l'accès ainsi que l'étendue de l'autorisation d'accès. 8

B. Limitation des atteintes à la personnalité à un minimum (let. b)

9 Afin de minimiser les risques que le projet pilote fait courir aux personnes concernées, des mesures organisationnelles, techniques et juridiques doivent être prises, notamment pour assurer la sécurité des données. Les mesures de protection doivent réduire au minimum les éventuelles menaces d'atteinte à la personnalité. La nouvelle formulation de l'art. 35 al. 1 let. b LPD tient ainsi compte du fait que le risque d'atteinte à la personnalité dans le cadre de traitements de données numérisées ne peut de facto jamais être totalement exclu.

C. Caractère indispensable de la phase de test (let. c)

10 Les projets pilotes de traitement de données personnelles sensibles et la relativisation du principe de légalité qui en découle ne doivent pas être lancés à la légère : L'art. 35 al. 1 let. c LPD présuppose que la phase de test est indispensable, notamment pour des raisons techniques. En même temps, le législateur admet qu'il peut y avoir d'autres raisons, par exemple organisationnelles, qui rendent nécessaire un essai pilote pour le traitement de données personnelles sensibles ("en particulier").

11 On peut également imaginer des combinaisons de conditions-cadres techniques et organisationnelles qui, à elles seules, ne justifieraient pas le recours à l'art. 35 LPD, mais qui, ensemble, rendraient tout de même nécessaire un essai pilote, notamment lorsqu'il s'agit de tester des systèmes d'information et d'examiner des interfaces à travers les différents niveaux fédéraux. Enfin, la pandémie Covid a montré qu'il peut aussi y avoir des raisons non anticipées de réaliser un essai pilote : L'application Swiss Covid a été exploitée pendant une phase d'essai d'un mois sur la base de l'ancien art. 17a aDSG (en relation avec l'art. 78 al. 1 LEp), afin de tester les "nouvelles approches de solutions développées en ce qui concerne la décentralisation du traitement des données et les méthodes cryptographiques, (la) stabilité de l'exploitation, (la) protection contre les manipulations involontaires ou non autorisées, (la) convivialité (ainsi que) l'intelligibilité des informations pour les participants et pour les spécialistes autorisés à y accéder". Dans ce cas et en raison de l'urgence de la situation, la phase pilote n'a duré que du 14 mai 2020 au 25 juin 2020, après quoi l'application a été mise en service régulier.

III. RÉGLEMENTATION DU PROJET PILOTE DANS UN RÈGLEMENT

Même si, contrairement à la disposition précédente, l'art. 17a al. 3 aDSG, l'art. 35 LPD ne prévoit plus explicitement que le Conseil fédéral doit réglementer précisément le projet pilote dans le cadre d'une ordonnance, cette obligation ne subsiste pas seulement en vertu de l'art. 33, al. 2, let. e, OLPD (obligation de l'organe fédéral compétent de consulter le PFPDT dans le cadre de la procédure d'autorisation et de lui soumettre un projet d'ordonnance) : Elle découle du principe de légalité ancré à l'art. 5 al. 1 Cst., dont on peut déduire qu'un minimum de contrôle de l'Etat de droit doit être maintenu même pendant un projet pilote, ou que les atteintes graves aux droits fondamentaux nécessitent au moins une base légale au niveau de l'ordonnance, même pour les projets pilotes. 12

L'ordonnance doit contenir toutes les règles qui devraient être prises au niveau de la loi et de l'ordonnance (en dehors d'un projet pilote). Il est important - en particulier aussi dans la perspective de l'évaluation qui doit impérativement être effectuée (n. 16) - de définir au préalable de manière aussi précise que possible ce qui doit être testé exactement. 13

IV. OBLIGATION DE DEMANDER L'AVIS DU PFPDT (AL. 2)

Le projet pilote doit être soumis au PFPDT pour avis. Cette disposition établit un mécanisme de contrôle essentiel qui tient compte du fait que les projets pilotes peuvent déroger au principe constitutionnel du niveau de la norme. En tant qu'élément des "checks and balances", le PFPDT est au moins responsable de l'examen de plausibilité du projet pilote, du contrôle des mécanismes de protection mis en place, de l'examen de l'ordonnance ainsi que des évaluations régulières. Pour ce faire, conformément à l'art. 33 al. 2 et 3 OLPD, des informations détaillées doivent être fournies au PFPDT, notamment sur le projet pilote en lui-même et sur les mesures (de sécurité) organisationnelles et techniques, un projet ou au moins un concept d'ordonnance devant régir l'expérience pilote, ainsi qu'une planification du projet. 14

Même si le PFPDT ne peut pas émettre d'avis contraignant, il faut partir du principe que le Conseil fédéral suivra en règle générale l'appréciation du PFPDT. 15

V. ÉVALUATION ET LIMITATION DANS LE TEMPS DE LA PHASE PILOTE (AL. 3 ET 4)

16 Le projet pilote doit être évalué au plus tard dans les deux ans suivant sa mise en service (art. 35 al. 3 LPD). L'organe responsable du projet pilote doit exposer au Conseil fédéral, dans le rapport d'évaluation, si le projet peut éventuellement déjà être transformé en une offre régulière, si le projet pilote doit être poursuivi (attention toutefois à la limitation maximale de cinq ans, n. 17) ou si le projet doit être interrompu.

17 Au total, la phase pilote peut durer cinq ans au maximum (art. 35 al. 4 LPD). Ce délai n'est pas extensible, et ce même si le projet pilote doit être transformé en une offre régulière, mais qu'aucune base légale n'a encore été élaborée - l'exploitation "régulière" sur la base d'un simple projet n'est pas admissible pour des raisons d'ordre juridique.

VI. APPRÉCIATION

18 Bien que l'art. 17a aDSG n'ait été appliqué que très rarement jusqu'à présent et que le Conseil fédéral affirme qu'il ne fera qu'exceptionnellement usage de l'art. 35 LPD, on peut tout à fait supposer que la transformation numérique de l'administration entraînera un recours plus fréquent à la disposition sur les essais pilotes. Cela va peut-être dans le sens du développement numérique de l'administration fédérale, mais il ne faut pas perdre de vue que l'application de l'art. 17a aDSG ou de l'art. 35 LPD va toujours de pair avec une érosion du principe de légalité. Il faut donc éviter de recourir trop généreusement à l'article 35 LPD sans qu'il existe par exemple une norme de mission au sens formel ou que l'indispensabilité de la phase de test ait été sérieusement vérifiée. Il ne faut pas non plus oublier que les projets pilotes s'accompagnent de coûts d'investissement élevés - la décision de ne pas poursuivre l'exploitation d'un système après la phase de test devrait donc être non seulement difficile, mais aussi rare.

Dans ce commentaire, l'auteur donne son avis personnel.

BIBLIOGRAPHIE

Husi-Stämpfli Sandra, Kommentierung zu Art. 35, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Huber René, die Teilrevision des Eidg. Datenschutzgesetzes, ungenügende Pinselrenovation, in: recht 2006, S. 205.

Schäfer Marc Frédéric, Kommentierung zu Art. 17a DSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz / Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014.

Oberlin Jutta Sonja/Kessler Rainer, Daten: Die Schlüsselrolle im Kampf gegen die Coronavirus-Pandemie?, in: jusletter 16.11.2020.

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Vokinger Kerstin Noëlle, Die digitale Bekämpfung von Covid-19 und die Rolle des Bundes(rates), SJZ 116/2020, S. 412.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 38 LPD

Un commentaire de Claudia Schreiber

PROPOSITION DE CITATION

Claudia Schreiber, Commentaire sur l'art. 38 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Schreiber, art. 38 LPD N. XXX.

Art. 38 Proposition des documents aux Archives fédérales

[1] Conformément à la loi fédérale du 26 juin 1998 sur l'archivage, les organes fédéraux proposent aux Archives fédérales de reprendre toutes les données personnelles dont ils n'ont plus besoin en permanence.

[2] Ils détruisent les données personnelles que les Archives fédérales ont désignées comme n'ayant plus de valeur archivistique, à moins que celles-ci:

a. ne soient rendues anonymes;

b. ne doivent être conservées à titre de preuve, par mesure de sûreté ou afin de sauvegarder un intérêt digne de protection de la personne concernée.

TABLE DES MATIÈRES

I. En bref 489
II. Généralités 489
A. Historique de la création 489
B. Champ d'application 492
C. Notions 493
III. Proposer des documents dans le contexte de l'évaluation prospective (al. 1) 494
IV. Données personnelles qui ne sont plus nécessaires en permanence (al. 1) 495
V. Destruction de documents sans valeur archivistique (al. 2) 496
VI. Anonymisation des données personnelles (al. 2 let. a) 497
VII. Conservation à des fins de preuve ou de sécurité, sauvegarde des intérêts légitimes de la personne concernée (al. 2 let. b) 497
VIII. Mise en œuvre avec des malentendus 498
IX. Appréciation 501
Bibliographie 502
Matériaux 502

I. EN BREF

L'art. 38 LPD joue un rôle important de passerelle entre la loi fédérale sur la protection des données (LPD) et la loi fédérale sur l'archivage (LAr). 1

Aujourd'hui, l'art. 38 LPD peut donner lieu à des malentendus, car la pratique de l'archivage a changé au niveau fédéral, notamment en relation avec l'introduction de l'évaluation prospective en 2010. 2

II. GÉNÉRALITÉS

A. Historique de la création

Le fait que la protection des données, l'archivage et la recherche historique dépendant de documents archivés présentent des intérêts différents a déjà été suffisamment thématisé. Dans le cadre de l'élaboration de la première loi fédérale sur la protection des données à la fin des années 1970, une partie du monde des archives a craint que les efforts de protection des données n'entraînent une "tendance croissante à la destruction/suppression" et une "retenue dans la pratique d'utilisation ou d'autorisation de certains services". Ces craintes avaient notamment été suscitées par le fait que l'élaboration de la première loi sur la protection des données au niveau fédéral avait eu lieu à une époque où l'archivage n'était réglementé au niveau fédéral qu'au niveau des règlements et des directives. 3

Au départ, il semblait que la nouvelle loi sur la protection des données aborderait en détail la question de l'archivage des données personnelles, puisque le groupe de travail "Protection des données dans l'administration fédérale" avait proposé d'élaborer un article 20 qui, sous le titre "Destruction et archivage des données" ou "Archivage et destruction des données", devait contenir une réglementation détaillée de l'archivage des données (personnelles) : Dans un projet du groupe de travail, on pouvait lire : "Les supports de données contenant des données de valeur durable peuvent être archivés (var. : conservés) aux Archives fédérales au-delà de la durée du traitement initialement nécessaire ; leur traitement ultérieur n'est autorisé que dans le cadre des prescriptions applicables aux Archives fédérales". 4

5 Cette proposition n'a toutefois pas trouvé d'écho par la suite. On a renoncé à une réglementation spéciale concernant l'archivage des données : L'ancien art. 18 al. 2 P-LPD ainsi que l'art. 21 de la première LPD du 19 juin 1992 supprimaient l'archivage de leur titre et stipulaient, sous le titre "Anonymisation et destruction de données personnelles", que les organes fédéraux devaient anonymiser ou détruire les données personnelles dont ils n'avaient plus besoin, dans la mesure où "les données ne servent pas à des fins de preuve ou de sécurité" ou "doivent être versées aux Archives fédérales". C'est ainsi qu'ont été posées les bases du caractère de l'actuel article 38 LPD.

6 Peu après l'entrée en vigueur de la première LPD au niveau fédéral en 1992, le Conseil fédéral a chargé, par décision du 18 août 1993, le Département fédéral de l'intérieur (DFI) d'élaborer un avant-projet de création d'une loi fédérale sur l'archivage. Les travaux ont ensuite été entrepris par un groupe de travail interdépartemental. Le besoin d'une base légale pour l'archivage dans une loi fédérale formelle résultait des bouleversements évidents dans le domaine de l'archivage (entre autres de l'augmentation massive du volume des documents produits par les services fédéraux après la Seconde Guerre mondiale et de la production accrue de documents électroniques dans le dernier quart du XXe siècle) ainsi que de l'exigence de "la réalisation d'une protection adéquate des données", comme l'expose le message relatif à la loi fédérale sur l'archivage du 26 février 1997.

7 Parallèlement, le message relatif à la LAr précise que le droit de consulter les archives ne signifie pas le droit de divulguer des données personnelles sans vérification ou sans esprit critique. Au contraire, le droit de consulter les archives "oblige à un examen critique du contenu des documents archivés ainsi qu'à une interprétation et à une présentation actuelles, tout en préservant la protection de la personnalité", cette responsabilité incombant aux utilisateurs des archives. Il faut noter ici que pour les documents qui sont encore dans le délai de protection et qui n'étaient pas déjà accessibles au public avant le versement (cf. art. 9 al. 2 LAr), le service versant vérifie au préalable, dans le cadre du traitement des demandes de consultation selon l'art. 13 LAr, conformément à l'art. 13 al. 1 let. b, si des intérêts privés prépondérants ne s'opposent pas à une consultation avant l'expiration du délai de protection et si, le cas échéant, la consultation doit être accordée sous certaines charges et conditions, comme par exemple l'anonymisation de données personnelles (art. 13 al. 3 LAr).

Avec l'entrée en vigueur de la LSF en 1999, les questions de protection des données dans le domaine de l'archivage ont désormais été abordées dans une perspective archivistique. En introduisant la réglementation des délais de protection et en créant ainsi la possibilité de prolonger dans certains cas le délai de protection pour la consultation des documents (art. 11 et 12 de la LAr), la LAr visait explicitement une "harmonisation". Comme les archives ne peuvent pas être modifiées (art. 14 al. 4 LAr), la mention de contestation selon l'art. 15 al. 3 LAr complète la réglementation des délais de protection. En outre, conformément à l'art. 14 al. 2 LAr, la consultation de données personnelles par le service producteur ou versant est limitée pendant le délai de protection, à moins que les conditions d'exception prévues à l'art. 14 al. 1 (let. a-d) ne soient remplies. Selon le message relatif à la LSF, il est ainsi garanti que "d'une part, les intérêts des personnes concernées doivent être protégés, mais que d'autre part, la recherche (historique) d'intérêt public ne doit pas être entravée". 8

La nouvelle LSF avait donc désormais un impact sur la loi sur la protection des données déjà existante. Toutefois, jusqu'en 2006, l'article 21 de la loi sur la protection des données ne réglementait le versement de données personnelles aux Archives fédérales qu'à titre exceptionnel, à des fins d'anonymisation et de destruction. 9

L'actuel article 38 LPD a toutefois subi une modification importante en 2008 (version selon le chiffre I de la LF du 24 mars 2006, en vigueur depuis le 1er janvier 2008). Désormais, l'archivage de données personnelles n'était plus un phénomène exceptionnel de destruction ou d'anonymisation. Au contraire, il a été fait référence à la nouvelle loi fédérale sur l'archivage, entrée en vigueur entre-temps. Avec les notions d'"offre", de "proposition" et de "valeur archivistique", cette loi introduit également des concepts issus du monde des archives dans la loi sur la protection des données. 10

Depuis 2008, l'art. 21 de l'aLPD, l'actuel art. 38 de la nouvelle LPD entrée en vigueur le 1er septembre 2023, est resté inchangé sur le fond, mais l'application de la législation sur l'archivage au niveau fédéral a évolué de manière significative durant cette période, comme le montreront les explications suivantes. 11

B. Champ d'application

12 L'art. 38 LPD s'adresse à tous les organes fédéraux selon l'art. 2 al. 1 let. b LPD. L'art. 1 al. 1 de la LSF énumère tous les organes dont l'archivage est réglementé par la LSF. Le destinataire de la norme est également le Tribunal fédéral qui, selon l'art. 1 al. 3, règle certes lui-même l'archivage de ses documents, mais selon les principes de la LAr et après consultation des Archives fédérales suisses (AFS).

13 Indirectement, l'art. 38 LPD peut également avoir de l'importance pour les producteurs de documents selon l'art. 17 al. 2 LGA, c'est-à-dire pour les personnes de droit privé ou public d'importance nationale qui remettent volontairement leurs documents aux AFS pour une conservation et une communication sûres et appropriées. En règle générale, les contrats de donation et de dépôt correspondants mentionnent que les documents à consulter sont soumis aux mêmes dispositions que les documents de l'Etat fédéral (art. 9 ss. de la loi fédérale sur l'archivage, LAr). Par conséquent, il faut partir du principe que, sauf accord contraire entre le producteur de documents et les AFS, les documents d'archives privées qui ont une valeur archivistique et qui représentent ou contiennent des données personnelles peuvent également être versés aux AFS par analogie avec l'art. 38 LPD et notamment en appliquant la réglementation sur les délais de protection selon les art. 9 ss.

14 En ce qui concerne la question de savoir si l'art. 38 LPD ne peut se référer qu'à des données personnelles dont la collecte ou le traitement a été effectué de manière licite, il convient de relever, avec Epiney et d'autres, qu'à l'exigence d'une destruction systématique des documents contenant ou représentant des données personnelles qui ont été collectées et traitées de manière totalement ou partiellement illicite, s'oppose, selon la situation de départ, un intérêt public à la conservation précisément des documents qui ont été établis par l'administration de manière illicite. En outre, une telle réglementation stricte saperait les principes et les objectifs de la LSF ainsi que les éventuelles demandes de consultation des personnes concernées, par exemple en vue d'obtenir un dédommagement. Les fiches de protection de l'Etat, par exemple, qui ont été remises aux AFS, sont des documents précieux de la Confédération, tant du point de vue juridique, politique qu'historique, qui documentent la pratique des autorités fédérales, comme le postule l'art. 2 al. 1 LAr.

C. Notions

Lorsque la législation sur les archives et la législation sur la protection des données entrent en contact - comme dans l'art. 38 LPD -, différentes perspectives et différents mondes conceptuels s'affrontent. La législation sur les archives s'oriente vers la notion de "documents". Selon l'art. 3 al. 1 LAr, les documents sont "toutes les informations enregistrées, quel que soit leur support, qui ont été reçues ou établies dans le cadre de l'accomplissement de tâches publiques de la Confédération, ainsi que tous les outils et données complémentaires nécessaires à la compréhension de ces informations et à leur utilisation". La législation sur la protection des données parle en revanche de données personnelles, définies à l'art. 3 let. a LPD comme "toutes les indications qui se rapportent à une personne identifiée ou identifiable". La question se pose donc de savoir quel est le rapport entre ces deux notions. Pour les explications qui suivent, nous postulons que les données personnelles sont à la fois une sous-catégorie et une caractéristique possible des informations enregistrées (documents). En d'autres termes, les données personnelles sont toujours des documents au sens de la LSF. Inversement, les documents peuvent contenir des données personnelles, mais pas nécessairement. 15

En utilisant les termes "offre" et "proposer", l'article 38 LPD jette un autre pont vers la LPD. Les notions d'offre et de proposition sont toutefois utilisées différemment dans la LSF et la législation d'exécution correspondante, et leur signification a partiellement changé au cours des quinze dernières années. 16

D'une part, la LSF parle des "services tenus de proposer leurs services" et définit ainsi, en relation avec l'art. 1 al. 1 LSF, la relation entre les AFS et les services fédéraux qui sont soumis à l'obligation de donner des instructions des AFS et qui sont tenus de proposer leurs services aux AFS. D'autre part, les termes "offre" et "proposer" décrivent également des étapes de travail dans le cycle de vie des documents. Ces étapes de travail sont liées à l'évaluation des documents et font l'objet d'un changement de pratique important, le passage de l'évaluation rétrospective à l'évaluation prospective, qui est décrit dans le concept général d'évaluation des Archives fédérales en 2010. Ce changement de pratique est abordé dans les chapitres suivants. 17

III. PROPOSER DES DOCUMENTS DANS LE CONTEXTE DE L'ÉVALUATION PROSPECTIVE (AL. 1)

18 Le concept général d'évaluation aux Archives fédérales, publié en 2010, postule en principe l'abandon de l'évaluation rétrospective au profit de l'évaluation prospective.

19 Alors que l'évaluation rétrospective consiste à évaluer des documents déjà produits quant à leur valeur archivistique, l'évaluation prospective prévoit d'évaluer les documents avant même leur production. Cette évaluation a lieu lors de l'élaboration ou de la révision des systèmes de classement conformément aux articles 7 et 8 de l'ordonnance GEVER. Les systèmes de classement sont élaborés par les services fédéraux et, dans le cas des services soumis à l'obligation de proposer, examinés et approuvés par les AFS, pour autant qu'ils répondent aux exigences de l'OGA ou des dispositions d'exécution de la LOGA. Dans un système de classement, les séries de documents sont évaluées au niveau des rubriques, c'est-à-dire qu'il est noté si les documents qui seront produits dans le cadre de l'accomplissement des tâches d'un service fédéral ont une valeur archivistique complète, partielle (sélection ou échantillonnage) ou nulle. Seuls les documents pertinents pour les affaires sont évalués, les documents non pertinents pour les affaires ne sont pas considérés comme des documents au sens de la LAr et ne sont pas soumis à l'obligation de proposer les documents.

20 Le passage à l'évaluation prospective n'a pas été sans conséquences sur la signification du terme "offre" ou "proposer". Lors de l'évaluation rétrospective en application de l'art. 6 al. 1 LAr, les séries de documents existantes étaient proposées aux AFS par les services qui n'archivaient pas de manière autonome avec une proposition d'évaluation juridico-administrative (offre de reprise) et les AFS procédaient à chaque fois en plus à une évaluation rétrospective dans une perspective historique et sociologique.

21 Avec l'introduction de l'évaluation prospective, des "offres" sont faites aux AFS à deux moments différents du cycle de vie des documents. L'évaluation de documents a lieu dans le cadre de l'élaboration ou de l'actualisation d'un système de classement et doit être comprise comme une offre d'évaluation. Les documents ayant une valeur archivistique créés par la suite sont annoncés aux AFS à une date ultérieure pour le versement (c'est-à-dire transmission de fichiers contenant des métadonnées et des données de classement SIP lors du

versement de documents électroniques ou de boîtes d'archives contenant des dossiers papier lors de versements sur papier). Depuis l'introduction de l'évaluation prospective, l'évaluation de documents en collaboration entre les producteurs de documents et les AFS et la transmission ou le versement de documents aux AFS ne coïncident donc plus dans le temps.

Comme indiqué ci-dessus, le service fédéral concerné participe à l'évaluation, en plus des AFS, aussi bien dans le cadre de l'évaluation rétrospective, majoritairement pratiquée avant 2010, que dans celui de l'évaluation prospective après 2010. Le service fédéral qui constitue le dossier évalue les documents par rubrique d'un point de vue juridico-administratif. Cette évaluation est placée sous la responsabilité de la direction/du directoire des services fédéraux concernés et garantit la prise en compte des aspects techniques, juridiques et politiques. Dans un deuxième temps, les AFS vérifient l'évaluation juridico-administrative du service producteur de documents et procèdent en outre à une évaluation selon des critères historiques et sociologiques. Si l'une des deux évaluations est positive, les documents sont considérés comme dignes d'être archivés (entièrement ou partiellement sous forme de sampling ou de sélection). Exceptionnellement, l'évaluation prospective peut être soumise à un contrôle ultérieur. 22

IV. DONNÉES PERSONNELLES QUI NE SONT PLUS NÉCESSAIRES EN PERMANENCE (AL. 1)

La littérature traite souvent la question de savoir quand les données personnelles ne sont plus nécessaires en permanence, sans se référer au contexte du document. Cette approche ne peut guère être mise en œuvre dans la pratique. En effet, les données personnelles sont toujours des documents au sens de la LSF, à moins qu'elles ne soient pas pertinentes pour l'entreprise. L'art. 6 de la LAr stipule que les documents doivent être versés aux AFS lorsqu'ils ne sont plus nécessaires en permanence. 23

Si l'on partait du principe que la réponse à la question de savoir quand les données personnelles ne sont plus nécessaires en permanence est différente de la réponse à la question de savoir quand les documents ne sont plus nécessaires en permanence, il en résulterait que les documents ayant une valeur archivistique qui contiennent ou représentent des données personnelles doivent éventuellement être versés aux AFS à un autre moment 24

que les documents qui ne contiennent ou ne représentent pas de données personnelles. Les AFS partent toutefois du principe que le dossier d'affaires est l'unité déterminante qui doit être soumise à un archivage. A cet égard, les dossiers commerciaux sont souvent de nature mixte : ils se composent aussi bien de documents contenant des données personnelles que de documents qui ne contiennent ou ne représentent pas de données personnelles. Il est donc logique pour les autorités fédérales de considérer la question de savoir quand les données personnelles ne sont plus nécessaires en permanence dans le contexte des documents et de tenir compte des dispositions d'exécution de la LAr sur cette question.

25 Selon l'art. 4 al. 1 OLAr, les documents sont considérés comme n'étant plus requis en permanence lorsque le service tenu de les proposer n'en fait plus un usage fréquent et régulier, mais au plus tard cinq ans après le dernier accroissement du dossier. L'art. 3 al. 1 des Instructions concernant l'obligation de proposer les documents aux Archives fédérales suisses et leur versement du 28 septembre 1999 prévoit en outre que les services tenus de proposer leurs documents aux Archives fédérales vérifient régulièrement, mais au moins tous les cinq ans, leurs classements et leurs mémoires d'informations en vue de repérer les documents dont ils n'ont plus un usage fréquent et régulier. L'art. 4 al. 2 OLAr et l'art. 3 al. 2 des instructions règlent la prolongation de ce délai. L'art. 4 al. 3 OLAr et l'art. 3 al. 3 des instructions règlent en outre les cas de délais raccourcis. Pour certaines catégories de documents, l'art. 4 al. 3 OLAr et l'art. 4 des directives prévoient des dispositions plus spécifiques.

26 Depuis l'introduction de l'évaluation prospective en 2010, ces délais doivent être compris comme le délai de versement aux AFS des documents déjà évalués, donc ayant une valeur archivistique.

V. DESTRUCTION DE DOCUMENTS SANS VALEUR ARCHIVISTIQUE (AL. 2)

27 Concernant le processus de traitement de la destruction, nous renvoyons à l'art. 5 let. d ainsi qu'à l'art. 6 al. 4 LPD.

28 L'expression "données personnelles désignées par les Archives fédérales comme n'ayant pas de valeur archivistique" utilisée à l'alinéa 2 de l'art. 21 est ambiguë, car, comme expliqué plus haut, l'évaluation des documents (et donc

aussi des données personnelles) n'est pas effectuée par les seules AFS, mais par le service producteur du dossier en collaboration avec les AFS. Depuis l'introduction de l'évaluation prospective en 2010, au moment de l'enregistrement des documents dans la gestion électronique des affaires (GEVER), le rattachement du dossier d'affaire correspondant (ou d'une application spécialisée) à une rubrique du système de classement évalué permet de savoir clairement si les documents contenant des données personnelles ou représentant de telles données ont une valeur archivistique (partielle ou totale) ou non.

Dans ce contexte, il convient de mentionner que la destruction de documents doit être consignée et que les procès-verbaux de cassation qui en résultent doivent être envoyés aux AFS. 29

VI. ANONYMISATION DES DONNÉES PERSONNELLES (AL. 2 LET. A)

Concernant la notion d'anonymisation, nous renvoyons au commentaire de l'art. 2 al. 1 let. a LPD ainsi qu'à l'art. 6 al. 4 LPD. L'al. 2 let. a LPD permet aux autorités fédérales de conserver ou de conserver intégralement des documents qui n'ont pas de valeur archivistique ou des documents qui n'ont été évalués que comme ayant une valeur archivistique partielle (sampling ou sélection) et qui ne sont plus utilisés en permanence, à condition qu'ils soient anonymisés. Depuis le passage à la gestion électronique des affaires, il ne peut toutefois s'agir que d'une conservation limitée dans le temps et non d'un archivage au sens des AFS, car les autorités fédérales ne disposent de l'infrastructure nécessaire à un archivage électronique à long terme que dans le cadre du versement aux AFS. 30

VII. CONSERVATION À DES FINS DE PREUVE OU DE SÉCURITÉ, SAUVEGARDE DES INTÉRÊTS LÉGITIMES DE LA PERSONNE CONCERNÉE (AL. 2 LET. B)

Dans le cadre de l'évaluation administrative et juridique, le service chargé de la constitution des dossiers examine si les documents doivent être conservés durablement. L'implication des personnes chargées de constituer les dossiers doit garantir que "les aspects professionnels, juridiques et politiques sont soigneusement pris en compte lors de l'évaluation". D'un point de vue 31

juridico-administratif, les documents ont une valeur archivistique notamment lorsqu'ils servent de preuve de la pratique commerciale, présentent une pertinence juridique ou servent à garantir la sécurité juridique.

32 Si des documents contenant des données personnelles ou représentant des données personnelles doivent être conservés à des fins de preuve ou de sécurité ou pour sauvegarder les intérêts dignes de protection des personnes concernées, ils ont en règle générale déjà été évalués comme ayant une valeur archivistique lors de l'évaluation juridico-administrative. Comme cas d'application de l'art. 38 al. 2 let. b LPD, il faut donc s'attendre, comme dans les cas de l'art. 38 al. 2 let. a LPD, à ce que seules des données personnelles soient contenues dans des documents ou constituent des documents qui ont été évalués comme n'ayant pas de valeur archivistique dans le cadre de l'évaluation prospective ou qui, en cas de valeur archivistique partielle, ne font pas partie de l'échantillon à archiver ou de la sélection à archiver. On peut imaginer par exemple des pièces comptables qui n'ont pas de valeur archivistique et qui sont utilisées comme moyen de preuve dans une procédure en cours ou en préparation.

VIII. MISE EN ŒUVRE AVEC DES MALENTENDUS

33 Dans la pratique, l'art. 38 LPD n'est toutefois pas encore systématiquement compris dans ce sens, comme le montrent la littérature et la jurisprudence. Dans l'arrêt A-4236/2021 du TAF du 21 mars 2023, qui se réfère à l'art. 21 aDSG, l'AFC, par exemple, qui dispose d'un système de classement accepté, défend le point de vue, dans le cadre d'une demande de destruction de données, que l'AFC "peut décider elle-même" quand "les données traitées légalement doivent être proposées aux Archives fédérales". Une partie ne peut pas demander que les données personnelles traitées légalement soient proposées aux Archives fédérales ou qu'elles soient détruites. C'est pourquoi elle n'est pas tenue de proposer aux Archives fédérales, à la demande du recourant, les données personnelles traitées légalement dans un dossier dont le dernier ajout au dossier a eu lieu en 2020, ni de les détruire". L'AFC se réfère ainsi aux délais fixés par la LAr et la législation d'exécution de la LAr, mais omet en même temps de signaler que les documents en question ont déjà été évalués par l'AFC et les AFS.

34 Dans sa décision du 21 mars 2023, le Tribunal administratif fédéral s'oriente également vers la pratique d'évaluation d'avant 2010 et écrit : "Il n'appartient

pas au Tribunal administratif fédéral de clarifier la question de la valeur archivistique des données collectées par l'instance précédente dans le cadre de la procédure d'assistance administrative en tant que première instance dans la procédure de recours, d'autant plus que la compétence pour prendre cette décision n'appartient pas à l'instance précédente, mais aux Archives fédérales, qui n'ont pas encore pu se prononcer à ce sujet. [...] L'instance inférieure doit proposer les données collectées dans le cadre de la procédure d'entraide administrative aux Archives fédérales et, si celles-ci estiment que les données ont une valeur archivistique, les leur verser. Si les données ne sont pas considérées comme ayant une valeur archivistique, l'instance inférieure doit détruire les données".

Cette décision récente du Tribunal administratif fédéral illustre de manière exemplaire les malentendus auxquels la version actuelle de l'art. 38 al. 1 LPD peut donner lieu : L'article 38 al. 1 LPD semble suggérer - en tout cas selon la lecture qu'en font l'AFC et le TAF - que les services soumis à l'obligation de proposer ne peuvent détruire des données personnelles, en l'occurrence sous la forme d'un dossier commercial concernant un cas fiscal et se rapportant à une personne déterminée, que si les AFS se sont prononcées concrètement sur ce dossier particulier et son évaluation. Cela n'est pas compatible avec la pratique d'archivage des AFS, et ce pour les raisons suivantes : 35

a) Dans le cas présent, l'AFC, service tenu de proposer ses documents, et les AFS ont déjà procédé à une évaluation prospective lors de l'élaboration du système de classement de l'AFC en 2015. Le système de classement de l'AFC ou le rattachement du dossier commercial en question à une rubrique du système de classement permet de déterminer si les documents issus de cette activité spécifique de l'AFC (échange d'informations en matière fiscale) ont ou non une valeur archivistique. Les AFS et l'AFC se sont donc déjà prononcées sur la question de savoir si la série de documents à laquelle appartient le dossier ou le document en question a une valeur archivistique (partielle ou totale) ou non.

b) L'évaluation, prospective ou rétrospective, porte sur des séries de documents produits dans le cadre de l'accomplissement de certaines tâches et, le cas échéant, sur des applications spécialisées - mais pas sur des enregistrements individuels, des données personnelles individuelles, des documents individuels ou des dossiers commerciaux. En d'autres termes : La manière dont ces séries de documents sont établies et, en particulier, la forme

sous laquelle les documents sont classés dans des dossiers, relèvent, selon l'art. 2, al. 2, ainsi que l'art. 5, al. 2 et 3, LAr, en relation avec l'art. 5, al. 2, de la loi sur la protection des données. L'art. 3 OLAr ainsi que l'art. 6 de l'ordonnance GEVER et l'art. 22 de l'OLOGA relèvent de la compétence des services tenus de proposer les documents ou de créer des dossiers. Ceux-ci sont tenus de veiller à la traçabilité et à la preuve de leur activité commerciale dans leurs dossiers.

36 Si, dans le cas mentionné ci-dessus, la série de documents correspondante avait été évaluée dans le système de classement de l'AFC comme ayant une valeur archivistique ou comme ayant une valeur archivistique partielle (sélection ou échantillonnage), le service producteur de documents n'aurait qu'à décider, en application de la LAr et des dispositions d'exécution de la LAr, quand le dossier en question doit être versé aux AFS. Dans ce cas, le service producteur déciderait en outre si le document en question est nécessaire à la traçabilité et à la preuve de l'activité commerciale dans ce dossier. En cas de valeur archivistique partielle, le service chargé de la constitution des dossiers appliquerait également les critères de sélection et d'échantillonnage définis dans le système d'information. Dans cette constellation, les AFS n'auraient plus non plus de pouvoir de décision après la réalisation de l'évaluation prospective.

37 Si la série de documents correspondante n'avait pas été jugée digne d'être archivée, c'est également le service producteur du dossier qui déciderait comment traiter le document ou le dossier d'affaire en question contenant des données personnelles. Il s'agirait de savoir si ce dossier devrait être conservé temporairement par le producteur du dossier lui-même, sous une forme anonymisée conformément à l'art. 38, al. 2, let. a LPD ou sous une forme non anonymisée conformément à l'art. 38, al. 2, let. b LPD, à des fins de preuve et de sécurité ou pour sauvegarder les intérêts dignes de protection de la personne concernée. Dans ce cas de figure également, les AFS n'auraient plus de pouvoir de décision après la réalisation de l'évaluation prospective.

38 Dans ce contexte, l'art. 8 al. 1 LSF doit être compris en ce sens que seuls les documents qui n'ont pas été proposés aux AFS pour une évaluation (prospective) ne peuvent pas être détruits sans l'accord des AFS. Compte tenu de l'obligation globale de proposer les documents aux AFS, de tels documents devraient avoir une valeur de rareté.

IX. APPRÉCIATION

L'art. 38 LPD trouve son origine dans les années 1980 et a été conçu comme un instrument destiné à empêcher que les producteurs de documents, sous prétexte de protection des données, ne soustraient à l'archivage par les AFS des documents contenant des données personnelles ou représentant des données personnelles qui ont une valeur archivistique, sur la seule base de ce fait. L'art. 38 LPD est encore pertinent aujourd'hui dans la mesure où cette disposition précise le principe du traitement proportionné des données en ce qui concerne l'archivage : Ce n'est pas seulement l'anonymisation ou la destruction de documents qui n'ont pas de valeur archivistique et qui contiennent ou représentent des données personnelles qui est proportionnelle, mais aussi le versement (non anonymisé) de tels documents aux AFS, pour autant qu'ils aient une valeur archivistique. 39

Dans sa version actuelle, l'art. 38 al. 1 LPD s'oriente vers la pratique de l'évaluation rétrospective, telle qu'elle était pratiquée de manière standard par les AFS jusque dans les années 2000. Depuis le passage à l'évaluation prospective en tant que processus standard, tous les services fédéraux évaluent leurs documents d'un point de vue juridico-administratif conformément à l'art. 1 al. 1 LAr et les AFS d'un point de vue socio-historique dans le cadre de l'élaboration de systèmes de classement, c'est-à-dire avant la création des documents. 40

Un article 38 révisé pourrait à l'avenir se limiter, sous le titre "Archivage de données personnelles", à stipuler que les documents selon les LAr contiennent ou peuvent représenter des données personnelles et doivent être traités conformément aux prescriptions des LAr (alinéa 1). Un nouvel al. 2 pourrait stipuler que les documents ne présentant pas de valeur archivistique et contenant ou représentant des données personnelles doivent être détruits, à moins que les conditions mentionnées dans l'actuel al. 2 let. a et b ne s'appliquent. 41

L'auteure remercie MAS ISc Barbara Kräuchi pour l'échange professionnel stimulant qui a eu lieu au cours des recherches effectuées pour le présent article.

BIBLIOGRAPHIE

Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014 (zit. BSK-Bühler).

Epiney Astrid, Commentaire de l'art. 38 LPD, in: Meier Philippe/Métille Sylvain (Hrsg.), Commentaire romand, Loi fédérale sur la protection des données, Bâle 2023 (zit. CR-Epiney).

Graf Christoph, Datenschutz als Herausforderung für Historiker und Archivare, in: Schweizerisches Bundesarchiv (Hrsg.), Studien und Quellen 8, Bern 1982, S. 75–115 (zit. Graf).

MATÉRIAUX

BAR, E3120B#1995/16#374*: Allgemeines [PUK I (EJPD)]. 1990–1991.

BAR, E3120B#1995/16#379*: Allgemeines [PUK II (EMD)]. 1990–1991.

BAR, E3120B#1996/434#391*: Resolution zum Problem der Datenschutzgesetzgebung der Vereinigung Schweizerischer Archivare VSA vom 29.4.1983. 1983–1985.

BAR, E4110B#1992/42#319*: Arbeitsgruppe Datenschutz in der Bundesverwaltung. 1979.

Botschaft über das Bundesgesetz über die Archivierung vom 26.2.1997, BBl 1997 II, S. 941–976, abrufbar unter https://fedlex.data.admin.ch/eli/fga/1997/2_941_829_753, besucht am 5.2.2024 (zit. Botschaft BGA 1997).

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988 II 413, S. 413–534, abrufbar unter https://fedlex.data.admin.ch/eli/fga/1988/2_413_421_353, besucht am 5.2.2024 (zit. Botschaft DSG 1988).

Schweizerisches Bundesarchiv, Bewertungsentscheid (Auszug), Prospektive Bewertung ESTV (Ordnungssystem 2015), 2015, abrufbar unter https://www.bar.admin.ch/dam/bar/de/dokumente/bewertungsentscheide/ESTV%20Bewertungsentscheid%20OS%202015.pdf.download.pdf, besucht am 5.2.2024 (zit. Schweizerisches Bundesarchiv, Bewertungsentscheid).

Schweizerisches Bundesarchiv, Gesamtkonzept für die Bewertung im Bundesarchiv, Bern 2010, abrufbar unter https://www.bar.admin.ch/dam/bar/

de/dokumente/konzepte_und_weisungen/gesamtkonzept_2010.pdf.download.pdf, besucht am 5.2.2024 (zit. Schweizerisches Bundesarchiv, Bewertung).

Schweizerisches Bundesarchiv, Merkblatt Löschprotokoll, abrufbar unter https://www.bar.admin.ch/dam/bar/de/dokumente/kundeninformation/Merkblatt%20L%C3%B6schprotokoll.pdf.download.pdf, besucht am 5.2.2024 (zit. Schweizerisches Bundesarchiv, Löschprotokoll).

Schweizerisches Bundesarchiv, Schenkungsvertrag, abrufbar unter https://www.bar.admin.ch/dam/bar/de/dokumente/kundeninformation/schenkungsvertrag.pdf.download.pdf, zuletzt konsultiert am 05.2.2024 (zit. Schweizerisches Bundesarchiv, Schenkungsvertrag).

Schweizerisches Bundesarchiv, Staatsschutzfichen und -dossiers: Einsichtsverfahren und praktische Hinweise, in: bar.admin.ch, https://www.bar.admin.ch/bar/de/home/recherche/recherchetipps/themen/nachrichtendienste--spione--landesverraeter-und-staatsschutz-in-/staatsschutzfichen-und--dossiers--einsichtsverfahren-und-praktis.html, besucht am 5.2.2024 (zit. Schweizerisches Bundesarchiv, Staatsschutzfichen).

Schweizerisches Bundesarchiv, Von der Geschäftsablage ins Bundesarchiv, Angebot und Bewertung von Unterlagen des Bundes, Arbeitshilfe, Bern 2023, abrufbar unter https://www.bar.admin.ch/dam/bar/de/dokumente/publikationen/von_der_geschaeftsablageinsbundesarchivangebotundbewertungvonunt.pdf.download.pdf, besucht am 5.2.2024 (zit. Schweizerisches Bundesarchiv, Arbeitshilfe).

Weisungen über die Aktenführung in der Bundesverwaltung vom 13.7.1999, BBl 1999, S. 5428–5438, abrufbar unter https://www.fedlex.admin.ch/eli/fga/1999/1_5428_4988_4679/de, besucht am 5.2.2024 (zit. Weisungen Aktenführung).

Weisungen über die Anbietepflicht und die Ablieferung von Unterlagen an das Schweizerische Bundesarchiv vom 28.9.1999, https://www.bar.admin.ch/dam/bar/de/dokumente/gesetzgebung/weisungen_ueber_dieanbietepflichtunddieablieferungvonunterlagena.pdf.download.pdf, besucht am 5.2.2024 (zit. Weisungen Anbietepflicht).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 39 LPD

Un commentaire de Philipp do Canto

PROPOSITION DE CITATION

Philipp do Canto, Commentaire de l'art. 39 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-do Canto, art. 39 LPD N. XXX.

Art. 39 Traitements à des fins ne se rapportant pas à des personnes

[1] Les organes fédéraux sont en droit de traiter des données personnelles à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, si les conditions suivantes sont réunies:

a. les données sont rendues anonymes dès que la finalité du traitement le permet;

b. l'organe fédéral ne communique des données sensibles à des personnes privées que sous une forme ne permettant pas d'identifier les personnes concernées;

c. le destinataire ne communique les données à des tiers qu'avec le consentement de l'organe fédéral qui les lui a transmises;

d. les résultats du traitement ne sont publiés que sous une forme ne permettant pas d'identifier les personnes concernées.

[2] Les art. 6, al. 3, 34, al. 2, et 36, al. 1, ne sont pas applicables.

TABLE DES MATIÈRES

En bref ... 508
I. Généralités ... 508
II. Al. 1, conditions en détail ... 509
A. Fait de base : finalité non personnelle ... 509
B. Let. a, Anonymisation la plus précoce possible ... 510
C. Let. b, Données sensibles ... 511
D. Let. c, Exigence de consentement en cas de transmission. ... 512
E. Let. d, publication des résultats. ... 512
III. Al. 2, Exceptions ... 513
IV. Législation spéciale ... 514
A. Loi sur la statistique fédérale ... 514
B. Loi sur l'harmonisation des registres ... 514
C. Systèmes d'information de police ... 514
D. Droit de la recherche sur l'être humain et recherche des EPF ... 515
E. Archives de la Confédération ... 515
Bibliographie ... 515
Matériaux ... 516

EN BREF

L'art. 39 LPD autorise les organes fédéraux à traiter des données à des fins non personnelles sous certaines conditions. Cette règle accorde des facilités au sens du « privilège de la recherche » pour la recherche, la statistique, la planification et d'autres domaines. Le sens de cette disposition est le grand intérêt public des activités concernées. Le privilège n'est valable que si les conditions-cadres sont respectées. Premièrement, l'art. 39 al. 1 LPD exige l'anonymisation la plus précoce possible dans le cadre du traitement des données personnelles. Deuxièmement, l'accord de l'organe fédéral est nécessaire pour la communication de données du destinataire à des tiers. Troisièmement, comme pour le traitement privé des données selon l'art. 31 al. 2 let. e LPD, les organes fédéraux ne peuvent publier des résultats de recherche ou autres que de manière à ce que les personnes concernées ne soient pas identifiables.

Comme le traitement de données non personnelles ne concerne pas l'identité des personnes concernées, l'art. 39 al. 2 LPD déclare que des principes importants ne sont pas applicables. Ainsi, le principe de finalité et l'exigence d'une base légale ne s'appliquent pas dans certains cas de figure, comme par exemple pour la communication de données personnelles. En revanche, il convient de tenir compte de nombreuses dispositions de lois spéciales, notamment dans le domaine de la statistique et de la recherche, qui relativisent l'importance pratique de l'article 39 LPD.

I. GÉNÉRALITÉS

1 L'art. 39 LPD relatif au traitement de données à des fins ne se rapportant pas à des personnes par des organes fédéraux reprend dans une large mesure la disposition précédente de l'art. 22 aDSG avec le « **privilège de la recherche** ». Une précision concernant les données personnelles sensibles est nouvelle. Selon l'art. 39 LPD, les organes fédéraux doivent (continuer à) bénéficier d'allègements lors de traitements à des fins non personnelles s'ils respectent les conditions-cadres. Ce privilège est justifié par l'intérêt public des activités concernées de l'État. La recherche et les statistiques fournissent des bases pour tous les aspects de la vie publique.

Parmi les **conditions à remplir pour bénéficier d'allégements**, on trouve d'une part l'obligation de rendre les données anonymes le plus tôt possible (al. 1 let. a). D'autre part, des conditions doivent être respectées en ce qui concerne la communication de données personnelles sensibles à des tiers (al. 1 let. b). Ensuite, le consentement du destinataire est requis en cas de transmission (al. 1 let. c) et, enfin, le principe d'indétermination s'applique lors de la publication des résultats (al. 1 let. d). L'art. 39 al. 2 déclare certains principes de la LPD inapplicables en raison des risques réduits liés aux traitements non personnels (al. 2). 2

La disposition ne concerne que les **traitements de données effectués par des organes fédéraux**. La disposition cite la recherche, la statistique et la planification comme domaines privilégiés, l'énumération n'étant pas exhaustive. Outre la statistique de la Confédération, sont donc concernées, entre autres, la recherche effectuée par des institutions de la Confédération ou sur son mandat, la planification nationale du territoire et des transports, la Banque nationale, l'administration des migrations ou la santé publique. Contrairement au domaine privé, la recherche médicale réglementée par le droit de la recherche sur l'être humain est plutôt à l'arrière-plan de la disposition, car le domaine est principalement porté par les cliniques universitaires cantonales et la recherche pharmaceutique privée. En revanche, la recherche du domaine des EPF est couverte en tant qu'unité fédérale décentralisée. 3

En raison de l'exigence d'une base légale pour les traitements de données effectués par l'Etat, il existe aujourd'hui une vaste **réglementation** des différentes activités **par des lois spéciales** (ci-dessous, IV). L'article 39 LPD perd donc sa signification propre dans de nombreux cas de figure ou doit être lu en relation avec les dispositions spécifiques à la matière. 4

II. AL. 1, CONDITIONS EN DÉTAIL

A. Fait de base : finalité non personnelle

L'élément central de la disposition est le traitement à des fins non personnelles. On entend par finalités non personnelles celles pour lesquelles l'**identité de la personne concernée n'est pas pertinente**. En d'autres termes, la finalité de l'activité est également remplie si des données anonymes ou codées étaient traitées. Le traitement de données relatives à une grande 5

partie de la population ou à des groupes particuliers est couvert, pour autant qu'il s'agisse uniquement des caractéristiques et non de l'identité des personnes saisies. Si seules des données factuelles ou des données préalablement anonymisées sont traitées, la disposition n'est pas applicable.

6 La mention expresse des domaines ne signifie pas que le traitement des données dans les domaines de la recherche, de la statistique et de la planification ne sert pas à des fins personnelles. Il arrive notamment que des traitements servent **également à des fins personnelles**. Pour de telles activités, l'art. 35 OPDo stipule que les exceptions prévues à l'art. 39, al. 2, LPD ne s'appliquent qu'au traitement à des fins ne se rapportant pas à des personnes.

7 La phrase introductive de l'al. 1 contient la conséquence juridique, à savoir l'**autorisation** facilitée **du traitement des données**, si les conditions de la disposition, qui seront expliquées plus loin, sont respectées.

B. Let. a, Anonymisation la plus précoce possible

8 Les organes fédéraux doivent (en principe) **anonymiser** les données dès que le but du traitement le permet. La disposition reprend ainsi le principe de l'art. 6 al. 4 LPD. Un délai jusqu'à l'anonymisation n'est pas mentionné. Une réglementation générale et abstraite ne tiendrait pas compte des besoins respectifs de la statistique, de la recherche et de la planification.

9 Contrairement à l'art. 31 al. 2 let. e LPD, aucune dérogation n'a été introduite pour permettre d'autres mesures visant à empêcher l'identification de la personne si l'anonymisation est impossible ou disproportionnée. Les avis divergent sur la question de savoir si la **pseudonymisation** ou le cryptage des données personnelles est également suffisant. S'il existe un code ou une clé permettant de réidentifier des données personnelles (partiellement) anonymisées, on parle de pseudonymisation. Une partie de la doctrine ne veut autoriser le cryptage que si le traitement conduit en fin de compte à l'anonymisation. L'opinion contraire s'appuie sur le besoin, répandu dans la pratique, de pouvoir revenir à l'identité de la personne concernée, ce qui s'oppose à l'anonymisation, notamment à l'anonymisation précoce exigée. L'anonymisation générale ne se recoupe en outre pas avec la let. b, selon laquelle il suffit déjà, pour les données personnelles sensibles, que celles-ci ne soient pas identifiables lors de leur communication à des personnes privées,

ce qui permet également un cryptage. Si le cryptage ou « l'anonymisation de fait » suffisent pour la communication de données sensibles, cela devrait *a maiore minus* également s'appliquer aux données moins sensibles. Le message relatif à l'aDSG mentionne un besoin de pseudonymisation. Un arrêt du Tribunal fédéral ne répond pas de manière définitive à la question, mais considère que la solution réside dans l'objectif de chaque procédure : « La dissimulation a certes des limites. Elle ne doit pas avoir pour conséquence que le jugement ne soit plus compréhensible. Il ne peut donc pas être totalement exclu que des personnes connaissant les détails de l'affaire puissent, le cas échéant, reconnaître de qui il s'agit malgré la dissimulation ». Si l'anonymisation retire donc la finalité du traitement (qui ne doit cependant toujours pas être liée à la personne), d'autres mesures appropriées visant à empêcher l'identification de la personne devraient par conséquent également être autorisées.

C. Let. b, Données sensibles

La deuxième condition concerne la communication de données sensibles à des personnes privées. Cette disposition vient s'ajouter, en tant que réglementation spécifique, aux dispositions générales sur la communication de données de l'article 36 LPD. S'il s'agit de données sensibles, le principe est que celles-ci ne peuvent être communiquées à des tiers que de manière **à ce que la personne concernée ne soit pas identifiable**. Contrairement au libellé de la let. a, l'anonymisation n'est pas exigée ici, mais le cryptage préalable suffit également pour renforcer la protection des données. 10

En ce qui concerne les mesures visant à empêcher l'identification, il convient de mentionner le vaste catalogue de **mesures techniques et organisationnelles** de l'article 3 OPDo, notamment les règles relatives à la confidentialité et à l'intégrité. Il existe en outre différentes directives sur le cryptage, comme les directives de liaison scientifiques obligatoires de l'Office fédéral de la statistique ou les Guidelines de l'Agence européenne pour la cybersécurité (Enisa). Les directives contiennent entre autres des conditions relatives à la manipulation des codes et à la dé-pseudonymisation. 11

Les prescriptions légales en matière de confidentialité jouent également un rôle important. Lorsque la législation spéciale n'autorise pas intégralement la transmission de données sensibles (à des personnes privées), elle prévaut en tant que réglementation spéciale. La let. b ne peut donc pas être invoquée 12

comme motif justificatif pour la communication de données protégées par le secret.

D. Let. c, Exigence de consentement en cas de transmission.

13 Troisièmement, les données peuvent être transmises pour être traitées à des fins non personnelles. Toutefois, selon la let. c, le consentement de l'organe fédéral est nécessaire pour la transmission des données. L'accord de l'organe fédéral doit être assorti de la condition que les obligations relatives à l'anonymisation et à la publication soient transmises au tiers.

14 La **Banque nationale** est soumise à la disposition spéciale de l'art. 16 al. 4bis LBN, selon laquelle elle est autorisée à communiquer à l'OFS des données à des fins statistiques sous une forme non agrégée. Nonobstant l'article 39 LPD, l'OFS ne peut pas transmettre les données de la Banque nationale sans son consentement.

15 L'art. 39 al. 1 let. c ne précise pas la **forme du consentement**. Selon le message relatif à l'aDSG, le consentement peut ou doit être donné par voie contractuelle ou par voie de décision.

E. Let. d, publication des résultats.

16 Let. d reprend la disposition actuelle selon laquelle les personnes concernées ne doivent pas être identifiables lors de la publication des résultats (art. 22 al. 1 let. c aDSG). Malgré la même formulation que l'art. 31 al. 2 let. e ch. 3 LPD, une **anonymisation** (complète) est ici exigée lors de la publication. Une anonymisation partielle ou une pseudonymisation, comme c'est le cas dans la recherche médicale sur l'être humain, ne suffit donc pas. Des exceptions sont toutefois envisageables lorsqu'il s'agit de données relatives à des personnes de l'histoire contemporaine ou lorsque des intérêts prépondérants à la transparence des relations exigent la consultation du dossier.

17 La doctrine fait remarquer que la publication d'études avec peu de personnes concernées peut entraîner un **risque d'inférence** sur la personne, ce qui est concevable par exemple pour les statistiques concernant des zones géographiques restreintes. Lors de la publication de résultats sur la base de données de nombreuses personnes concernées, cela semble toutefois moins problématique dans la mesure où l'identification de la personne par un être humain est plus difficile. En revanche, les systèmes technologiques

fonctionnent indépendamment des restrictions géographiques ou numériques, de sorte qu'en fin de compte, le progrès technique accroît constamment les exigences en matière de publication des résultats.

III. AL. 2, EXCEPTIONS

L'article 39 al. 2 LPD déclare trois dispositions de la LPD inapplicables. 18

Tout d'abord, l'**obligation d'affectation** ou d'interdiction de modification de la finalité selon l'art. 6 al. 3 LPD n'est pas applicable. Comme les travaux de recherche, de planification et de statistique n'ont pas d'effets directs sur les personnes concernées, conformément à l'article 39 LPD, les données peuvent être utilisées dans un autre contexte que celui pour lequel elles ont été collectées. La limite de l'utilisation est toutefois fixée par l'article 39 al. 1, selon lequel il ne peut s'agir que d'objectifs ne se rapportant pas à des personnes. Dans ce cadre, les données peuvent être traitées à n'importe quelle fin légitime. En d'autres termes, la disposition d'exception n'autorise pas le traitement à d'autres fins se rapportant à des personnes. 19

La deuxième exception est l'art. 34 al. 2 LPD. Selon cet article, l'**exigence d'une base légale formelle** est supprimée pour le traitement de données personnelles et de profils sensibles ainsi que pour les activités risquant de porter gravement atteinte aux droits fondamentaux. Le principe de légalité ne disparaît donc pas complètement. L'art. 34 al. 1 LPD reste applicable. Une base juridique au niveau de l'ordonnance est donc encore attendue pour les traitements correspondants. 20

La troisième exception concerne l'art. 36, al. 1 LPD sur la communication de données personnelles. Par conséquent, **aucune base légale spécifique n'est nécessaire** pour la **communication de données personnelles**. Outre le fait que l'art. 39 al. 1 LPD contient des conditions relatives à la communication de données personnelles, des prescriptions devront également être régulièrement respectées en vertu de la législation spéciale. En l'absence de prescriptions, un organe fédéral peut se fonder sur cette exception. Cette disposition ne supprime pas non plus le principe de légalité pour la communication. 21

IV. LÉGISLATION SPÉCIALE

22 En raison de l'**exigence** susmentionnée **d'une base légale** pour les traitements de données effectués par l'État, il existe aujourd'hui une législation spéciale étendue pour les activités des organes fédéraux. Selon le degré de détail, celles-ci peuvent dans une large mesure remplacer l'article 39 LPD, y renvoyer ou compléter cette disposition.

A. Loi sur la statistique fédérale

23 L'art. 19 al. 2 LSF contient une prescription presque identique dans son libellé à l'adresse des producteurs de statistiques de la Confédération concernant la communication de données à des fins ne se rapportant pas à des personnes. La disposition se limite à la communication, car la LSF contient des prescriptions déterminantes sur la collecte et le traitement (art. 4 ss LSF). Au-delà des conditions fixées à l'art. 39 al. 1 LPD, l'art. 19 al. 2 let. d LSF exige le respect du **secret statistique** ainsi que des autres dispositions relatives à la protection des données. A cet égard, l'art. 16 al. 1 LSF précise que les données personnelles sont soumises « en outre », c'est-à-dire à titre subsidiaire, aux prescriptions de la LPD en matière de recherche, de statistique et de planification.

B. Loi sur l'harmonisation des registres

24 Dans le domaine des **statistiques démographiques**, c'est ensuite la loi sur l'harmonisation des registres (LHR) qui est déterminante. L'harmonisation des registres vise à uniformiser et à simplifier les registres communaux et cantonaux afin d'accroître leur utilité statistique et de réduire la charge administrative. En outre, l'harmonisation des registres apporte des allégements pour les registres concernés. Elle permet l'échange électronique de données, réglementé par la loi, entre différents registres officiels (cf. art. 1 LHR).

C. Systèmes d'information de police

25 Les autorités policières et judiciaires exploitent de nombreux registres et systèmes d'information. Ces systèmes sont régis par la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP). L'art. 6 al. 4 LSIP autorise les responsables à conserver sous forme anonymisée des données

destinées à être effacées, dans la mesure où cela est nécessaire à **des fins statistiques ou d'analyse criminelle**. La recherche utilisant des données anonymisées ne relève plus de l'article 39 LPD, car il ne s'agit plus de données personnelles.

D. Droit de la recherche sur l'être humain et recherche des EPF

Le droit de la recherche sur l'être humain (en cours de révision), avec la LRH et les actes législatifs apparentés, comme la loi sur l'enregistrement du cancer, qui contiennent des prescriptions propres sur la pseudonymisation ainsi que des dispositions de triage concernant l'application de la LRH et de la LPD (p. ex. art. 28 LEMO), est également important. Dans le domaine de la recherche, le développement du **consentement électronique** (e-consent, art. 8b P-CH), qui permet de renoncer à la forme écrite sous certaines conditions, revêt une importance particulière. Le consentement électronique joue un rôle particulier pour la réutilisation future dans la recherche, où les projets n'ont souvent pas (ou plus) de finalité personnelle (art. 17 LRH). 26

Enfin, pour le **domaine des EPF**, l'art. 36c al. 1 révisé de la Loi sur les EPF stipule que des données personnelles, y compris des données personnelles sensibles, peuvent être traitées dans le cadre de projets de recherche, dans la mesure où le projet correspondant l'exige. Selon l'al. 2, la LPD doit être respectée. 27

E. Archives de la Confédération

Il convient enfin de mentionner la loi fédérale sur l'archivage (LAr), qui contient le cadre réglementaire pour les archives de la Confédération, notamment pour l'administration fédérale, le Parlement et les tribunaux de la Confédération. Eu égard aux données personnelles sensibles contenues dans des archives non anonymisées, l'art. 11 al. 1 LAr prévoit un **délai de protection prolongé** de 50 ans. 28

BIBLIOGRAPHIE

Baeriswyl Bruno, Die Einwilligung hilft (nicht) weiter, digma 2020 S. 62 ff. (zit. Baeriswyl).

Baeriswyl Bruno/Pärli Kurt (Hrsg.), Datenschutzgesetz (DSG), Stämpflis Handkommentar, Bern 2015 (zit. SHK aDSG-Bearbeiter/-in).

Kley Andreas/Zihler Florian, Geschichtswissenschaftliches Arbeiten im Rahmen der Kommunikationsgrundrechte, Medialex 2003 S. 85 ff.

Maurer-Lambrou, Urs/Blechta, Gabor-Paul (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014 (zit. BSK-Bearbeiterin).

Perucchi Stefano/Bernasconi Jonathan/Ceroni Davide, in: Kellerhals Carrard/Bürgschaftsgenossenschaften Schweiz (Hrsg.), Corona-Kredite für KMU, Umsetzung des Massnahmenpakets und Kommentierung des Covid-19-Solidarbürgschaftsgesetzes (Covid-19-SBüG), Zürich 2021 (zit. Perucchi/Bernasconi/Ceroni).

Reudt-Demont Janine, Digitalisierung des Gesundheitswesens 2023, LSR 2023 S. 39 ff. (zit. Reudt-Demont).

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. Rosenthal/Jöhri (2008)).

Belser Eva Maria/Noureddine Houssein, Die Datenschutzgesetzgebung des Bundes, Das Zusammenwirken datenschutzrechtlicher Normen, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard (Hrsg.), Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, S. 412-460 und S. 461-509 (zit. Belser/Houssein).

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 6941 ff., abrufbar https://www.fedlex.admin.ch/eli/fga/2017/2057/de (zit. Botschaft 2017).

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988 II 413 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/ de (zit. Botschaft 1988).

Erläuterungsbericht Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz, BJ, 23.6.2021; Entwürfe zur Revision der Verordnungen in der Humanforschung, abrufbar unter https://www.bag.admin.ch/bag/de/home/

medizin-und-forschung/forschung-am-menschen/revision-verordnungen-hfg.html (zit. Erläuterungsbericht).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 40 LPD

Un commentaire de Anna Kuhn

PROPOSITION DE CITATION

Anna Kuhn, Kommentierung zu Art. 40 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Kuhn, N. XXX zu Art. 40 DSG.

Art. 40 Activités de droit privé exercées par des organes fédéraux

Lorsqu'un organe fédéral agit selon le droit privé, le traitement des données personnelles est régi par les dispositions applicables aux personnes privées.

TABLE DES MATIÈRES

En bref ... 521
I. Généralités ... 521
A. Remarques préliminaires ... 521
B. But de la norme et contexte ... 521
C. Historique ... 522
II. Champ d'application ... 523
III. Actions de l'Etat relevant de la puissance publique et du droit privé ... 523
A. Catégorisation de l'action étatique ... 523
B. L'action souveraine comme principe ... 524
C. Action de droit privé ... 524
1. Principes de base ... 524
2. Délimitation selon le pluralisme des méthodes ... 525
3. Les cas d'actes licites de droit privé ... 526
IV. Conséquences juridiques ... 527
A. Dispositions applicables en matière de protection des données ... 527
B. Procédures ... 527
C. Autre application du droit public ... 528
1. Principes constitutionnels ... 528
2. Obligation de respecter les droits fondamentaux ... 528
3. Théorie des deux niveaux dans la procédure de soumission ... 528
V. Casuistique ... 529
Bibliographie ... 530
Matériaux ... 531

EN BREF

L'art. 40 LPD s'applique lorsque des organes fédéraux agissent en vertu du droit privé au sens de l'art. 5 let. i LPD. Cela est possible lorsqu'un domaine n'est pas réglé de manière exhaustive par le droit public et laisse donc la place à des actes de droit privé. Pour déterminer cela au cas par cas, il faut d'abord vérifier l'existence d'une réglementation spéciale et ensuite procéder à une délimitation entre les actions relevant de la puissance publique et celles relevant du droit privé. Les activités administratives auxiliaires, la gestion du patrimoine financier, les activités de l'État relevant de l'économie privée et certaines parties de la gestion des prestations constituent des domaines dans lesquels les pouvoirs publics peuvent normalement agir en vertu du droit privé. En cas d'action de droit privé, les organes fédéraux sont soumis aux dispositions applicables aux personnes privées lors du traitement des données correspondantes.

Cependant, même en appliquant l'article 40 LPD, les collectivités publiques qui agissent en vertu du droit privé ne peuvent jamais se soustraire complètement aux principes constitutionnels. Ainsi, le respect des droits fondamentaux et le principe de légalité restent valables.

I. GÉNÉRALITÉS

A. Remarques préliminaires

L'art. 40 LPD reste inchangé par rapport à la version précédente (art. 23, al. 1, aDSG) et n'a subi que de légères modifications rédactionnelles. 1

L'ancien deuxième alinéa, selon lequel la surveillance est régie par les dispositions applicables aux organes fédéraux (art. 23 al. 2 aDSG), a été supprimé sans être remplacé. La raison en est que la version de la LPD commentée ici prévoit de toute façon le même système de surveillance pour les personnes privées et les organes fédéraux. 2

B. But de la norme et contexte

La LPD est conçue comme une loi unique et régit les traitements de données effectués par des personnes privées et par des organes fédéraux dans un seul 3

acte législatif. En tant que partie intégrante de la collectivité, les organes fédéraux sont généralement soumis à des prescriptions juridiques plus strictes, ce qui vaut également pour le traitement de données personnelles et les obligations en matière de protection des données (voir à ce sujet l'art. 5 let. i LPD).

4 L'art. 40 LPD rompt cette dichotomie. Cette disposition prévoit que les organes fédéraux agissant en vertu du droit privé sont soumis aux dispositions moins strictes de la législation sur la protection des données applicables aux particuliers (en particulier le chapitre 5 LPD). Cette réglementation vise à garantir que les organes fédéraux ne soient pas désavantagés par rapport à leurs concurrents privés lorsqu'ils participent à la concurrence économique. Le législateur s'adresse ainsi au fait que les organes fédéraux, en tant que sujets de droit privé, n'exercent pas de souveraineté et qu'il n'existe parfois pas de rapport de subordination par rapport aux particuliers, qu'il faudrait compenser par un habillage juridique plus strict.

5 L'art. 40 LPD est en quelque sorte le pendant de l'art. 5 let. i LPD, selon lequel les particuliers qui assument des tâches publiques sont soumis aux dispositions plus strictes applicables aux organes fédéraux (voir à ce sujet le commentaire de l'art. 5 let. i LPD).

C. Historique

6 Le projet du Conseil fédéral pour la première loi fédérale sur la protection des données de 1988 prévoyait déjà l'assujettissement des activités de droit privé des organes fédéraux aux dispositions applicables aux personnes privées. Ce principe est toujours d'actualité et n'a pas été modifié.

7 Lors des débats parlementaires sur le projet de 1988, le Conseil des États a plaidé pour que les organes fédéraux restent soumis aux dispositions applicables aux organes fédéraux, même lorsqu'ils exercent des activités de droit privé. Ceci sous réserve que le Conseil fédéral se voie accorder la compétence de régler des situations exceptionnelles. Le Conseil des Etats souhaitait que les activités de droit privé des collectivités publiques ne soient pas rendues inutilement attrayantes par des dispositions moins restrictives en matière de protection des données. Il s'agissait également de garantir que les actions de droit privé des organes fédéraux - si elles devaient tout de même se produire exceptionnellement - s'appuient sur une base légale. Après une

procédure d'élimination des divergences avec le Conseil national, qui a soutenu le projet du Conseil fédéral, le Conseil des Etats s'est finalement déclaré d'accord. Il a toutefois posé comme condition que les exigences relatives à la base légale des organes fédéraux agissant en vertu du droit privé soient renforcées.

Dans la version initiale de la LPD 1988, il était stipulé que la surveillance des organes fédéraux ne serait pas non plus assouplie dans le domaine des activités de droit privé. Les mêmes possibilités de surveillance devaient donc être maintenues. Dans la version commentée ici, cette disposition (art. 23 al. 2 aDSG) a toutefois été supprimée sans être remplacée. La raison en est l'uniformisation du régime de surveillance pour les particuliers et les organes fédéraux. 8

II. CHAMP D'APPLICATION

L'art. 40 LPD se rattache à la notion d'organe fédéral. Selon l'art. 5 let. i LPD, sont considérés comme organes fédéraux les autorités et les services de la Confédération ainsi que les particuliers chargés de tâches publiques (voir le commentaire de l'art. 5 let. i LPD pour plus de détails). 9

En principe, les dispositions spécifiques aux organes fédéraux s'appliquent à ces derniers (en particulier le chapitre 6 LPD). Si un organe fédéral agit dans le cadre de l'économie privée, il est toutefois soumis aux dispositions applicables aux personnes privées en vertu de l'article 40 LPD (en particulier le chapitre 5 LPD). 10

III. ACTIONS DE L'ETAT RELEVANT DE LA PUISSANCE PUBLIQUE ET DU DROIT PRIVÉ

A. Catégorisation de l'action étatique

Les conceptions sur la manière dont l'action de l'Etat doit être subdivisée et catégorisée sont aussi variées que les formes d'action de l'Etat elles-mêmes. Dans le contexte de l'art. 40 LPD, la subdivision en "action relevant de la puissance publique" et "action relevant du droit privé" est pertinente, car cette disposition conditionne l'action relevant du droit privé. La paire de termes fonctionne comme une contrepartie et décrit la forme de l'action étatique, et non son objet et son contenu. 11

B. L'action souveraine comme principe

12 En principe, l'État agit en tant que puissance publique dans l'accomplissement de ses tâches. L'action souveraine comprend le pouvoir de fixer unilatéralement les droits et les obligations des personnes privées et s'accompagne d'une supériorité de l'État par rapport aux personnes privées (rapport de subordination). Un exemple d'action souveraine est l'adoption de décisions en contrepartie de la conclusion de contrats de droit privé.

13 L'État agit de manière souveraine, par exemple dans le domaine de l'administration d'intervention. Il s'agit d'une intervention dans les droits et libertés de personnes privées qui doivent la tolérer. Elle sert directement à l'accomplissement de tâches publiques. L'expropriation ou la limitation de la propriété foncière par la police en sont des exemples. L'État agit également en tant que puissance publique dans certains domaines de l'administration des prestations, c'est-à-dire lorsque des prestations étatiques de nature économique et sociale sont fournies à des particuliers (p. ex. la prestation de l'assurance sociale étatique). Elle sert également directement à l'accomplissement de tâches publiques.

C. Action de droit privé

1. Principes de base

14 Il est incontestable que les pouvoirs publics peuvent, dans certaines constellations, agir selon le droit privé. Il convient toutefois de déterminer au cas par cas s'il existe une possibilité d'action de droit privé de la part de l'Etat. Le point de départ est que l'Etat est toujours tenu de respecter le principe de légalité dans ses actions (cf. art. 5 al. 1 Cst.). Il ne dispose donc en principe d'aucune autonomie dans l'organisation de ses relations juridiques. Si un domaine juridique est réglé de manière exhaustive par le droit public, il n'existe donc aucune marge de manœuvre pour une action de droit privé. Celle-ci n'est possible que dans les conditions suivantes :

- Il n'existe pas de réglementation exhaustive de droit public.
- Pour le domaine d'activité concerné, l'action de droit privé est la forme d'action appropriée.

Dans le contexte de l'art. 40 LPD, c'est donc l'action de droit privé d'un organe fédéral qui est déterminante. L'action de droit privé se caractérise, comme nous l'avons décrit, par le fait qu'aucune norme de droit public ne s'applique à une activité, qu'il n'existe pas de rapport de subordination et que l'Etat et les tiers traitent sur un pied d'égalité (p. ex. conclusion d'un contrat de droit privé). En revanche, l'existence d'un rapport de concurrence avec des personnes privées n'est pas nécessaire selon l'article 40 LPD. 15

Dans le domaine du droit de la protection des données, la délimitation entre les actions de droit privé et de droit public se base sur la nature juridique de la relation de base avec la personne concernée. Cette délimitation n'est souvent pas triviale. Le pluralisme des méthodes peut servir d'aide (voir à ce sujet infra n. 18). En outre, certaines constellations de cas se sont formées, dans lesquelles l'Etat agit normalement en vertu du droit privé (voir à ce sujet infra N. 21 ss.). 16

2. Délimitation selon le pluralisme des méthodes

Au sens du principe de légalité, il faut d'abord examiner, pour attribuer au droit public ou au droit privé la relation de base entre la personne concernée et l'organe public, s'il existe une solution de droit spécial pour régler cette question (voir supra n. 14). 17

Si tel n'est pas le cas ou si l'interprétation de la réglementation laisse subsister des doutes, il est possible de recourir aux critères de délimitation développés par la doctrine et la pratique. Selon ce pluralisme méthodologique, les points suivants sont examinés : 18

- Théorie de l'intérêt : le rapport juridique sert-il principalement à la poursuite d'intérêts privés ou publics ?
- Théorie de la subordination : l'institution étatique agissante agit-elle en tant que puissance publique et donc en tant que supérieur par rapport aux particuliers ?
- Théorie fonctionnelle : le rapport juridique a-t-il pour objet l'accomplissement d'une tâche publique ?
- Théorie modale : une violation est-elle sanctionnée par le droit civil ou le droit public ?

19 Selon la pratique, il convient de vérifier séparément pour chaque cas quelle théorie est la plus appropriée pour la délimitation. Selon la jurisprudence de la plus haute juridiction, la théorie fonctionnelle est par exemple considérée comme la plus appropriée pour évaluer la nature juridique des contrats.

3. Les cas d'actes licites de droit privé

20 Dans la pratique, certains domaines d'activité se sont développés, dans lesquels la collectivité publique agit normalement (de manière admissible) en vertu du droit privé.

21 Dans l'activité administrative auxiliaire (également appelée gestion des besoins), la collectivité publique se procure les moyens matériels et humains nécessaires à l'accomplissement direct de tâches publiques. L'activité administrative auxiliaire ne sert qu'indirectement à l'exécution de tâches publiques. Pour la mise en œuvre, la collectivité publique conclut des contrats de droit privé.

22 Tous les actifs réalisables font partie du patrimoine financier de la collectivité publique. Ils ne servent qu'indirectement à la réalisation de la tâche publique et leur gestion relève du droit privé. La location d'immeubles sur le marché libre ou le commerce de titres à des fins de placement en sont des exemples.

23 Si la collectivité publique agit dans le cadre de l'économie privée, elle participe à la vie économique et se trouve dans un rapport de concurrence avec l'économie privée. Dans les relations extérieures, c'est-à-dire en interaction avec la concurrence, la collectivité publique agit selon le droit privé. L'exploitation d'un restaurant communal ou certains domaines d'activité des banques cantonales en sont des exemples.

24 Dans la gestion des prestations, la collectivité publique fournit des prestations économiques à des particuliers. Elle agit selon le droit privé lorsque la fourniture de prestations ne sert qu'indirectement à la poursuite d'intérêts publics, comme dans le cas des contrats de transport public ou des contrats de fourniture d'énergie. En revanche, elle agit en tant que puissance publique lorsqu'elle verse des rentes AI.

IV. CONSÉQUENCES JURIDIQUES

A. Dispositions applicables en matière de protection des données

S'il s'agit d'un domaine d'action de droit privé admissible de l'Etat, les organes fédéraux sont soumis aux dispositions de protection des données applicables aux particuliers (art. 40 LPD). Concrètement, cela signifie qu'en plus des dispositions générales (chapitre 2), les dispositions spéciales pour les personnes privées (chapitre 5) s'appliquent. 25

Les organes fédéraux agissant en vertu du droit privé sont donc liés par des dispositions moins strictes. Cela se caractérise par exemple par l'absence d'application de l'article 34 LPD, qui prescrit l'existence d'une base légale pour le traitement des données par les organes fédéraux. Une autre conséquence est l'applicabilité du mécanisme de l'art. 31 s. LPD, selon lequel certaines atteintes à la personnalité peuvent être corrigées par des motifs justificatifs appropriés (base légale, intérêt prépondérant privé ou public, consentement). 26

Mais même dans le cadre de l'art. 40 LPD, il n'y a pas de découplage total du régime juridique applicable aux organes fédéraux. Certains principes constitutionnels doivent également être respectés par les organes fédéraux agissant en vertu du droit privé (cf. infra N. 31 ss.). 27

B. Procédures

Lorsque l'art. 40 LPD est applicable, les dispositions de droit privé s'appliquent également à l'exercice des droits. Si une personne concernée veut faire valoir ses droits de personne concernée ou d'autres droits par voie d'action en justice contre un organe fédéral agissant selon le droit privé, les dispositions du chapitre 5 de la LPD s'appliquent. 28

En cas de procédure judiciaire, les tribunaux civils sont compétents dans la procédure d'action. La procédure est régie par le code de procédure civile. 29

C. Autre application du droit public

1. Principes constitutionnels

30 Malgré l'application de l'art. 40 LPD, il ne faut pas s'écarter à la légère de l'obligation de respecter les principes constitutionnels (voir art. 5 Cst.). En cas d'action de droit privé des organes fédéraux, il faut toujours vérifier si elle est conforme à ces principes supérieurs.

31 En premier lieu, il convient de tenir compte du principe de légalité (art. 5 al. 1 Cst.). Celui-ci remplit à la fois une fonction démocratique et une fonction d'État de droit. Sous le régime de droit privé de la LPD, la mise en œuvre conforme à la loi du principe de transparence, des obligations d'information ou de la demande de consentement peut, dans certains cas, compenser la fonction de l'Etat de droit. En revanche, la fonction démocratique ne peut pas être remplacée par les obligations mentionnées (voir également l'article 34 du présent commentaire, en particulier la digression sur les consentements).

2. Obligation de respecter les droits fondamentaux

32 Dans le domaine des droits fondamentaux également, il faut s'abstenir de toute assimilation totale à des personnes privées lorsque l'Etat agit en vertu du droit privé, conformément à l'art. 40 LPD. La collectivité publique ainsi que les particuliers qui assument des tâches publiques sont toujours liés aux droits fondamentaux dans leurs actions et doivent contribuer à leur réalisation. Après avoir fait l'objet d'une jurisprudence des plus hautes juridictions, ce principe a été expressément inscrit dans la Constitution fédérale de 1999 à l'art. 35 al. 2 Cst. Ce n'est pas non plus l'action de droit privé ou de souveraineté qui est déterminante pour l'obligation de respecter les droits fondamentaux, mais - plus largement - le fait qu'une tâche publique soit assumée (l'art. 35 al. 2 Cst. parle de "tâche étatique").

3. Théorie des deux niveaux dans la procédure de soumission

33 Pour délimiter les actions relevant du droit privé et celles relevant de la puissance publique, on a parfois recours à la théorie des deux étapes dans la procédure de soumission. Selon cette théorie, l'adjudication (formation de la volonté) se fait par voie de décision et relève donc du droit public, tandis que le contrat avec l'adjudicataire relève du droit privé.

La théorie des deux étapes n'a toutefois pas été reconnue par la jurisprudence de la Cour suprême. De toute façon, le contexte du droit de la protection des données pose également des problèmes de délimitation: L'application de la théorie des deux niveaux signifierait, à la lumière de l'article 40 LPD, que les traitements de données seraient soumis à des régimes juridiques différents jusqu'à l'adjudication et après celle-ci. Une telle séparation stricte des traitements de données présente toutefois des difficultés (techniques) considérables dans la pratique. 34

Dans le sens d'une solution non seulement pragmatique, mais aussi acceptable du point de vue du droit constitutionnel, il faut donc partir du principe que les dispositions plus restrictives en matière de protection des données pour les organes fédéraux s'appliquent globalement aux procédures de soumission. Dans ce domaine également, l'État agissant en vertu du droit privé ne doit pas être mis à la légère et totalement sur un pied d'égalité avec les particuliers. 35

V. CASUISTIQUE

L'arrêt du Tribunal administratif fédéral "SwissPass" illustre de manière exemplaire la procédure décrite ci-dessus pour vérifier l'existence d'un acte relevant de l'économie privée au sens de l'article 40 LPD. Le tribunal devait déterminer si l'émission d'un SwissPass et les traitements de données effectués par les CFF dans ce cadre relevaient du droit public ou du droit privé. 36

Dans ce contexte, c'est tout d'abord la réglementation de la loi spéciale pour le domaine du transport de personnes qui est pertinente, selon laquelle les entreprises de transport - indépendamment de leur forme juridique - sont soumises aux dispositions applicables aux organes fédéraux pour l'activité soumise à concession et à autorisation et à celles applicables aux particuliers en cas d'action de droit privé (art. 54 LTV). Il en résulte que les entreprises de transport peuvent également agir selon le droit privé dans le domaine concédé et qu'elles doivent alors respecter les prescriptions de protection des données pour les personnes privées. 37

Selon le Tribunal administratif fédéral, l'émission du SwissPass ne sert pas directement au transport de personnes soumis à concession, car celui-ci peut être émis même sans prestation de transports publics. Mais comme le SwissPass est un moyen auxiliaire pour la conclusion d'un contrat de transport 38

de personnes, le tribunal a tout de même tenu compte de sa nature juridique. En appliquant le pluralisme des méthodes et en particulier la théorie des fonctions, le tribunal a qualifié le contrat de transport de personnes de droit civil et en a déduit que les CFF étaient soumis aux dispositions de protection des données applicables aux particuliers lors de l'émission du SwissPass.

39 En conclusion, le jugement est correct et l'action de droit privé des CFF semble autorisée et pertinente dans le cas concret. Il convient ensuite d'attirer l'attention sur deux points :

- D'une part, dans ses considérants, le tribunal a également retenu comme critère "l'accomplissement d'une tâche publique", qui n'a pas sa place dans une interprétation stricte de l'art. 40 LPD. D'après son libellé, la norme se base uniquement sur la forme juridique de l'action. Les deux concepts "tâche publique" et "action relevant du droit privé ou de la puissance publique" doivent en principe être séparés.
- Malgré ce principe, nous défendons ici l'idée qu'une simple référence à la nature juridique du rapport de base entre la personne concernée et l'organe public peut conduire à un contournement des normes de droit public supérieures. L'action et, dans le présent contexte, le traitement de données personnelles par des organes fédéraux ne doivent pas être mesurés uniquement en fonction du choix de la forme d'action. L'action doit être placée dans un contexte plus large, celui du droit constitutionnel. Ainsi, l'art. 40 LPD n'est pas non plus applicable s'il ne concerne pas un organe fédéral, entre autres des particuliers qui assument des tâches publiques. L'évaluation du contrat de transport par le Tribunal administratif fédéral sur la base du pluralisme des méthodes et parfois de la théorie des fonctions est donc, selon le présent avis, logique et prévient un contournement des principes de droit public.

BIBLIOGRAPHIE

Bühlmann Lukas/Schüepp Michael, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht, Jusletter 15.3.2021.

Fey Marco, Kommentierung zu Art. 40 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2022 (zit. SHK DSG-Bearbeiterin).

Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich et al. 2020.

Kunz Simon, Kommentierung zu Art. 23 DSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014 (zit. BSK-Bearbeiterin).

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. Rosenthal/Jöhri).

Rudin Beat, Kommentierung zu Art. 2 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2022 (zit. SHK DSG-Bearbeiterin).

Rütsche Bernhard, Was sind öffentliche Aufgaben?, recht 2013, S. 153-162.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz (DSG) und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 S. 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 6.5.2023 (zit. Botschaft 2017).

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988 II S. 413 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/de, besucht am 6.5.2023 (zit. Botschaft 1988).

Sitzung des Ständerats zum Datenschutzgesetz vom 14.3.1990, Amtl. Bull. NR 1990 S. 149 ff. (zit. Amtl. Bull. SR 1990).

Sitzung des Nationalrats zum Datenschutzgesetz vom 10.3.1992, Amtl. Bull. NR 1992 S. 381 ff. (zit. Amtl. Bull. NR 1922).

Sitzung des Ständerats zum Datenschutzgesetz vom 18.3.1992, Amtl. Bull. SR S. 228 ff. (zit. Amtl. Bull. SR 1922).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 41 LPD

Un commentaire de Sarah Bischof

PROPOSITION DE CITATION

Sarah Bischof, Commentaire de l'art. 41 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Bischof, art. 41 LPD N. XXX.

Art. 41 Prétentions et procédure

[1] Quiconque a un intérêt digne de protection peut exiger de l'organe fédéral responsable:

a. qu'il s'abstienne de procéder à un traitement illicite;

b. qu'il supprime les effets d'un traitement illicite;

c. qu'il constate le caractère illicite du traitement.

[2] Le demandeur peut en particulier demander que l'organe fédéral:

a. rectifie les données personnelles, les efface ou les détruise;

b. publie ou communique à des tiers sa décision, concernant notamment la rectification, l'effacement ou la destruction des données,

l'opposition à une communication (art. 37) ou la mention du caractère litigieux des données personnelles (al. 4).

3 Au lieu d'effacer ou de détruire les données personnelles, l'organe fédéral limite le traitement dans les cas suivants:

a. l'exactitude des données est contestée par la personne concernée et leur exactitude ou inexactitude ne peut pas être établie;

b. des intérêts prépondérants d'un tiers l'exigent;

c. un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Suisse, l'exige;

d. l'effacement ou la destruction des données est susceptible de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative.

4 Si l'exactitude ou l'inexactitude d'une donnée personnelle ne peut pas être établie, il ajoute à la donnée la mention de son caractère litigieux.

5 La rectification, l'effacement ou la destruction de données personnelles ne peut pas être exigée pour les fonds gérés par des institutions ouvertes au public telles que les bibliothèques, les établissements d'enseignement, les musées, les archives et les autres institutions patrimoniales publiques. Si le demandeur rend vraisemblable qu'il dispose d'un intérêt prépondérant, il peut exiger que l'institution limite l'accès aux données litigieuses. Les al. 3 et 4 ne s'appliquent pas.

6 La procédure est régie par la PA. Les exceptions prévues aux art. 2 et 3 PA ne sont pas applicables.

TABLE DES MATIÈRES

En bref ... 536
I. Généralités ... 536
A. Remarques préliminaires ... 536
B. Historique ... 537
II. Conditions du droit et de la procédure ... 537
III. Les demandes ... 538
A. Condition de l'illicéité ... 538
B. Droit à l'omission (al. 1 let. a et al. 2 let. a) ... 539
1. Généralités ... 539
2. Rectification et mention de contestation (al. 4) ... 539
C. Droit à l'élimination (al. 1 let. b) ... 541
D. Droit à la constatation (al. 1 let. c) ... 541
E. Limitation du traitement (al. 3) ... 542
IV. Disposition d'exception (al. 5) ... 543
V. Droit de la procédure administrative (al. 6) ... 544
Bibliographie ... 544
Matériaux ... 545

EN BREF

Si une personne estime qu'un organe fédéral viole les dispositions applicables de la LPD lors du traitement de données personnelles, l'art. 41 LPD (conjointement avec le droit d'accès selon l'art. 25 LPD) met à sa disposition les droits nécessaires pour pouvoir imposer un traitement des données conforme à la loi à l'organe fédéral responsable. Elle peut notamment exiger que l'organe fédéral **s'abstienne** de traiter des données de manière illicite, qu'il **élimine** les conséquences d'un traitement illicite ou encore qu'il **constate** le caractère illicite du traitement (art. 41 al. 1 LPD). Cet article prévoit des exceptions, comme notamment la limitation du traitement (art. 41 al. 3 LPD). La décision de l'organe fédéral de ne pas entrer en matière ou d'accorder ou de refuser ces droits prend la forme d'une décision qui peut à son tour, si les conditions nécessaires sont remplies, être contestée selon les règles de la procédure fédérale générale.

I. GÉNÉRALITÉS

A. Remarques préliminaires

1 Le traitement de données personnelles par un organe fédéral constitue une atteinte au droit fondamental de la personne concernée à l'autodétermination en matière d'information, conformément à l'art. 13 al. 2 Cst. et à l'art. 8 CEDH. C'est pourquoi les autorités fédérales ne peuvent traiter des données personnelles que dans un cadre limité et en respectant les principes de traitement énoncés à l'article 6 LPD et en particulier aux articles 34 et suivants LPD. LPD, de traiter des données personnelles. Elles ont notamment besoin d'une base légale pour ce faire.

2 Les traitements de données effectués par un service fédéral constituent en règle générale des actes réels. L'article 41 LPD accorde à la personne concernée (ainsi que, le cas échéant, à des tiers, voir N. 8) une série de droits lui permettant d'exiger que la légalité d'un traitement de données soit rétablie ou que son caractère illicite soit au moins constaté. Au moins dans le cas d'une décision (partiellement) négative, la personne concernée obtient ainsi une décision contestable.

Il convient de distinguer la protection juridique individuelle de l'art. 41 LPD, qui ne s'applique qu'en cas de revendication active de la personne concernée, des droits de contrôle du Préposé fédéral à la protection des données et à la transparence (cf. les explications relatives aux art. 49 ss LPD). Dans le cadre de ses compétences en matière de surveillance, le PFPDT est habilité à mener des enquêtes d'office et à rendre des décisions, ce qui permet de protéger également les personnes qui ne peuvent ou ne veulent pas intenter une action en justice contre un organe fédéral fautif (p. ex. parce qu'elles n'ont pas connaissance de l'illicéité ou du traitement des données en soi). 3

B. Historique

Selon le message du Conseil fédéral relatif à la LPD initiale de 1992, le système juridique proposé devait d'une part s'inspirer des actions de droit privé de l'art. 28a CC, mais d'autre part s'intégrer dans le droit de procédure administrative alors en vigueur. Par la suite, les Chambres n'ont pas remis en question le principe de ce concept proposé par le Conseil fédéral et n'ont apporté que quelques modifications. 4

La disposition a subi quelques modifications suite à la révision qui est entrée en vigueur le 1er septembre 2023. Un droit explicite à l'effacement ainsi qu'une limitation du traitement ont notamment été ajoutés. Ces modifications et compléments proposés par le Conseil fédéral ont été adoptés sans difficulté par les Chambres. 5

II. CONDITIONS DU DROIT ET DE LA PROCÉDURE

Le destinataire du droit est l'**organe fédéral** responsable qui traite ou fait traiter les données dans le cadre de l'exécution de son mandat légal. Sont considérés comme organes fédéraux non seulement les autorités fédérales, mais aussi les particuliers qui accomplissent des tâches de droit public de la Confédération (voir explications relatives à l'art. 5 let. i LPD). Ainsi, les prétentions découlant d'un traitement illicite de données à l'encontre d'une caisse de pension, qui est certes organisée en tant que fondation de droit privé, mais qui offre la prévoyance professionnelle obligatoire conformément à la LPP et qui est donc considérée comme un organe fédéral, doivent être formulées conformément à l'art. 41 LPD (et non à l'art. 32 LPD). 6

7 Il convient de noter que le fait de faire valoir un droit à l'encontre d'un organe fédéral n'a pas d'effet contraignant pour les autres organes fédéraux (voir n. 21 concernant la communication à des tiers ou la publication) ; le cas échéant, il faut donc les faire valoir individuellement à l'encontre de chaque organe fédéral responsable qui traite des données.

8 Toute personne disposant d'un **intérêt digne de protection** peut faire valoir son droit. L'existence d'un tel intérêt s'apprécie selon les principes généraux de la procédure administrative. L'intérêt digne de protection ne se limite pas non plus aux intérêts relevant du droit de la personnalité et ne doit en outre pas coïncider avec l'intérêt protégé par la norme violée. Il est uniquement nécessaire que le requérant ait un intérêt actuel, juridique ou factuel, dans l'issue de la procédure qu'il a engagée et que celle-ci puisse lui apporter un avantage pratique direct. Il doit avoir un rapport particulier avec l'objet du litige et être ainsi plus concerné que le grand public.

9 Dans le cas de la personne concernée, un intérêt digne de protection sera généralement donné. Des exceptions sont toutefois possibles, par exemple lorsque l'organe fédéral ne traite plus du tout les données, ce qui rendrait la demande sans objet. Dans quelques rares cas de figure, il est également envisageable que des tiers dont les données ne sont pas du tout traitées puissent faire valoir un intérêt digne de protection. Mais cela n'est généralement le cas que si ce tiers est un proche parent ou un ami de la personne concernée (décédée) et qu'il peut se prévaloir de la protection de la mémoire reconnue par le Tribunal fédéral.

III. LES DEMANDES

A. Condition de l'illicéité

10 Conformément à l'article 41 al. 1 LPD, le requérant peut demander la **cessation** d'un traitement illicite de données, l'**élimination des conséquences** d'un traitement illicite de données ou la **constatation** du caractère illicite d'un traitement de données.

11 Ces droits ont en commun le fait qu'ils présupposent le **caractère illicite** du traitement des données. Ceci contrairement à l'opposition à la communication de données personnelles selon l'art. 37 LPD ; dans ce cas, seul l'intérêt digne de protection de la personne concernée est déterminant, mais

pas le caractère illicite de la communication (voir le commentaire de l'art. 37 LPD).

L'illicéité peut notamment résider dans le fait que l'organe fédéral ne dispose **pas d'une base légale suffisante** pour le traitement de données en question. Par exemple, le Tribunal administratif fédéral a décidé qu'une caisse de pension qui envoie les certificats de prévoyance directement à l'employeur sans les fermer agit de manière illicite, car une telle communication n'est pas nécessaire à l'exécution de la prévoyance professionnelle selon la LPP et qu'aucune autre base légale (en particulier l'art. 86a LPP qui règle la communication des données dans le cadre de la LPP) ne le légitimerait. En outre, le **traitement de données inexactes** est également illicite dans la mesure où l'organe fédéral responsable ne remplit pas son obligation de vérification à cet égard (cf. commentaire de l'art. 6 al. 5 LPD). 12

B. Droit à l'omission (al. 1 let. a et al. 2 let. a)

1. Généralités

Le droit à l'omission présuppose qu'au moment où l'on fait valoir ce droit, il y a **de sérieuses raisons de craindre** que l'organe fédéral responsable procède à un traitement illicite de données déterminé dans un avenir proche. Une telle crainte sérieuse peut exister, d'une part, lorsque l'organe fédéral effectue déjà le traitement des données et que celui-ci se poursuit ou, d'autre part, lorsque des indices concrets permettent de conclure que les données seront traitées de manière illicite dans un avenir proche. Selon la jurisprudence du Tribunal fédéral, ce n'est qu'à ce moment-là que l'on peut admettre l'intérêt actuel de la protection juridique à l'omission. 13

Si ces conditions sont remplies, la personne concernée ne peut pas seulement exiger que l'organe fédéral renonce à un traitement illicite des données. Elle peut également demander le **rétablissement de la légalité**, notamment en exigeant la rectification, l'effacement ou la destruction des données concernées sur la base de l'art. 41 al. 2 let. a LPD. 14

2. Rectification et mention de contestation (al. 4)

Le traitement de données personnelles inexactes n'est illicite que si l'inexactitude résulte d'une **violation de l'obligation de vérifier les** données conformément à l'art. 6 al. 5 LPD. Un organe fédéral traitant des données doit 15

donc s'assurer d'office de l'exactitude des données dès leur collecte ou pendant la durée du traitement en prenant des mesures appropriées (cf. commentaire de l'art. 6 al. 5 LPD). Même s'il le fait, le traitement des données devient illicite au moins à partir du moment où la personne concernée s'adresse à l'organe fédéral avec un droit de rectification et que celui-ci omet de clarifier à nouveau de manière suffisante l'exactitude ou l'inexactitude.

16 Si l'exactitude ou l'inexactitude des données ne peut pas être établie ou ne peut pas être établie facilement malgré la demande de rectification motivée de la personne concernée, l'organe fédéral doit restreindre le traitement conformément à l'art. 41 al. 3 LPD pendant la durée des clarifications nécessaires (voir ci-dessous let. E). Cela signifie que pendant cette durée, l'organe fédéral ne peut plus traiter les données que pour constater leur exactitude ou leur inexactitude.

17 Si l'organe fédéral n'est pas en mesure de prouver l'exactitude des données traitées, le cas échéant malgré des investigations supplémentaires, mais que la personne concernée n'est pas non plus en mesure de prouver en retour l'exactitude des rectifications qu'elle a demandées, l'organe fédéral doit apposer une **mention de contestation**. Cela permet d'une part de satisfaire les intérêts de la personne concernée en démontrant qu'elle n'est pas d'accord avec la présentation des faits par l'organe fédéral. D'autre part, elle garantit que l'organe fédéral ne doit pas renoncer à des traitements de données dont il a besoin pour remplir son mandat légal.

18 Le matériel législatif relatif à la nouvelle restriction introduite par la révision 2023 ne s'exprime pas sur le rapport entre l'art. 41 al. 3 et al. 4 LPD. Toutefois, comme expliqué, la mention de contestation a notamment pour but de permettre à l'organe fédéral de continuer à accomplir ses tâches légales. Si l'examen de l'exactitude ou de l'inexactitude des données n'aboutit pas, l'organe fédéral doit pouvoir lever une limitation du traitement au sens de l'art. 41, al. 3, LPD, apposer une mention de contestation et traiter à nouveau l'intégralité des données en question, du moins dans la mesure où il n'est pas possible de renoncer totalement au traitement et où aucun autre motif de limitation (cf. let. E) ne s'applique.

C. Droit à l'élimination (al. 1 let. b)

La personne concernée a en outre le droit d'obtenir **l'élimination des conséquences** d'un traitement illicite de données au moyen de mesures appropriées et proportionnées. Il s'agit ici de l'élimination réelle des conséquences négatives dues à un traitement illicite des données, par exemple l'octroi ultérieur de prestations légales. Si une assurance-maladie dans le domaine de l'assurance obligatoire des soins (AOS) devait déterminer l'état de santé général d'un assuré au moyen d'un questionnaire de santé et, sur cette base, ne pas lui proposer certaines prestations AOS, la base légale ferait défaut (et serait en contradiction avec l'obligation d'admission de la LAMal) ; la collecte de données serait illicite et l'assurance-maladie devrait accorder à l'assuré les prestations prévues par la loi sur l'assurance-maladie. 19

Le droit ne permet toutefois pas aux personnes concernées d'annuler des décisions formellement exécutoires. Cela n'est toujours possible qu'avec les motifs de révision prévus par la loi conformément à l'art. 66 PA. Il n'est pas non plus possible pour les personnes concernées de demander des dommages-intérêts ou une réparation du tort moral sur la base de l'art. 41 al. 1 let. b LPD, car ces droits doivent être exercés par le biais de la loi fédérale sur la responsabilité. 20

Dans la pratique, le droit à la suppression jouera régulièrement un rôle en cas de communication illicite de données. Dans ce cas, la personne concernée peut notamment exiger la publication de la décision concernant le traitement illicite des données (notamment la rectification, l'effacement ou la destruction, la mention de contestation mais aussi l'opposition à la communication selon l'art. 37 LPD) ou sa communication aux éventuels destinataires des données (art. 41 al. 2 let. b LPD). Cela a pour but de permettre à un destinataire de données de reprendre volontairement la décision et d'effacer ou de rectifier les données ; il ne peut toutefois pas y être contraint. Dans ce cas, la personne concernée n'a d'autre choix que de faire valoir ses droits éventuels auprès du destinataire des données. 21

D. Droit à la constatation (al. 1 let. c)

Le requérant peut en outre demander la **constatation du caractère illicite** du traitement des données. Ce droit n'**est** que **subsidiaire** par rapport au droit à l'omission et à la suppression. Tant qu'il est possible d'exiger la 22

cessation du traitement illicite ou l'élimination des conséquences qui en découlent, il n'existe pas d'intérêt digne de protection à la constatation du caractère illicite.

23 Selon la jurisprudence du Tribunal fédéral, un intérêt à la constatation est donné lorsqu'un traitement illicite (passé) de données ou l'atteinte à la personnalité qui y est liée continue à avoir des effets perturbateurs et que la constatation de l'illicéité est de nature à éliminer ces effets persistants.

E. Limitation du traitement (al. 3)

24 L'art. 41 al. 3 LPD a été ajouté lors de la révision de 2023. Selon celui-ci, l'organe fédéral doit, au lieu d'effacer ou de détruire les données, limiter le traitement si l'un des cas suivants se présente :

- La personne concernée conteste l'exactitude des données personnelles, mais ni l'exactitude ni l'inexactitude ne peuvent être établies (voir ci-dessus N. 18) ;
- Des intérêts prépondérants de tiers ou des intérêts publics prépondérants exigent que les données continuent d'exister ;
- L'effacement ou la destruction des données compromettrait une enquête, une investigation ou une procédure administrative ou judiciaire.

25 Il convient de noter que l'article 18 du RGPD prévoit également la "limitation du traitement". Contrairement à la disposition du RGPD, où il s'agit d'un droit de la personne concernée à l'égard du responsable du traitement, l'art. 41 al. 3 LPD est conçu comme une exception à l'effacement/la destruction ou également à la rectification. Lors du traitement d'une demande d'effacement/de destruction, mais aussi de rectification (bien qu'elle ne soit pas explicitement mentionnée, la limitation du traitement pour vérifier l'exactitude ou l'inexactitude des données a un sens du point de vue de la logique légale), l'organe fédéral doit vérifier d'office si l'un des motifs de limitation existe. Si la demande est acceptée et que la limitation est confirmée, l'organe fédéral doit réduire le traitement à la finalité qui s'oppose à l'effacement/la destruction ou à la rectification.

26 La décision relative à la limitation doit être rendue sous forme de décision ou de décision incidente si elle ne met pas fin à la procédure.

Le message prévoit que la limitation doit être mise en œuvre de manière à ce que les données contestées soient clairement identifiées, ce qui peut signifier dans la pratique qu'elles soient temporairement déplacées vers un autre système de traitement ou que les droits d'accès soient limités. Dans cette argumentation, le législateur n'a pas tenu compte du fait que cela entraînera régulièrement des problèmes de mise en œuvre dans la pratique, car on ne peut pas partir du principe que tous les systèmes permettent de prendre de telles dispositions pour des données individuelles, c'est-à-dire pour ainsi dire "sur le terrain", et qu'ils ne peuvent pas non plus les mettre en œuvre sans autre. Si les possibilités techniques de mise en œuvre font défaut, la restriction doit au moins être garantie par des mesures organisationnelles, par exemple au moyen d'indications dans le système, de directives ou de listes séparées. 27

IV. DISPOSITION D'EXCEPTION (AL. 5)

La rectification, l'effacement ou la destruction de données personnelles ne peut pas être exigée en ce qui concerne les fonds de ce que l'on appelle les lieux de mémoire publics, comme notamment les bibliothèques accessibles au public, les établissements d'enseignement, les musées ou les archives. Dans ces cas, il n'est pas non plus possible d'obtenir une note de contestation. Le but de ces institutions est de reproduire un moment du passé, ce qui ne peut être atteint que si les fonds sont fidèles à l'original et inchangés. 28

La personne concernée peut tout de même exiger que l'accès aux données controversées soit limité. En principe, l'intérêt public à un accès libre et non faussé aux documents prévaut. Toutefois, il faut admettre un intérêt prépondérant de la personne concernée à la limitation de l'accès si elle subirait des inconvénients personnels considérables en raison d'un accès libre, par exemple parce qu'elle serait limitée dans son avancement professionnel et que la valeur archivistique des données en question apparaît en revanche comme moindre. Selon le message, cette exception doit être prise en compte en particulier dans la perspective de la publication croissante de documents d'archives sur Internet. 29

V. DROIT DE LA PROCÉDURE ADMINISTRATIVE (AL. 6)

30 La procédure pour faire valoir les droits de l'art. 41 al. 1-2 LPD est régie par la PA. Ceci même si la PA ne s'applique pas du tout au domaine concerné (les exceptions des articles 2 et 3 de la PA ne s'appliquent pas).

31 Cela signifie notamment que l'organe fédéral doit établir les faits d'office (principe de l'instruction, art. 12 PA). Le requérant est toutefois soumis à une obligation de collaborer (art. 13 PA) ; par exemple, dans le cadre d'une demande de rectification, il doit présenter des moyens de preuve qui démontrent l'exactitude des modifications qu'il demande.

32 L'organe fédéral peut également décider de ne pas entrer en matière, d'approuver ou de rejeter la demande. La décision est rendue sous la forme d'une décision qui peut à son tour faire l'objet d'un recours devant le Tribunal administratif fédéral.

BIBLIOGRAPHIE

Bangert Jan, Kommentierung zu Art. 25/25bis DSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Basler Kommentar, Datenschutzgesetz, 3. Aufl., Basel, 2014.

Burkert Herbert, Datenschutz und Rechtsschutz, in: Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht, ZBl 108 (2007), S. 374-379.

Fanger Reto, Kommentierung zu Art. 41 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), OFK-Orell Füssli Kommentar (Navigator.ch), Zürich 2023.

Gautschi Adrian, Kommentierung zu Art. 42 DSG, in: Blechta, Gabor-Paul/Vasella David (Hrsg.), Balser Kommentar, Datenschutzgesetz, 4. Aufl. Basel 2024.

Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich/St. Gallen 2020.

Häner Isabelle, Kommentierung zu Art. 25 und 25a VwVG, in: Waldmann Bernhard/Weissenberger Philippe (Hrsg.), Praxiskommentar Verwaltungsverfahrensgesetz, 2. Aufl., Zürich 2016.

Jöhri Yvonne, Kommentierung zu Art. 25 DSG, in: Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008.

Sturny Monique, Kommentierung zu Art. 41, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika, Stämpflis Handkommentar (SHK) zum Datenschutzgesetz, 2. Aufl., Zürich 2023.

MATÉRIAUX

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988 (BBl 1988 413).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017 (BBl 2017 6941).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 42 LPD

Un commentaire de Sarah Bischof

PROPOSITION DE CITATION

Sarah Bischof, Commentaire de l'art. 42 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Bischof, art. 42 LPD N. XXX.

Art. 42 Procédure en cas de communication de documents officiels contenant des données personnelles

Tant que l'accès à des documents officiels contenant des données personnelles fait l'objet d'une procédure au sens de la loi du 17 décembre 2004 sur la transparence, la personne concernée peut, dans le cadre de cette procédure, faire valoir les droits que lui confère l'art. 41 de la présente loi concernant les documents qui sont l'objet de la procédure d'accès.

TABLE DES MATIÈRES

En bref 549
I. Remarques préliminaires 549
II. Exercice des droits selon l'art. 41 LPD dans la procédure d'accès 549
Bibliographie 550
Matériaux 551

EN BREF

Selon l'art. 42 LPD, les droits découlant de l'art. 41 LPD peuvent être invoqués dans le cadre d'une procédure d'accès selon la loi sur la transparence, pour autant que les documents concernés contiennent des données personnelles. Cette disposition tient ainsi compte du fait que les objectifs de protection de la LPD et de la LTrans, notamment l'autodétermination en matière d'information en tant qu'élément de la protection de la sphère privée d'une part, et le principe de transparence de l'administration d'autre part, peuvent entrer en conflit.

I. REMARQUES PRÉLIMINAIRES

L'ancien art. 25bis aDSG a été introduit lors de l'entrée en vigueur de la loi fédérale sur la transparence de l'administration (loi sur la transparence, LTrans). Les principes de coordination entre la LPD et la LTrans ont ainsi été fixés. Dans la version révisée de la LPD de 2023, le contenu de la disposition n'a pas été modifié ; elle se trouve désormais à l'art. 42 LPD. 1

La disposition garantit qu'une personne concernée puisse faire valoir ses droits en matière de protection des données dans le cadre de la procédure d'accès prévue par la loi sur la transparence. Cela a pour conséquence d'élargir la procédure d'accès à ces intérêts liés à la protection des données. 2

II. EXERCICE DES DROITS SELON L'ART. 41 LPD DANS LA PROCÉDURE D'ACCÈS

La LTrans prévoit que toute personne a le droit de consulter des documents officiels et d'obtenir des autorités des renseignements sur le contenu des documents officiels (**principe de transparence**, art. 6, al. 1, LTrans). L'accès peut toutefois être limité, différé ou refusé si son octroi est susceptible de porter atteinte à la sphère privée de tiers ; à condition que l'intérêt public à l'accès ne soit pas prépondérant (art. 7, al. 2 LTrans). 3

Pour que la sphère privée de tiers soit préservée dans la procédure d'accès, les documents officiels contenant des données personnelles doivent en principe **être rendus anonymes** (art. 9 LTrans). Si l'anonymisation n'est toutefois pas possible, par exemple parce qu'elle rendrait incompréhensible le 4

contenu et le contexte du document officiel ou parce qu'elle impliquerait un travail disproportionné (ce qui implique une pesée complète des intérêts par l'organe fédéral), l'accès n'est autorisé qu'à la condition de l'art. 36 LPD, qui règle la communication de données par les organes fédéraux (voir le commentaire à ce sujet). Si l'autorité envisage d'accorder l'accès, elle doit préalablement donner à la personne concernée, dont les données personnelles figurent dans les documents en question et dont la sphère privée peut s'en trouver affectée, **la possibilité de prendre position** dans un délai de 10 jours. Dans le cadre de cette prise de position, la personne concernée ne peut pas seulement demander que ses données ne soient pas communiquées au demandeur. L'article 42 LPD lui permet au contraire de faire valoir son droit à la **cessation** d'un traitement illicite de données, à l'**élimination** des conséquences d'un traitement illicite de données ou à la **constatation** du caractère illicite d'un traitement de données (voir commentaire de l'article 41 LPD). Les prétentions doivent porter sur les documents qui font l'objet de la procédure d'accès.

5 Si l'autorité souhaite accorder l'accès contrairement à l'avis de la personne concernée, elle doit en informer cette dernière (art. 11 al. 2 LTrans). Celle-ci peut alors demander au PFPDT de **procéder à une médiation** dans un délai de 20 jours. Si la médiation échoue, le PFPDT émet une recommandation. L'autorité doit ensuite rendre une décision, soit si elle ne suit pas la recommandation, soit si la personne concernée (ou même le demandeur) en fait la demande (art. 15 al. 1 et al. 2, let. b LTrans). Cette décision peut faire l'objet d'un recours auprès du Tribunal administratif fédéral (art. 16 al. 1 LTrans).

6 L'art. 42 LPD vise ainsi notamment à garantir l'économie de la procédure, étant donné que la personne concernée ne prend éventuellement connaissance du fait que ses données personnelles figurent dans les documents officiels en question que lorsqu'elle est invitée à prendre position. Il peut donc être judicieux que les aspects liés à la protection des données soient également évalués dans le cadre de la procédure d'accès. Cette solution est critiquée parce qu'elle rend la procédure d'accès lourde et fastidieuse.

BIBLIOGRAPHIE

Egli Patricia, Datenschutz und Öffentlichkeitsprinzip, in: Forum Europarecht Band/Nr. 35, Jahr 2015, S. 133-155.

Gautschi Adrian, Kommentierung zu Art. 42 DSG, in: Blechta, Gabor-Paul/Vasella David (Hrsg.), Balser Kommentar, Datenschutzgesetz, 4. Aufl. Basel 2024.

Jöhri Yvonne, Kommentierung zu Art. 25bis DSG, in: Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008.

Kölz Alfred/Häner Isabell/Bertschi Martin, Verwaltungsverfahren und Verwaltungsrechtspflege des Bundes, 3. Aufl., Zürich 2013.

Stoffel Martine/Poncet Marie, Kommentierung zu Art. 41 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), OFK-Orell Füssli Kommentar (Navigator.ch), Zürich 2023.

Sturny Monique, Kommentierung zu Art. 42, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar (SHK) zum Datenschutzgesetz, 2. Aufl., Zürich 2023.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Öffentlichkeit der Verwaltung vom 12.2.2003 (BBl 2003 1963).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017 (BBl 2017 6941).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 43 LPD

Un commentaire de Carl Jauslin / Danielle Schneider

PROPOSITION DE CITATION

Carl Jauslin/Danielle Schneider, Kommentierung zu Art. 43 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Jauslin/Schneider, N. XXX zu Art. 43 DSG.

Chapitre 7
Préposé fédéral à la protection des données personnelles et à la transparence

Section 1 Organisation

Art. 43 Élection et statut

[1] L'Assemblée fédérale (Chambres réunies) élit le chef du PFPDT (le préposé).

[2] Quiconque a le droit de vote en matière fédérale est éligible.

[3] Pour autant que la présente loi n'en dispose pas autrement, les rapports de travail du préposé sont régis par la loi du 24 mars 2000 sur le personnel de la Confédération (LPers)[13]. Le préposé est assuré jusqu'à l'âge de 65 ans révolus auprès de la caisse de pensions PUBLICA contre

les conséquences économiques de la vieillesse, de l'invalidité et du décès. Sur demande du préposé, la prévoyance vieillesse est maintenue au-delà de l'âge de 65 ans jusqu'à la cessation des rapports de travail mais, au plus tard, jusqu'à la fin de l'année au cours de laquelle le préposé atteint l'âge de 68 ans. Dans ce cas, le PFPDT finance les cotisations d'épargne de l'employeur.[14]

[3bis] L'Assemblée fédérale édicte par voie d'ordonnance les dispositions d'exécution relatives aux rapports de travail du préposé.[15]

[4] Le préposé exerce ses fonctions de manière indépendante et sans recevoir ni solliciter d'instructions de la part d'une autorité ou d'un tiers. Il est rattaché administrativement à la Chancellerie fédérale.

[5] Il dispose d'un secrétariat permanent et de son propre budget. Il engage son personnel.

[6] Il n'est pas soumis au système d'évaluation prévu à l'art. 4, al. 3, LPers.

TABLE DES MATIÈRES

En bref 556
I. Généralités 556
II. Organe d'élection (al. 1) 559
III. Éligibilité (al. 2) 559
IV. Rapport de travail (al. 3) 560
V. Dispositions d'exécution relatives aux rapports de travail (al. 3bis) 561
VI. Indépendance et attribution (al. 4) 563
VII. Secrétariat, budget et personnel (al. 5) 564
VIII. Évaluation (al. 6) 565
Bibliographie 567
Matériaux 567

EN BREF

Le choix et le statut du responsable du PFPDT (le préposé) sont déterminants pour l'indépendance et la légitimité de l'activité de surveillance. Le préposé est élu par l'Assemblée fédérale (Chambres réunies) et exerce sa fonction en toute indépendance : Le ou la préposé(e) n'accepte pas d'instructions, n'est pas soumis(e) au système d'évaluation prévu par la LPers et n'est rattaché(e) à la Chancellerie fédérale que sur le plan administratif. Il ou elle dispose d'un secrétariat permanent et de son propre budget.

L'élection et la révocation du préposé relèvent de la compétence de l'Assemblée fédérale (Chambres réunies). Les autres décisions de l'employeur à l'égard du préposé relèvent de la compétence de la commission judiciaire. Le droit du personnel de la Confédération ne s'applique aux rapports de travail du préposé que dans la mesure où la LPD et ses dispositions d'exécution n'en disposent pas autrement.

I. GÉNÉRALITÉS

1 L'art. 43 règle la nomination et le statut du responsable du PFPDT chargé de surveiller l'application des prescriptions fédérales en matière de protection des données (art. 4, al. 1, LPD).

2 D'un point de vue terminologique, il convient de distinguer le préposé en tant que personne du PFPDT en tant qu'autorité : Lorsqu'il s'agit de la personne du chef du Préposé fédéral à la protection des données et à la transparence, on parle du "préposé" ; par contre, lorsqu'il s'agit de l'autorité du Préposé fédéral à la protection des données et à la transparence au sens institutionnel, on utilise l'abréviation "PFPDT". L'institution PFPDT comprend, outre le préposé, également le secrétariat.

3 Alors que, selon l'ancien droit, le préposé était nommé par le Conseil fédéral et que sa nomination devait être approuvée par l'Assemblée fédérale (Chambres réunies) (art. 26, al. 1, aDSG), le droit en vigueur prévoit que l'Assemblée fédérale (Chambres réunies) est compétente pour nommer le préposé (art. 43, al. 1, LPD). L'élection par l'Assemblée fédérale (Chambres réunies) vise à renforcer l'indépendance du préposé et sa légitimité démocratique.

La garantie de l'indépendance du préposé en tant que personne et du PFPDT en tant qu'autorité est au cœur de cette disposition sur l'élection et le statut. La notion d'indépendance comprend l'indépendance institutionnelle, l'indépendance fonctionnelle et l'indépendance matérielle. 4

- L'indépendance institutionnelle signifie que le PFPDT n'est pas subordonné à une autre autorité sur le plan organisationnel. Cela n'exclut toutefois pas un rattachement administratif, comme dans le cas du PFPDT à la Chancellerie fédérale (ChF) (voir art. 43, al. 4, deuxième phrase, LPD).
- L'indépendance fonctionnelle exige que le PFPDT exerce ses tâches et ses compétences en toute indépendance, sans recevoir d'instructions de quelque autorité que ce soit (voir art. 43, al. 4, première phrase, LPD) et que le préposé ne soit pas soumis à un système d'évaluation au sens de l'art. 4, al. 3, LPers (voir art. 43, al. 6, LPD). L'indépendance fonctionnelle du PFPDT est en outre garantie par le fait que le préposé est engagé à 100% (art. 8 de l'ordonnance sur les rapports de travail du préposé), que les activités accessoires ne sont possibles que de manière très limitée (art. 46 et 47 LPD) et que le préposé ne peut être relevé de ses fonctions que dans des cas exceptionnels à traiter de manière très restrictive (art. 44 al. 3 LPD).
- L'indépendance matérielle exige que les conditions et le cadre soient créés pour que le PFPDT puisse exercer ses tâches et ses compétences de manière indépendante, c'est-à-dire qu'il ait la possibilité, non seulement sur le papier, mais aussi dans les faits, d'accomplir son mandat légal en toute indépendance. Cette indépendance matérielle implique notamment que le PFPDT dispose d'un secrétariat et d'un budget permanents et qu'il puisse engager son personnel de manière autonome (voir art. 43 al. 5 LPD).

La révision de cette disposition relative à la nomination, au statut et aux rapports de travail du préposé s'est déroulée en trois étapes : 5

- Dans un premier temps, le Parlement a renforcé l'indépendance du PFPDT en adoptant la loi fédérale du 28 septembre 2018 sur la mise en œuvre de la directive européenne 2016/680, qui fait partie du développement de l'acquis de Schengen.
- Dans un deuxième temps, le Parlement a encore renforcé l'indépendance du PFPDT dans le cadre de la révision totale de la loi sur la protection des données du 25 septembre 2020, en précisant que le préposé serait

désormais élu par l'Assemblée fédérale (Chambres réunies). La modification de l'organe d'élection n'a été introduite qu'au cours des débats parlementaires, contrairement à l'avis du Conseil fédéral qui s'en tenait à la solution précédente. L'initiative parlementaire Leutenegger Oberholzer 16.409 demandait déjà que le préposé soit élu par l'Assemblée fédérale (Chambres réunies). Lors des débats parlementaires, le renforcement de l'indépendance et de la position du PFPDT ainsi qu'une légitimité démocratique accrue ont été invoqués pour argumenter en faveur d'une modification de la procédure d'élection en faveur de l'Assemblée fédérale réunie. Le Conseil fédéral et les défenseurs de la solution actuelle craignaient une politisation de l'élection, qui pourrait être influencée par différents groupes d'intérêts au sein du Parlement, et ont souligné que même selon la solution actuelle, l'Assemblée fédérale réunie devait approuver l'élection par le Conseil fédéral et était donc impliquée.

- Dans un troisième temps, certains aspects des rapports de travail ont été précisés au niveau de la loi et l'Assemblée fédérale a reçu la compétence d'édicter des dispositions d'exécution sur les rapports de travail du préposé (initiative parlementaire CIP-N 21.443). Les modifications de la LPD totalement révisée accompagnant l'initiative parlementaire CIP-N 21.443 ainsi que les nouvelles dispositions d'exécution créées ont été adoptées le 17 juin 2022 et entreront en vigueur en même temps que la révision totale de la LPD (1.9.2023). Elles ont eu pour effet que l'indépendance du préposé se reflète également dans les rapports de travail.

6 L'art. 43 al. 4 et 5 LPD reste inchangé par rapport à l'ancien droit (art. 26 al. 4 et 5 LPD), l'art. 43 al. 5 LPD ayant été complété par l'art. 45 LPD relatif au processus budgétaire. L'art. 43 al. 3, première phrase, correspond à l'art. 26 al. 2 LPD et a été complété par trois phrases relatives à la caisse de pension du préposé.

7 L'art. 43 LPD respecte les prescriptions du droit européen à l'art. 15 de la Convention 108+ modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel, aux art. 41 ss de la directive UE 2016/680 relative à Schengen ainsi qu'à la norme prévue aux art. 51 ss du règlement UE sur la protection des données 2016/679 pour une surveillance efficace de la protection des données en relation avec la décision d'adéquation de la Commission européenne (art. 45, al. 2, let. b du règlement UE sur la protection des données).

II. ORGANE D'ÉLECTION (AL. 1)

L'Assemblée fédérale (Chambres réunies) élit le préposé. La Commission judiciaire est compétente pour la mise au concours du poste et la préparation de l'élection (art. 40a al. 1 let. d et al. 2 première phrase LParl ; cf. également art. 2 de l'ordonnance sur les rapports de travail du préposé). Le suppléant du préposé ne tombe pas sous le coup de cette disposition et n'est pas élu par le Parlement. Les dispositions générales du droit du personnel fédéral s'appliquent au suppléant. 8

L'art. 43 al. 1 LPD se fonde sur l'art. 168 al. 2 Cst. selon lequel une loi peut habiliter l'Assemblée fédérale à élire d'autres personnes que celles visées à l'art. 168 al. 1 Cst. (les membres du Conseil fédéral, le chancelier ou la chancelière de la Confédération, les juges du Tribunal fédéral et le général). Le procureur général de la Confédération et les procureurs généraux suppléants ainsi que les membres de l'autorité de surveillance du Ministère public de la Confédération en sont des exemples (voir art. 20 et 23 LOAP). 9

Le droit européen ne prescrit pas la procédure d'élection des membres de l'autorité de protection des données (cf. art. 43 al. 1 de la directive (UE) 2016/680 ; de même art. 53 al. 1 du règlement (UE) 2016/679). Conformément à ces actes, il appartient aux États membres de veiller à ce que la nomination se déroule selon une procédure transparente et de prévoir une nomination par le parlement, le gouvernement, le chef d'État ou une autorité indépendante chargée de cette tâche conformément au droit de l'État membre. 10

III. ÉLIGIBILITÉ (AL. 2)

Conformément à l'al. 2, sont éligibles comme préposés les personnes ayant le droit de vote en matière fédérale. Conformément à l'art. 136 al. 1 Cst., ont le droit de vote en matière fédérale tous les Suisses et Suissesses âgés de 18 ans révolus qui ne sont pas interdits pour cause de maladie mentale ou de faiblesse d'esprit. La nationalité suisse, en particulier, est donc requise pour la fonction de préposé. 11

Cette disposition relative à l'éligibilité, qui se fonde sur la qualité d'électeur, se retrouve par analogie dans d'autres lois fédérales. Elle correspond par exemple à l'art. 20 al. 1bis LOAP pour l'élection du procureur général de la 12

Confédération et des procureurs généraux suppléants ou à l'art. 5 al. 2 LTAF pour l'élection des juges du Tribunal administratif fédéral.

13 Les exigences en matière d'aptitude matérielle et personnelle du préposé ne sont pas expressément fixées dans la LPD. Elles découlent toutefois du droit du personnel de la Confédération qui, selon l'art. 43 al. 3 LPD, reste applicable à titre subsidiaire au préposé, notamment de l'obligation de mettre le poste au concours public (cf. art. 7 LPers en relation avec l'art. 22 OPers). Ainsi, le préposé doit être un spécialiste avéré dans le domaine de la LPD comme de la LTrans et disposer d'une intégrité personnelle. Les aptitudes professionnelles et personnelles ne constituent toutefois pas une condition d'éligibilité, mais relèvent plutôt de la responsabilité de l'autorité électorale. La commission judiciaire responsable de la préparation de l'élection du préposé doit tenir compte des aptitudes professionnelles et personnelles dès la mise au concours du poste. Les Commissions de gestion et la Délégation des finances sont tenues d'examiner les aptitudes professionnelles et personnelles du préposé et de porter leurs constatations à la connaissance de la Commission judiciaire (art. 40a, al. 6, LParl).

14 Le préposé n'est pas soumis à un contrôle de sécurité relatif aux personnes par l'administration fédérale (art. 29, al. 4, let. e^{bis} , LSI), ce qui a pour conséquence que l'examen des aspects liés à la sécurité relève également de la responsabilité de l'organe électoral.

IV. RAPPORT DE TRAVAIL (AL. 3)

15 Les rapports de travail du préposé sont régis par la LPers, sauf disposition contraire de la LPD. La LPers s'applique par conséquent à titre subsidiaire, pour le cas où la LPD ne prévoit pas de dispositions spéciales. La LPD contient des dispositions divergentes ou plus précises aux endroits suivants :

- Art. 43 al. 1 et 2 LPD (élection)
- Art. 43 al. 3 LPD (caisse de pension)
- Art. 43 al. 3bis LPD (base légale pour les dispositions d'exécution)
- Art. 43 al. 4, première phrase LPD (indépendance et liberté de donner des instructions)
- Art. 43 al. 6 LPD (système d'évaluation)

- Art. 44 al. 1 et 2 LPD (durée du mandat et résiliation)
- Art. 44 al. 3 LPD (révocation)
- Art. 44a LPD (avertissement)
- Art. 46 LPD (incompatibilité)
- Art. 47 LPD (activité accessoire)
- Art. 47a LPD (récusation)
- Art. 72 LPD (disposition transitoire)
- Art. 72a LPD (disposition transitoire)

Des dérogations au droit du personnel de la Confédération sont notamment nécessaires lorsque l'indépendance du préposé ou la procédure de nomination particulière (élection par l'Assemblée fédérale réunie) l'exigent.

L'art. 43, al. 3, contient ensuite, dans les phrases 2 à 4, une disposition précisant le rôle du préposé en matière de prévoyance professionnelle. Une telle disposition est nécessaire car, selon le rapport de la CIP-N, la LPers ne s'applique pas directement dans ce cas. L'art. 43, al. 3, stipule que le mandataire est assuré jusqu'à l'âge de 65 ans auprès de la Caisse fédérale de pensions PUBLICA contre les conséquences économiques de la vieillesse, de l'invalidité et du décès. En outre, le mandataire a la possibilité de maintenir la prévoyance vieillesse jusqu'à la fin de l'année au cours de laquelle il atteint l'âge de 68 ans (cf. également l'art. 4 al. 2 de l'ordonnance sur les rapports de travail du mandataire), à condition que les rapports de travail se poursuivent. Le contenu de cette disposition correspond à l'art. 8 al. 2 et 3 de l'ordonnance de l'Assemblée fédérale du 1er octobre 2010 concernant les rapports de travail et le traitement du procureur général de la Confédération et des procureurs généraux suppléants (ci-après : ordonnance concernant les rapports de travail du procureur général de la Confédération, RS 173.712.23). Le PFPDT finance les cotisations d'épargne de l'employeur. 16

V. DISPOSITIONS D'EXÉCUTION RELATIVES AUX RAPPORTS DE TRAVAIL (AL. 3BIS)

En raison de sa position d'organe d'élection, c'est le Parlement et non le Conseil fédéral qui est compétent pour édicter les dispositions d'exécution relatives aux rapports de travail du préposé. Le fait que les dispositions 17

d'exécution soient édictées par l'organe de nomination est à saluer pour des raisons de cohérence et de préservation de l'indépendance. Le Parlement a pris en main ces travaux dans le cadre de l'initiative parlementaire CIP-N 21.443 et a adopté le 17 juin 2020 l'"Ordonnance sur les rapports de travail du chef du Préposé fédéral à la protection des données et à la transparence".

18 L'ordonnance de l'Assemblée fédérale sur les rapports de travail du préposé se fonde sur l'art. 43 al. 3bis LPD. Elle stipule notamment que

- les principales décisions de l'employeur concernant la nomination du préposé et la révocation relèvent de la compétence de l'Assemblée fédérale (Chambres réunies) (renvoi purement déclaratoire à l'art. 2 al. 1), tandis que la commission judiciaire est compétente pour les autres décisions de l'employeur (p. ex. mise au concours du poste) à l'égard du préposé (art. 2 al. 3).
- les rapports de travail du préposé sont fondés sur une décision d'élection de l'Assemblée fédérale soumise à approbation (art. 3, al. 1) et que, contrairement à d'autres magistrats, le préposé n'est pas tenu de prêter serment ni de faire vœu d'accomplissement consciencieux de ses devoirs (art. 3, al. 4).
- le préposé cesse d'exercer ses fonctions au plus tard à la fin de l'année au cours de laquelle il atteint l'âge de 68 ans (art. 4 al. 2).
- le ou la mandataire est classé(e) dans la classe de salaire 34 selon l'art. 36 OPers (art. 5 al. 1) et que ni les primes de prestations selon l'art. 49 OPers ni les primes spontanées selon l'art. 49a OPers ne peuvent être versées (art. 6 al. 1).
- le mandataire est assuré pour la prévoyance professionnelle dans le cadre de la caisse de prévoyance de la Confédération (art. 7).
- le taux d'occupation du mandataire est de 100 pour cent (art. 8) et qu'il doit être domicilié en Suisse (art. 9).
- la commission judiciaire est compétente pour délier le préposé du secret de fonction conformément à l'art. 320, ch. 2, CP (art. 10).
- une suspension provisoire du ou de la préposé(e) dans ses fonctions n'est possible qu'aux conditions de l'art. 14 al. 5 LRCF et que les prescriptions du droit du personnel de la Confédération (art. 103 et 103a OPers) sont exclues (art. 11).

- la commission judiciaire peut en principe accorder au préposé, en cas de résiliation des rapports de travail, une indemnité correspondant au maximum à un salaire annuel, si le cas d'espèce le justifie (art. 12 ; pour les exceptions, cf. art. 12 al. 3 et pour l'obligation de remboursement, cf. art. 12 al. 5).
- le traitement des données personnelles du préposé dans le cadre de ses rapports de travail est régi par l'ordonnance concernant la protection des données personnelles du personnel de la Confédération (OPDP), sous réserve des dispositions de l'ordonnance sur l'administration du Parlement (Oparl) (art. 13).

VI. INDÉPENDANCE ET ATTRIBUTION (AL. 4)

Conformément à l'art. 43, al. 4, première phrase, LPD, le préposé exerce sa fonction en toute indépendance, sans solliciter ni accepter d'instructions d'une autorité ou d'un tiers. La liberté de recevoir des instructions comporte deux éléments : Le préposé ne peut ni solliciter activement des instructions ni en recevoir passivement. Cela concerne aussi bien les instructions d'autres autorités publiques que celles de tiers privés. 19

Le fait que le PFPDT ne soit pas lié par des instructions permet notamment de tenir compte des exigences de droit européen relatives à l'indépendance de l'autorité de surveillance en matière de protection des données figurant à l'art. 12bis al. 4 dans la Convention 108+ modernisée du Conseil de l'Europe et à l'art. 42 al. 1 et 2 de la directive (UE) 2016/680 relative à Schengen ainsi qu'à l'art. 52 al. 1 et 2 du règlement (UE) 2016/679 en relation avec la décision d'adéquation de la Commission européenne (cf. art. 45 al. 2 let. b du règlement de base UE sur la protection des données 2016/679). 20

Même après la révision totale de la LPD, le préposé ou la préposée et le secrétariat permanent du PFPDT constituent une unité administrative décentralisée sans personnalité juridique (art. 2, al. 3 LOGA en relation avec l'art. art. 8 al. 1 let. b OLOGA en relation avec. Annexe 1 let. A, ch. 2.1.1). Sur le plan administratif, le PFPDT reste une autorité rattachée à la Chancellerie fédérale (ChF) (art. 43, al. 4, 2e phrase), mais ne lui est pas subordonné sur le plan institutionnel. La ChF doit faciliter et soutenir l'accomplissement des tâches du PFPDT sur le plan administratif, sans pour autant porter atteinte à son indépendance. Sur la base d'un contrat de prestations, la ChF fournit au 21

PFPDT une série de prestations dans le domaine de l'administration du personnel, des finances et de la bureautique. Il s'agit par exemple de l'attribution de bureaux, de la garantie d'une infrastructure TIC appropriée et du soutien organisationnel du site Internet. Malgré son intégration organisationnelle dans l'administration fédérale, le PFPDT ne doit pas être considéré comme une véritable autorité administrative, mais comme une institution sui generis. Ce statut sui generis est façonné par la LPD et d'autres actes législatifs. En garantissant la liberté d'instruction du PFPDT, on assure son indépendance institutionnelle et fonctionnelle.

22 L'indépendance institutionnelle et fonctionnelle du PFPDT, tout en étant rattaché administrativement à la ChF, se manifeste également dans le mode de communication prescrit. L'art. 37 al. 1 OLPD prévoit que le PFPDT communique avec le Conseil fédéral par l'intermédiaire du chancelier ou de la chancelière de la Confédération. Le chancelier ou la chancelière de la Confédération est alors tenu(e) de transmettre les propositions, avis et rapports au Conseil fédéral sans les modifier. Le PFPDT ne soumet toutefois pas ses rapports à l'Assemblée fédérale par l'intermédiaire de la ChF, mais directement par l'intermédiaire des Services du Parlement (art. 37, al. 2, OLPD).

23 La question se pose de savoir si, au lieu d'un rattachement administratif à la ChF, il n'existerait pas des solutions plus appropriées pour le PFPDT en termes d'organisation administrative. Un rattachement administratif du PFPDT aux Services du Parlement aurait toutefois un effet artificiel, car il n'existe aucun lien entre les tâches du PFPDT et celles des Services du Parlement. L'absence totale de rattachement administratif, comme c'est le cas par exemple pour le Tribunal fédéral, aurait pour conséquence que la collaboration entre le PFPDT et les organes fédéraux ne serait plus aussi étroite si le préposé en tant que personne ou le PFPDT en tant qu'autorité ne faisait plus partie de l'administration fédérale.

VII. SECRÉTARIAT, BUDGET ET PERSONNEL (AL. 5)

24 Les ressources humaines et financières sont déterminantes pour l'indépendance matérielle du PFPDT. L'art. 43 al. 5 LPD prévoit donc que le préposé dispose de son propre budget et d'un secrétariat permanent. Le processus budgétaire est réglé à l'art. 45 LPD.

Le PFPDT doit disposer de ressources humaines et informatiques suffisantes pour accomplir ses tâches légales. Pour ce faire, le secrétariat a notamment besoin de connaissances juridiques, organisationnelles, techniques (de sécurité) et en matière de communication. En ce qui concerne les relations de la Suisse avec l'Union européenne, la dotation de ressources suffisantes est également importante, et ce à double titre : elle constitue un élément important tant en ce qui concerne la décision d'adéquation que la mise en œuvre de l'acquis de Schengen. Ainsi, l'obligation de doter les autorités de contrôle de ressources humaines, techniques et financières, de locaux et d'infrastructures suffisants est inscrite dans les textes européens (art. 12bis al. 5 du 108+ de la Convention modernisée du Conseil de l'Europe, art. 42 al. 4 de la directive UE 2016/680 et art. 52 al. 4 du règlement UE 2016/679). 25

L'art. 43, al. 5, deuxième phrase, LPD prévoit, comme jusqu'à présent, que le préposé engage lui-même son personnel et dispose de certaines compétences à cet égard. Il ou elle signe par exemple les contrats de travail. Le ou la préposé(e) n'est toutefois toujours pas considéré(e) comme un employeur au sens de la LPers pour les collaborateurs du secrétariat, qu'il s'agisse de personnel ou de prévoyance. Selon l'art. 3 al. 1 let. a LPers, l'employeur est le Conseil fédéral. La question de savoir si le ou la préposé(e) aura à l'avenir la qualité d'employeur devra être clarifiée à la prochaine occasion au niveau formel et légal. Conformément à l'art. 36, al. 2, OLPD, le droit du personnel de la Confédération continue donc de s'appliquer aux rapports de travail des employés du secrétariat permanent du PFPDT. L'OPers, l'O-OPers et l'OPers restent donc applicables aux employés du secrétariat. 26

VIII. ÉVALUATION (AL. 6)

Le ou la préposé-e n'est pas soumis-e au système d'évaluation prévu à l'art. 4, al. 3, LPers. Ce système d'évaluation selon la LPers constitue la base d'une rémunération conforme aux prestations et d'un développement ciblé des employés. Comme le PFPDT exerce sa fonction de manière indépendante et n'est soumis à aucune directive, il doit être exclu du système d'évaluation de la LPers. Le fait que les prestations du préposé ne soient pas évaluées selon le système d'évaluation de la LPers est donc la conséquence logique qui découle de son absence de lien avec des instructions et correspond au revers de la médaille. Celui qui n'est pas lié par des instructions ne peut pas non plus être évalué en conséquence, sans que cela ne porte atteinte à son indépendance. 27

28 Au lieu d'une rémunération basée sur les prestations et assortie de primes, il a été prévu pour le chef du PFPDT une évolution salariale indépendante des prestations, sur le modèle de celle du procureur général de la Confédération. Selon l'art. 5 al. 3 de l'ordonnance concernant les rapports de travail, le salaire augmente au 1er janvier de chaque année de trois pour cent du montant maximal de la classe de salaire jusqu'à ce qu'il atteigne ce montant maximal (cf. art. 6 al. 3 de l'ordonnance concernant les rapports de travail du procureur général de la Confédération).

29 L'obligation du PFPDT de rendre compte de son activité (art. 57 LPD) revêt une importance capitale en l'absence d'un système d'évaluation. En cas de violation des devoirs de fonction, il est en outre possible d'adresser un avertissement (art. 44a LPD). S'il s'agit d'une violation grave des devoirs de fonction, la révocation (art. 44 al. 3 LPD) ou la non-réélection par l'Assemblée fédérale entrent en ligne de compte (ultima ratio).

30 Le ou la préposé(e) et l'institution du PFPDT ne sont pas libres de toute forme de surveillance. L'activité du PFPDT est soumise à un contrôle judiciaire, puisque ses décisions peuvent être contestées jusqu'au Tribunal fédéral. En outre, le PFPDT est soumis à la surveillance financière exercée par le Contrôle fédéral des finances (art. 8 al. 1 let. a LCF ; cf. sur les prescriptions relatives à Schengen : Art. 42 al. 6 de la directive européenne 2016/680). Les modalités du contrôle financier doivent tenir compte de l'indépendance du PFPDT. Enfin, le PFPDT reste soumis à la haute surveillance de l'Assemblée fédérale (art. 169 al. 1 Cst.). En vertu de l'art. 8, al. 2, LCF, les tribunaux fédéraux, l'Autorité fédérale de surveillance des marchés financiers, l'Autorité fédérale de surveillance en matière de révision, l'Autorité de surveillance du Ministère public de la Confédération et le Ministère public de la Confédération ne sont soumis à la surveillance financière exercée par le Contrôle fédéral des finances que dans la mesure où elle sert à l'exercice de la haute surveillance par l'Assemblée fédérale. Nous estimons qu'il convient au moins d'examiner la possibilité de compléter l'art. 8, al. 2, LCF pour y inclure le préposé, afin de renforcer son indépendance.

L'avis exprimé reflète l'opinion personnelle des auteurs et n'engage pas l'Office fédéral de la justice.

BIBLIOGRAPHIE

Baeriswyl Bruno, Kommentierung zu Art. 43 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Huber René, Kommentierung zu Art. 43 DSG, in: Maurer-Lambrou, Urs/Blechta, Gabor-Paul (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014.

Petermann Büttler Judith, Kommentierung zu Art. 43 DSG, in: Bieri Adrian / Powell Julian (Hrsg.), Datenschutzgesetz, Orell Füssli Kommentar, Zürich 2023.

MATÉRIAUX

Botschaft des Bundesrates vom 15.9.2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 S. 6941).

Bericht des Bundesamtes für Justiz von Oktober 2018 zum Bundesgesetz über die Umsetzung der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung; Bericht der SPK-N vom 27.1.2022 zur parlamentarischen Initiative 21.443 «Verordnung über das Arbeitsverhältnis der Leiterin oder des Leiters des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten» (BBl 2022 S. 345).

Erläuternder Bericht des BJ zur Datenschutzverordnung DSV vom 31.8.2022.

30. Tätigkeitsbericht des EDÖB, 2022/2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 44 LPD

Un commentaire de Danielle Schneider / Carl Jauslin

PROPOSITION DE CITATION

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 44 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Schneider/Jauslin, N. XXX zu Art. 44 DSG.

Art. 44 Durée, renouvellement et fin des rapports de fonction

[1] La période de fonction du préposé est de quatre ans et peut être renouvelée deux fois. Elle débute le 1er janvier suivant le début de la législature du Conseil national.

[2] Le préposé peut résilier ses rapports de travail pour la fin de chaque mois moyennant un délai de congé de six mois. La Commission judiciaire peut, dans des cas particuliers, accorder au préposé un délai de congé plus court lorsqu'aucun intérêt essentiel ne s'y oppose.

[3] L'Assemblée fédérale (Chambres réunies) peut révoquer le préposé avant la fin de sa période de fonction:

a. s'il a violé gravement ses devoirs de fonction de manière intentionnelle ou par négligence grave;

b. s'il a durablement perdu la capacité d'exercer sa fonction.

TABLE DES MATIÈRES

En bref ... 572
I. Généralités ... 572
A. But de la norme ... 572
B. Contexte et genèse ... 572
II. Durée du mandat et réélection (al. 1) ... 574
III. Résiliation des rapports de travail par le préposé (al. 2) ... 574
IV. Révocation (al. 3) ... 575
A. Conditions ... 575
1. Violation grave des devoirs de fonction ... 575
2. Incapacité durable d'exercer la fonction ... 576
B. Procédure ... 576
Bibliographie ... 577
Matériaux ... 578

EN BREF

Les dispositions relatives à la durée du mandat, à la réélection et à la fin des rapports de travail sont importantes à plusieurs égards pour l'indépendance du ou de la mandataire. On peut notamment citer la limitation de la durée du mandat ainsi que les possibilités restrictives de mettre fin aux rapports de travail. En raison de ses conséquences importantes, une éventuelle révocation du préposé relève de la compétence de l'Assemblée fédérale (Chambres réunies) et non de la Commission judiciaire.

I. GÉNÉRALITÉS

A. But de la norme

1 L'art. 44 LPD règle l'entrée en fonction et la durée du mandat (al. 1 ; n. 6 ss) ainsi que la résiliation des rapports de travail du préposé (al. 2 et 3 ; n. 10 ss). Les motifs et la procédure de résiliation des rapports de travail sont particulièrement importants pour l'indépendance du préposé. Dans ce sens, l'art. 44 LPD, avec la durée limitée du mandat du préposé et les possibilités restrictives de révocation, contribue à une surveillance indépendante de la protection des données.

B. Contexte et genèse

2 La limitation à deux réélections (art. 44, al. 1, première phrase, LPD ; cf. n. 6) a déjà été introduite à l'art. 26a al. 1 aDSG lors de la première étape de la révision totale de la LPD (dispositions de protection des données pour la coopération Schengen en matière pénale). L'art. 44 al. 1 let. e de la directive (UE) 2016/680 relative à Schengen a ainsi été pris en compte. Selon cette disposition, les Etats Schengen doivent régler si et - dans l'affirmative - à quelle fréquence les membres de l'autorité de surveillance de la protection des données peuvent être reconduits dans leurs fonctions. La modification de l'art. 26a al. 1 aDSG est entrée en vigueur le 1er mars 2019.

3 Lors de la deuxième étape de la révision totale de la LPD, l'Assemblée fédérale réunie a été désignée comme organe de nomination du préposé (cf. art. 43 al. 1 LPD). Par la suite, les règles relatives à la durée du mandat, à la réélection et à la fin du mandat ont également dû être adaptées. Il a

notamment été précisé que la durée du mandat commence le 1er janvier suivant le début de la législature du Conseil national (art. 44, al. 1, 2e phrase, LPD ; cf. N. 8). En outre, l'Assemblée fédérale (Chambres réunies) a été déclarée compétente pour révoquer le préposé (art. 44 al. 3 LPD ; cf. N. 18). En revanche, les motifs de la révocation restent matériellement inchangés par rapport au droit en vigueur (art. 26a, al. 3, aDSG) (cf. N. 13 ss).

Enfin, dans le cadre de l'initiative parlementaire CIP-N 21.443, la résiliation des rapports de travail à l'initiative du préposé a été remaniée à l'art. 44 al. 2 LPD : Un droit de résiliation (unilatéral) a été ancré à la place de l'ancienne demande de licenciement (voir N. 10 s.). 4

La question de savoir si le préposé devait recevoir une indemnité de départ en cas de résiliation de ses rapports de travail a fait l'objet d'une controverse au Parlement. Le projet de la CIP-N visant à mettre en œuvre l'initiative parlementaire 21.443 prévoyait un nouvel art. 44 al. 4 LPD qui - en dérogation aux prescriptions du droit du personnel de la Confédération - excluait expressément toute indemnité de départ. Cette disposition était motivée par le fait que le préposé était moins exposé politiquement que d'autres personnes élues par l'Assemblée fédérale (comme le procureur général de la Confédération) ou que d'autres fonctions de haut niveau de l'administration fédérale. En outre, le potentiel de conflit lors de la résiliation des rapports de travail n'est pas tel qu'il justifie une indemnité de départ. Après que le Conseil fédéral se soit prononcé en faveur d'une indemnité de départ dans son avis sur l'initiative parlementaire 21.443, en raison de l'égalité de traitement et de l'indépendance du préposé, la CIP-N a modifié son projet d'acte législatif et proposé une indemnité de départ analogue à celle prévue pour le procureur général de la Confédération. le procureur général de la Confédération ainsi que les juges fédéraux de première instance (actuellement : art. 12 de l'ordonnance de l'Assemblée fédérale du 17.6.2022 relative aux rapports de travail du chef du Préposé fédéral à la protection des données et à la transparence [ci-après "ordonnance sur les rapports de travail du préposé"]). En revanche, les doutes concernant l'indemnité de départ devaient être examinés dans un cadre général (c'est-à-dire pas uniquement pour le préposé). Le Conseil national et le Conseil des Etats ont approuvé cette solution. 5

II. DURÉE DU MANDAT ET RÉÉLECTION (AL. 1)

6 Conformément à l'art. 44 al. 1, première phrase LPD, la durée du mandat du préposé est de quatre ans et peut être renouvelée deux fois. Le préposé peut donc rester en fonction pendant douze ans au maximum. Selon le message du Conseil fédéral, cette limitation de la durée du mandat vise à renforcer l'indépendance du préposé.

7 Au terme de la période de quatre ans, le préposé doit être réélu par l'Assemblée fédérale (Chambres réunies) s'il souhaite continuer à exercer sa fonction. Contrairement au droit en vigueur (art. 26a, al. 1bis, aDSG) et en dérogation à l'art. 14, al. 2, let. c, LPers, il n'y a plus de prolongation tacite ou automatique de la durée du mandat. La légitimité démocratique du préposé est ainsi favorisée.

8 L'art. 44 al. 1, 2e phrase LPD fixe le début du mandat du préposé au 1er janvier suivant le début de la législature du Conseil national. De cette manière, la nomination est confiée au parlement nouvellement constitué. L'art. 72 al. 2 LPD prévoit une exception (unique) pour le cas où, lors de la première élection du préposé par l'Assemblée fédérale (Chambres réunies), c'est l'ancien titulaire du mandat qui est élu. Dans ce cas de figure, la nouvelle durée de mandat du préposé commence déjà le jour suivant l'élection (cf. art. 72, n. 6 s.).

9 Le préposé quitte automatiquement ses fonctions au plus tard à la fin de l'année au cours de laquelle il atteint l'âge de 68 ans (art. 4 al. 2 de l'ordonnance sur les rapports de travail des préposés). Avec le relèvement de la limite d'âge à 68 ans, le préposé est traité de la même manière que les juges fédéraux et le procureur général de la Confédération, également élus par l'Assemblée fédérale.

III. RÉSILIATION DES RAPPORTS DE TRAVAIL PAR LE PRÉPOSÉ (AL. 2)

10 Le préposé peut résilier ses rapports de travail pour la fin de chaque mois, moyennant un préavis de six mois (art. 44, al. 2, première phrase, LPD). Alors que le droit en vigueur ne lui donnait que la possibilité de demander son congé (art. 26a, al. 2, aDSG), le préposé peut désormais résilier unilatéralement les rapports de travail en donnant son congé. Le préposé est

ainsi soumis à une réglementation analogue à celle du procureur général de la Confédération.

La commission judiciaire peut, dans des cas particuliers, accorder au préposé un délai de congé plus court si aucun intérêt essentiel ne s'y oppose (art. 44 al. 2, 2e phrase LPD). Elle tient alors compte des circonstances du cas concret, comme par exemple la période de transition jusqu'à l'entrée en fonction éventuelle d'un nouveau préposé. Un délai de préavis réduit entre surtout en ligne de compte en cas de raisons de santé. 11

IV. RÉVOCATION (AL. 3)

L'art. 44 al. 3 LPD règle la procédure de révocation. Le contenu de cette disposition correspond à la réglementation actuelle de l'art. 26a al. 3 aDSG (voir N. 13 ss). Toutefois, c'est désormais l'Assemblée fédérale (Chambres réunies) et non plus le Conseil fédéral qui est compétent pour révoquer le préposé (cf. n. 18 ss). 12

A. Conditions

Compte tenu des exigences élevées en matière d'indépendance du préposé, la révocation n'est autorisée que dans des cas graves. Les motifs sont énumérés de manière exhaustive à l'art. 44 al. 3 LPD : Le préposé peut être révoqué s'il a gravement violé ses devoirs de fonction intentionnellement ou par négligence grave (let. a ; n. 14 ss) ou s'il a perdu durablement la capacité d'exercer sa fonction (let. b ; n. 17). 13

1. Violation grave des devoirs de fonction

Le devoir principal du préposé est d'accomplir avec légalité et diligence les tâches qui lui sont confiées par la loi dans le domaine de la protection des données et du principe de transparence. Il s'agit notamment d'enquêter sur les violations des prescriptions en matière de protection des données (art. 49 ss LPD), mais aussi de conseiller les personnes privées traitant des données ou les organes fédéraux et les personnes concernées (art. 58 al. 1 let. a, c et d LPD), ainsi que de nombreuses autres tâches, par exemple en relation avec la communication de données à l'étranger (art. 16 al. 2 LPD), l'analyse d'impact en matière de protection des données (art. 23 LPD) ou la notification des violations de la sécurité des données (art. 24 LPD). Parmi les autres devoirs de 14

fonction figurent notamment l'obligation de garder le secret (art. 320 CP, mais voir aussi l'art. 20 al. 2 LPDrans), la limitation des activités accessoires (art. 46 et 47 LPD) ou l'obligation d'élire domicile (art. 9 de l'ordonnance concernant les rapports de travail du préposé).

15 La révocation n'est pas autorisée pour toute violation des devoirs de fonction. La violation doit être grave et intentionnelle ou résulter d'une négligence grave (art. 44 al. 3 let. a LPD). En cas de violation moins grave des devoirs de fonction, un avertissement par la commission judiciaire est envisageable (cf. art. 44a LPD).

16 Dans la doctrine, la non-exécution manifestement infondée de tâches légales ou (en règle générale) une violation du secret de fonction sont notamment qualifiées de violations graves des devoirs de fonction. En revanche, la simple critique de la manière dont l'office est exercé ne peut pas justifier une révocation. La violation des devoirs de fonction doit être telle qu'elle porte irrémédiablement atteinte à la confiance dans la personne et qu'elle rend intolérable la poursuite de la fonction.

2. Incapacité durable d'exercer la fonction

17 La révocation est autorisée lorsque la capacité d'exercer la fonction a été durablement perdue (art. 44 al. 3 let. b LPD). Cela ne devrait être le cas que dans des cas exceptionnels. On pense notamment à des raisons médicales ou de maladie. Mais des raisons familiales entrent également en ligne de compte. Enfin, la capacité d'exercer la fonction peut aussi faire durablement défaut si le préposé est porté disparu ou a disparu.

B. Procédure

18 La révocation du préposé relève - avec son élection - de la compétence de l'Assemblée fédérale (Chambres réunies) en tant que l'une des décisions patronales les plus importantes. Cela est indiqué non seulement à l'art. 44 al. 3 LPD, mais aussi, à titre déclaratoire, à l'art. 2 al. 1 de l'ordonnance concernant les rapports de travail du préposé.

19 La Commission judiciaire prépare une éventuelle révocation et soumet les propositions nécessaires à l'Assemblée fédérale (art. 40a al. 1 let. d, LParl et art. 2 al. 2, de l'ordonnance concernant les rapports de travail du préposé). Mais en règle générale, pour des raisons de proportionnalité, la commission

judiciaire prononce d'abord un avertissement (art. 44a LPD) avant d'entamer une procédure de révocation.

Dans le cadre de la procédure de révocation, le droit d'être entendu doit être accordé au préposé. Dans ses principes d'action relatifs à la procédure en vue d'une destitution ou d'une non-réélection, la Commission judiciaire prévoit notamment que la personne concernée par la procédure de destitution a le droit, après la clôture de l'enquête et avant la présentation du rapport à l'Assemblée fédérale (Chambres réunies), de prendre position par écrit ou oralement sur le résultat de l'enquête et sur les motifs de la décision (art. 7 al. 4 des principes d'action). Ensuite, la proposition de la commission judiciaire à l'Assemblée fédérale (Chambres réunies) doit contenir un compte rendu de la prise de position de la personne concernée (art. 14 al. 2 let. d des Principes d'action). 20

Si l'Assemblée fédérale décide de révoquer le préposé, la question se pose de savoir si cette décision peut être contestée en justice. Les décisions de l'Assemblée fédérale (Chambres réunies) ne sont en principe pas susceptibles de recours (art. 189 al. 4 de la Constitution fédérale). Dans son rapport sur l'initiative parlementaire 21.443, la CIP-N se réfère toutefois à la pratique récente de la Cour européenne des droits de l'homme, selon laquelle la garantie des voies de droit selon l'art. 6 al. 1 CEDH s'applique en cas de révocation de juges. La CIP-N estime - à juste titre selon nous - que cette jurisprudence pourrait être transposée au préposé, qui dispose également d'une forte indépendance. Dans ce cas, le préposé devrait pouvoir contester devant un tribunal (Tribunal administratif fédéral, Tribunal fédéral, CEDH) la révocation de son mandat par l'Assemblée fédérale (Chambres réunies). 21

Les opinions exprimées reflètent l'opinion personnelle des auteurs et n'engagent pas l'Office fédéral de la justice.

BIBLIOGRAPHIE

Baeriswyl Bruno, Kommentierung zu Art. 44 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Häner Isabelle, Die Ausgestaltung der Unabhängigkeit der Datenschutzaufsichtsbehörden in Bund und Kantonen, in: Epiney Astrid/ Hänni Julia/Brülisauer, Flavia (Hrsg.), Die Unabhängigkeit der

Aufsichtsbehörden. Und weitere aktuelle Fragen des Datenschutzrechts, Zürich/Basel/Genf 2012, S. 45-69.

Petermann Büttler Judith, Kommentierung zu Art. 44 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Datenschutzgesetz, Orell Füssli Kommentar, Zürich 2023.

MATÉRIAUX

Gutachten des Bundesamtes für Justiz vom 23.10.2007 «Amtspflichten der Richterinnen und Richter der erstinstanzlichen Bundesgerichte».

Handlungsgrundsätze der Gerichtskommission vom 3.3.2011 zum Verfahren der Kommission im Hinblick auf eine Amtsenthebung oder eine Nichtwiederwahl (BBl 2012 S. 1271).

Botschaft des Bundesrates vom 15.9.2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 S. 6941).

Bericht der SPK-N vom 27.1.2022 zur parlamentarischen Initiative 21.443 «Verordnung über das Arbeitsverhältnis der Leiterin oder des Leiters des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten» (BBl 2022 S. 345).

Stellungnahme des Bundesrates vom 16.2.2022 zum Bericht der SPK-N vom 27.1.2022 zur parlamentarischen Initiative 21.443 «Verordnung über das Arbeitsverhältnis der Leiterin oder des Leiters des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten» (BBl 2022 S. 432).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 44a LPD

Un commentaire de Danielle Schneider / Carl Jauslin

PROPOSITION DE CITATION

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 44a DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Schneider/Jauslin, N. XXX zu Art. 44a DSG.

Art. 44*a* Avertissement

La Commission judiciaire peut adresser un avertissement au préposé si elle constate qu'il a violé ses devoirs de fonction.

TABLE DES MATIÈRES

En bref 581
I. Généralités 581
A. Historique 581
B. Objectif de la norme 581
II. Mesure disciplinaire de l'avertissement 582
III. Procédure disciplinaire 583
Bibliographie 584
Matériaux 584

EN BREF

Le droit disciplinaire est régi par une loi spéciale à l'art. 44a LPD. Cette disposition limite le cercle des mesures disciplinaires possibles selon le droit du personnel de la Confédération et ne met à la disposition du préposé que la mesure de l'avertissement. L'indépendance du préposé est ainsi respectée. Parallèlement, la commission judiciaire dispose, avec la mesure disciplinaire de l'avertissement, d'un instrument lui permettant de dénoncer un comportement contraire aux devoirs du préposé et de protéger la réputation et la fiabilité de l'autorité du PFPDT.

I. GÉNÉRALITÉS

A. Historique

L'art. 44a LPD a été inséré dans la LPD totalement révisée dans le cadre de l'initiative parlementaire CIP-N 21.443. Lors de ces travaux relatifs à la législation d'exécution sur les rapports de travail du préposé, il est apparu que certains compléments de la LPD totalement révisée étaient nécessaires. Le législateur a considéré - entre autres - que le droit disciplinaire était une disposition importante qui devait être clarifiée au niveau de la loi formelle. 1

B. Objectif de la norme

L'art. 44a LPD prévoit une dérogation au droit du personnel fédéral pour les rapports de travail du préposé dans le domaine du droit disciplinaire (cf. art. 43 al. 3, première phrase LPD). La plupart des mesures disciplinaires énumérées à l'art. 99 al. 2 et 3 OPers (en relation avec l'art. 25 al. 2 let. b et c LPers), qui peuvent être prises en cas de violation des obligations découlant du droit du travail, ne sont en effet pas compatibles avec la fonction du préposé ou pourraient compromettre son indépendance. Cela concerne notamment les réductions de salaire et les amendes, ainsi que la modification de l'étendue des tâches, des horaires ou du lieu de travail. Toutefois, le législateur n'a pas non plus voulu renoncer totalement à des mesures disciplinaires à l'encontre du préposé, car de telles mesures peuvent contribuer à garantir l'exercice conforme à la loi de la fonction. 2

3 L'art. 44a LPD doit être compris à la lumière de cette tension entre la préservation de l'indépendance et l'intérêt à une exécution de la fonction conforme à la loi. Cette disposition limite le cercle des mesures disciplinaires possibles selon le droit du personnel de la Confédération et ne met à la disposition du préposé que la mesure de l'avertissement.

II. MESURE DISCIPLINAIRE DE L'AVERTISSEMENT

4 Conformément à l'art. 44a LPD, la commission judiciaire peut prononcer un avertissement si elle constate que le préposé a violé les devoirs de sa charge. Elle dispose ainsi d'un instrument qu'elle doit utiliser pour garantir la réputation et la fiabilité du PFPDT. Par un avertissement, "l'employeur fait comprendre à l'employé qu'il n'est pas disposé à continuer d'accepter le comportement reproché et qu'il entend prendre des mesures plus sévères en cas de répétition ou de poursuite du comportement reproché".

5 Contrairement à la révocation selon l'art. 44 al. 3 let. a LPD, un avertissement ne doit pas nécessairement reposer sur une violation grave des devoirs de fonction. La formulation de la loi semble autoriser un avertissement pour tout type de violation des devoirs de fonction. Au regard du principe de proportionnalité, un avertissement doit toutefois être approprié et nécessaire pour rétablir l'exercice correct de la fonction par le préposé. Selon les explications de la CIP-N relatives à l'initiative parlementaire 21.443, un avertissement pourrait par exemple entrer en ligne de compte si le préposé enfreint les dispositions relatives à l'activité accessoire (art. 47 LPD) ou à l'acceptation de cadeaux ou d'autres avantages (art. 1 al. 2 de l'Ordonnance de l'Assemblée fédérale du 17.6.2022 sur les rapports de travail du chef du Préposé fédéral à la protection des données et à la transparence [ci-après "Ordonnance sur les rapports de travail du préposé"] en relation avec la loi sur la protection des données). Art. 93 f. OPers). En revanche, la commission judiciaire ne peut pas prononcer d'avertissement si elle estime que le préposé fixe de mauvaises priorités dans l'accomplissement de ses tâches. Cela constituerait une ingérence dans l'exercice de la fonction incompatible avec l'indépendance du préposé.

6 En tant que mesure disciplinaire, l'avertissement suppose toujours une faute. Le ou la préposé(e) doit donc avoir agi intentionnellement ou au moins par négligence.

III. PROCÉDURE DISCIPLINAIRE

La commission judiciaire est compétente pour prononcer l'avertissement à l'encontre du ou de la préposé(e). Cela correspond à l'art. 2 al. 3 de l'ordonnance sur les rapports de travail du préposé, selon lequel la commission judiciaire prend les décisions de l'employeur qui ne relèvent pas de l'Assemblée fédérale (Chambres réunies). Si la commission judiciaire parvient à la conclusion que le comportement incriminé constitue une violation grave des devoirs de fonction au sens de l'art. 44 al. 3 let. a LPD, elle peut proposer à l'Assemblée fédérale (Chambres réunies) de révoquer le préposé. 7

La procédure disciplinaire contre le préposé est régie par les dispositions (applicables à titre subsidiaire) du droit du personnel de la Confédération (art. 1 al. 2 de l'ordonnance concernant les rapports de travail du préposé). 8

L'avertissement ne peut être prononcé qu'après une enquête disciplinaire (art. 99 al. 1 OPers). L'art. 98 OPers s'applique à l'enquête disciplinaire : selon cette disposition, la commission judiciaire ouvre l'enquête disciplinaire et désigne la personne qui sera chargée de l'enquête. Il peut également s'agir d'une personne externe (art. 98 al. 1 OPers). 9

La loi sur la procédure administrative est applicable à la procédure disciplinaire (art. 98 al. 2 OPers). Cela signifie en particulier que l'établissement des faits par la commission judiciaire est également régi par les dispositions de la PA, notamment en ce qui concerne la récusation (art. 10 PA), le principe de l'instruction et les moyens de preuve (art. 12 et art. 14 ss PA), l'obligation de collaborer du ou de la préposé-e (art. 13 PA) ainsi que les droits procéduraux du ou de la préposé-e (en particulier le droit de consulter le dossier et d'être entendu ; art. 26 ss PA). PA). 10

L'avertissement doit prendre la forme d'une décision au sens de l'art. 5 PA (art. 34 LPers). Le ou la préposé(e) peut contester l'avertissement de la Commission judiciaire devant le Tribunal administratif fédéral (art. 36 al. 1 LPers). 11

L'avis exprimé reflète l'opinion personnelle des auteurs et n'engage pas l'Office fédéral de la justice.

BIBLIOGRAPHIE

Baeriswyl Bruno, Kommentierung zu Art. 44*a* DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Petermann Büttler Judith, Kommentierung zu Art. 44*a* DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Datenschutzgesetz, Orell Füssli Kommentar, Zürich 2023.

MATÉRIAUX

Botschaft des Bundesrates vom 15.9.2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 S. 6941).

Bericht der SPK-N vom 27.1.2022 zur parlamentarischen Initiative 21.443 «Verordnung über das Arbeitsverhältnis der Leiterin oder des Leiters des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten» (BBl 2022 S. 345).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 45 LPD

Un commentaire de Carl Jauslin / Danielle Schneider

PROPOSITION DE CITATION

Carl Jauslin/Danielle Schneider, Kommentierung zu Art. 45 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Jauslin/Schneider, N. XXX zu Art. 45 DSG.

Art. 45 Budget

Le PFPDT remet chaque année, par l'intermédiaire de la Chancellerie fédérale, son projet de budget au Conseil fédéral. Celui-ci le transmet tel quel à l'Assemblée fédérale.

TABLE DES MATIÈRES

En bref 587
I. Généralités 587
II. Souveraineté budgétaire 588
III. Processus budgétaire 588
IV. Arrêté budgétaire 590
Bibliographie 591
Matériaux 591

EN BREF

Le PFPDT élabore son budget de manière indépendante et le fait parvenir au Conseil fédéral par l'intermédiaire de la Chancellerie fédérale (ChF). Celui-ci le soumet à l'Assemblée fédérale pour approbation sans le modifier. Ce processus budgétaire, dans le cadre duquel la Chancellerie fédérale et le Conseil fédéral peuvent transmettre le budget du PFPDT tel quel et ne peuvent pas le modifier, renforce l'indépendance du PFPDT en tant qu'autorité de surveillance.

I. GÉNÉRALITÉS

La souveraineté budgétaire, le processus budgétaire et la décision budgétaire sont d'une importance fondamentale pour l'indépendance du PFPDT en tant qu'autorité de surveillance (art. 43, n. 4). Seul celui qui décide de manière autonome de son budget est libre d'accomplir ses tâches dans le cadre de son mandat légal. L'indépendance fonctionnelle présuppose en effet une certaine indépendance financière ou matérielle. 1

L'art. 45 décrit le processus par lequel passe le budget du PFPDT. Le budget du PFPDT comprend les rémunérations du personnel, qui constituent de loin la plus grande partie du budget, la location des locaux, les charges matérielles informatiques, les charges de conseil ainsi que les autres charges d'exploitation. Cette disposition se rattache à l'art. 43 al. 5 LPD, qui prévoit déjà, en relation avec le statut du PFPDT, que le préposé dispose de son propre budget. 2

L'art. 45 LPD a été introduit dans la loi fédérale sur la protection des données lors de la révision totale du 25 septembre 2020 (entrée en vigueur le 1.9.2023). Cette disposition a été proposée par le Parlement et ne figure pas encore dans le projet du Conseil fédéral. Le préposé, en particulier, a estimé que la réglementation de son budget devait être alignée sur celle du Contrôle fédéral des finances. L'ancienne loi sur la protection des données du 19 juin 1992 prévoyait uniquement à l'art. 26 al. 4 aLPDG (aujourd'hui art. 43 al. 5 LPD) que le préposé disposait de son propre budget. Sous l'ancien droit, le Conseil fédéral n'était pas encore tenu de reprendre tel quel le projet de budget du PFPDT. En outre, le PFPDT n'avait pas encore la possibilité de défendre lui- 3

même son budget devant l'Assemblée fédérale (voir à ce sujet le nouvel art. 142, al. 2 et 3, troisième phrase, LParl).

II. SOUVERAINETÉ BUDGÉTAIRE

4 La souveraineté budgétaire signifie que le PFPDT établit son budget de manière autonome. La souveraineté budgétaire constitue un élément essentiel de l'indépendance du PFPDT. Le PFPDT doit déterminer de manière autonome les ressources dont il a besoin pour accomplir les tâches qui lui sont confiées par la loi. Dans le domaine de la protection des données, cela concerne les enquêtes sur les violations des dispositions relatives à la protection des données (art. 49 ss LPD), l'assistance administrative (art. 54 s. LPD), les tâches liées à la communication de données à l'étranger (art. 16 LPD), la consultation lors d'analyses d'impact relatives à la protection des données (art. 23 LPD) ainsi que la tenue de registres, l'information, la sensibilisation et la collaboration (art. 56 ss LPD). Le rattachement administratif du PFPDT à la Chancellerie fédérale n'a d'incidence que sur le processus budgétaire et n'affecte pas la souveraineté budgétaire du PFPDT (art. 43 N. 19 ss).

III. PROCESSUS BUDGÉTAIRE

5 Après avoir élaboré de manière autonome son projet de budget, le PFPDT le soumet au Conseil fédéral par l'intermédiaire de la Chancellerie fédérale, à laquelle il est rattaché administrativement (art. 43, al. 4, 2e phrase, LPD). Conformément à l'art. 142 al. 2 de la loi sur le Parlement (LParl), le Conseil fédéral doit intégrer le projet de budget ainsi que les comptes du PFPDT tels quels dans son projet de budget et dans les comptes de la Confédération. Il en va de même pour les budgets et les comptes de l'Assemblée fédérale, des tribunaux fédéraux, du Contrôle fédéral des finances, du Ministère public de la Confédération et de l'autorité de surveillance du Ministère public de la Confédération. Le point commun des institutions mentionnées réside dans leur indépendance vis-à-vis du Conseil fédéral. Dans leurs actions, les institutions mentionnées ne sont liées que par le droit et non par les instructions du Conseil fédéral. La Constitution elle-même (pour l'Assemblée fédérale et le Tribunal fédéral) ou une loi fédérale (dans le cas du Contrôle fédéral des finances, du Ministère public de la Confédération et de leur

autorité de surveillance) stipulent explicitement l'indépendance des unités organisationnelles mentionnées.

L'art. 45 LPD s'inspire, pour le dépôt via le département, de la solution adoptée pour l'autorité de surveillance des activités de renseignement (cf. art. 4 de l'ordonnance du 16 août 2017 sur la surveillance des activités de renseignement, OSR). En revanche, le Contrôle fédéral des finances CDF soumet son budget annuel directement au Conseil fédéral (cf. art. 2 al. 3 LCF) - sans passer par le Département fédéral des finances auquel le CDF est rattaché (art. 1 al. 3 LCF). 6

A cela s'ajoute le fait que, conformément à l'art. 142 al. 3, troisième phrase, LParl, le PFPDT défend lui-même le projet de son budget et de ses comptes devant l'Assemblée fédérale. Cela devrait en principe être fait par le préposé. En comparaison, c'est la Délégation des finances des deux Chambres fédérales (art. 51 LParl) qui assume cette tâche pour le CDF, alors que le Tribunal fédéral et l'autorité de surveillance du Ministère public de la Confédération défendent également leurs budgets devant le Parlement, comme le PFPDT lui-même devant l'Assemblée fédérale (art. 142 al. 3 LParl). 7

Le processus budgétaire peut être résumé comme suit : 8

- Le PFPDT établit un projet de budget qui prévoit toutes les ressources nécessaires pour remplir consciencieusement et conformément à ses obligations les tâches qui lui sont confiées par la loi en tant que préposé à la protection des données et à la transparence.
- Le PFPDT soumet son projet de budget à la Chancellerie fédérale, à laquelle il est rattaché administrativement (art. 43 al. 4, deuxième phrase LPD).
- La Chancellerie fédérale transmet le projet de budget du PFPDT au Conseil fédéral.
- Le Conseil fédéral transmet le projet de budget du PFPDT tel quel à l'Assemblée fédérale pour approbation (art. 45 LPD). Concrètement, cela signifie que le Conseil fédéral intègre sans modification le budget et les comptes du PFPDT dans le budget et les comptes de la Confédération (art. 142 al. 2 LParl) et soumet le projet de budget de la Confédération à l'Assemblée fédérale. Il le fait sous la forme d'un arrêté fédéral simple (art. 143 al. 3 LParl).

- Les commissions des finances des deux Chambres préavisent les budgets (art. 50 al. 1 LParl). L'entrée en matière des Chambres est obligatoire pour les budgets (art. 73 al. 3 LParl).
- Le PFPDT défend son projet de budget devant l'Assemblée fédérale (art. 142 al. 3, troisième phrase).
- L'Assemblée fédérale est compétente pour approuver le projet de budget du PFPDT. Si, dans le cadre de la procédure d'élimination des divergences entre les deux conseils, une proposition de conciliation concernant l'arrêté fédéral sur le budget de la Confédération est rejetée, l'arrêté de la troisième délibération prévoyant le montant le plus bas est considéré comme adopté (art. 94 LParl).

IV. ARRÊTÉ BUDGÉTAIRE

9 Il appartient au Parlement de décider du budget. Pour que le Parlement puisse délibérer utilement sur la proposition de budget du PFPDT, celui-ci doit motiver son budget.

10 Le Parlement ne peut pas lier l'approbation du budget à des charges ou des conditions ; les directives concernant l'utilisation des moyens ou la fixation de priorités ne sont pas autorisées. Le PFPDT peut disposer librement des fonds alloués dans le cadre de son mandat légal.

11 L'art. 15 al. 6 de la Convention 108+ modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel exige que l'autorité de contrôle dispose des ressources nécessaires à l'exécution effective de ses fonctions et à l'exercice de ses compétences. La directive 2016/680 de l'UE relative à Schengen prévoit également, à l'article 42 al. 4 que chaque autorité de contrôle doit être dotée des ressources nécessaires à l'exercice effectif de ses fonctions et de ses pouvoirs, y compris dans le cadre de l'assistance mutuelle, de la coopération et de la participation. En outre, des ressources suffisantes pour la surveillance de la protection des données constituent un critère essentiel pour évaluer le caractère adéquat du niveau de protection des données du point de vue du règlement général sur la protection des données 2016/679 de l'UE (voir à cet égard l'art. 52 al. 4 en relation avec l'art. 45 al. 2 let. b). Enfin, l'efficacité de la surveillance dépend des ressources disponibles.

Un budget insuffisant pour remplir les tâches conférées par la loi remet en question l'indépendance de la surveillance. Les mécanismes juridiques permettant de vérifier l'adéquation du budget font défaut. Parallèlement, les dépassements de budget dus à l'accomplissement de tâches légales ne sont pas considérés comme une violation des devoirs de fonction (art. 44 al. 3 let. a LPD). 12

L'avis exprimé reflète l'opinion personnelle des auteurs et n'engage pas l'Office fédéral de la justice.

BIBLIOGRAPHIE

Baeriswyl Bruno, Kommentierung zu Art. 45 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Petermann Büttler Judith, Kommentierung zu Art. 45 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Datenschutzgesetz, Orell Füssli Kommentar, Zürich 2023.

Koller Stefan, Kommentierung zu Art. 142 ParlG, in: Graf Martin/Theler Cornelia/Wyss von Moritz (Hrsg.) Kommentar zum Parlamentsgesetz (ParlG), Basel 2014.

MATÉRIAUX

Botschaft des Bundesrates vom 15.9.2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 S. 6941).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 46 LPD

Un commentaire de Carl Jauslin / Danielle Schneider

PROPOSITION DE CITATION

Carl Jauslin/Danielle Schneider, Kommentierung zu Art. 46 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Jauslin/Schneider, N. XXX zu Art. 46 DSG.

Art. 46 Incompatibilité

Le préposé ne peut pas être membre de l'Assemblée fédérale ou du Conseil fédéral ni exercer aucune autre fonction au service de la Confédération.

TABLE DES MATIÈRES

En bref 595
I. Généralités 595
II. Pas de membre de l'Assemblée fédérale 596
III. Aucun membre du Conseil fédéral 597
IV. Pas d'autre rapport de travail avec la Confédération 597
Bibliographie 597

EN BREF

Le ou la préposé(e) ne doit pas avoir d'autres rapports de travail avec la Confédération. En particulier, l'appartenance simultanée à l'Assemblée fédérale ou au Conseil fédéral n'est pas compatible avec la fonction de surveillance du préposé. Cette mesure vise à éviter les conflits d'intérêts et à renforcer l'indépendance du PFPDT.

I. GÉNÉRALITÉS

Le préposé ne doit pas être membre de l'Assemblée fédérale ou du Conseil fédéral, ni avoir d'autres rapports de travail avec la Confédération. Cette disposition vise à exclure les conflits d'intérêts découlant de fonctions différentes exercées simultanément. 1

L'art. 144 Cst. règle les incompatibilités entre les fonctions des membres du législatif, de l'exécutif et du judiciaire et est l'expression de la séparation personnelle des pouvoirs au niveau fédéral. Les membres du Conseil national, du Conseil des États, du Conseil fédéral et les juges du Tribunal fédéral ne peuvent pas appartenir simultanément à une autre de ces autorités. Les règles d'incompatibilité ont pour but d'empêcher la concentration du pouvoir sur une seule personne, de prévenir les conflits d'intérêts, de garantir l'indépendance des titulaires de fonctions et d'empêcher toute entrave à l'exercice de celles-ci. L'alinéa 3 de l'art. 144 Cst. stipule que la loi peut prévoir d'autres incompatibilités. Pour les membres du Parlement, les règles d'incompatibilité se trouvent aux art. 14 s. LLP. LParl ; pour les membres du Conseil fédéral et le chancelier ou la chancelière de la Confédération, les incompatibilités professionnelles sont spécifiées à l'art. 60 LOGA. 2

L'art. 46 LPD constitue également une incompatibilité prévue par la loi au sens de l'art. 144 al. 3 Cst. La disposition relative à l'incompatibilité du préposé en raison de sa fonction correspond à celle applicable aux juges fédéraux (art. 6 al. 1 LTF, art. 6 al. 1 LTAF, art. 44 al. 1 LOAP, de même que l'art. 10 al. 1 LBI) et à celle applicable aux membres de l'autorité de surveillance du Ministère public de la Confédération (art. 24 al. 1 LOAP). 3

L'art. 46 LPD a été introduit dans la loi fédérale sur la protection des données lors de la révision totale du 25 septembre 2020 (entrée en vigueur le 1.9.2023). 4

Cette disposition a été proposée par le Parlement et ne figure pas encore dans le projet du Conseil fédéral. Sous l'ancienne loi sur la protection des données du 19 juin 1992, les questions d'incompatibilité de fonctions devaient être évaluées sous l'angle de l'activité accessoire.

5 L'incompatibilité fonctionnelle est une condition sine qua non pour garantir l'indépendance du préposé et découle donc des dispositions de droit européen figurant à l'art. 15 al. 5 de la Convention 108+ modernisée du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel, à l'art. 42 al. 3 de la directive (UE) 2016/680 relative à Schengen et à l'art. 52 al. 3 du Règlement général sur la protection des données 2016/679 de l'Union européenne.

6 L'art. 46 LPD prévoit trois incompatibilités pour le préposé, qui seront brièvement abordées ci-après. Ces incompatibilités ne s'appliquent toutefois qu'au préposé et non à ses collaborateurs.

II. PAS DE MEMBRE DE L'ASSEMBLÉE FÉDÉRALE

7 Le préposé ne peut pas être en même temps membre de l'Assemblée fédérale, c'est-à-dire du Conseil national ou du Conseil des Etats. Ainsi, en cas d'élection au poste de préposé, la personne élue doit mettre fin aux éventuelles fonctions ou engagements déjà existants avant d'entrer en fonction.

8 Les membres de l'Assemblée fédérale peuvent être élus au poste de préposé, mais doivent démissionner du Parlement au plus tard à la date d'entrée en fonction. C'est déjà le cas dans deux élections sur trois par le Conseil fédéral. A l'inverse, le préposé peut, conformément à l'art. 44 al. 2 LPD, résilier ses rapports de travail pour la fin de chaque mois en respectant un délai de résiliation de six mois et assumer ensuite une nouvelle fonction en tant que membre du Parlement (ou du Conseil fédéral ; voir N. 9 ci-après). Conformément à l'art. 44 al. 2 LPD, la commission judiciaire peut, dans de tels cas, accorder au préposé un délai de résiliation plus court si aucun intérêt majeur ne s'y oppose.

III. AUCUN MEMBRE DU CONSEIL FÉDÉRAL

Le préposé ne peut pas être en même temps membre du Conseil fédéral. Même si, d'une part, le Conseil fédéral n'a pas le pouvoir de donner des instructions au PFPDT (art. 43, al. 4, LPD) et, d'autre part, le PFPDT ne peut pas exercer sa fonction de surveillance par l'intermédiaire du Conseil fédéral (art. 4, al. 2, let. b, LPD), les conflits d'intérêts ne peuvent pas être évités et l'indépendance du PFPDT ne serait pas garantie par une telle union personnelle. 9

IV. PAS D'AUTRE RAPPORT DE TRAVAIL AVEC LA CONFÉDÉRATION

La fonction de préposé n'est pas non plus compatible avec d'autres rapports de travail existant simultanément avec la Confédération. Les autres rapports de travail avec la Confédération doivent donc être résiliés avant l'entrée en fonction (cf. n. 8). Cette incompatibilité constitue une sorte de clause générale subsidiaire par rapport aux deux incompatibilités spécifiques concernant le Parlement et le Conseil fédéral. Compte tenu de l'importance centrale de l'indépendance du préposé, une telle règle d'incompatibilité au sens large doit être saluée. 10

Pour des raisons de compétence constitutionnelle, l'art. 46 ne se prononce pas sur l'incompatibilité avec des fonctions et des emplois au niveau cantonal ou communal. La question de savoir si de telles fonctions et de tels rapports de travail au niveau cantonal ou communal sont compatibles avec la fonction de responsable du PFPDT doit être examinée dans le cadre des activités accessoires au sens de l'art. 47 LPD. A l'inverse, les activités accessoires liées à un rapport de travail au sein de la Confédération sont déjà interdites en vertu de la disposition d'incompatibilité de l'art. 46 LPD. 11

L'avis exprimé reflète l'opinion personnelle des auteurs et n'engage pas l'Office fédéral de la justice.

BIBLIOGRAPHIE

Baeriswyl Bruno, Kommentierung zu Art. 46 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Petermann Büttler Judith, Kommentierung zu Art. 46 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Datenschutzgesetz, Orell Füssli Kommentar, Zürich 2023.

Schaub Lukas, Kommentierung zu Art. 144 BV, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar zur Bundesverfassung, Basel 2015.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 47 LPD

Un commentaire de Danielle Schneider / Carl Jauslin

PROPOSITION DE CITATION

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 47 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Schneider/Jauslin, N. XXX zu Art. 47 DSG.

Art. 47 Activité accessoire

[1] Le préposé ne peut exercer aucune activité accessoire.

[2] La Commission judiciaire peut autoriser le préposé à exercer une activité accessoire, pour autant que l'exercice de la fonction ainsi que l'indépendance et la réputation du PFPDT n'en soient pas affectés. Sa décision est publiée.

TABLE DES MATIÈRES

En bref 601
I. Généralités 601
A. But de la norme 601
B. Historique 601
II. principe : interdiction de l'activité accessoire (al. 1) 602
III. exception : autorisation de l'activité accessoire (al. 2) 602
A. Conditions relatives au contenu 603
B. Compétence 604
Bibliographie 604
Matériaux 604

EN BREF

En principe, le préposé ne peut pas exercer d'activité accessoire (art. 47 al. 1 LPD). Cette interdiction contribue à renforcer l'indépendance. Pour qu'une activité soit considérée comme accessoire, elle doit présenter une certaine qualité et une certaine intensité. En revanche, le fait que l'activité soit rémunérée ou non ne joue aucun rôle. Exceptionnellement, la Commission judiciaire peut autoriser le préposé à exercer une activité accessoire, pour autant que celle-ci ne porte atteinte ni à l'exercice de la fonction, ni à l'indépendance, ni à la réputation du PFPDT (art. 47 al. 2 LPD). Compte tenu des exigences élevées en matière d'indépendance du préposé, il convient d'appliquer des critères stricts. Les activités accessoires éventuelles du préposé doivent être publiées afin de tenir compte du besoin de transparence.

I. GÉNÉRALITÉS

A. But de la norme

L'art. 47 LPD prévoit que le préposé ne peut en principe pas exercer d'activité accessoire (art. 47 al. 1 ; n. 4 s.). Cette disposition de la loi spéciale, plus stricte que le droit général du personnel de la Confédération (art. 23 LPers en relation avec l'art. 91 OPers), permet de tenir compte de l'indépendance du préposé. Dans l'accomplissement de ses tâches, le préposé ne doit pas se trouver dans un conflit d'intérêts qui pourrait compromettre son indépendance et mettre en doute la crédibilité de la fonction. 1

B. Historique

L'interdiction de principe de l'activité accessoire pour le préposé a déjà été introduite à l'art. 26b aLPD dans le cadre de la première étape de la révision totale de la LPD (dispositions de protection des données pour la coopération Schengen en matière pénale). En ce qui concerne l'activité accessoire, les prescriptions de l'art. 42 al. 3 de la directive (UE) 2016/680 étaient déterminantes. Les dispositions sont entrées en vigueur le 1er mars 2019. 2

Le contenu de l'art. 47 LPD n'a pas changé depuis lors. Toutefois, la compétence en matière d'autorisation d'une activité accessoire du préposé a été adaptée à deux reprises : Dans la version de la LPD totalement révisée du 3

15 septembre 2020, cette tâche a été confiée à l'Assemblée fédérale (Chambres réunies). Par la suite, on a craint que l'attribution des tâches ne soit pas adaptée à l'échelon et que la procédure puisse s'avérer trop lourde dans la pratique. Dans le cadre de l'initiative parlementaire CIP-N 21.443, la Commission judiciaire a donc été déclarée compétente (art. 47 al. 2 ; cf. n. 11 ss).

II. PRINCIPE : INTERDICTION DE L'ACTIVITÉ ACCESSOIRE (AL. 1)

4 L'art. 47 al. 1 LPD interdit au préposé d'exercer une activité accessoire. Cela vaut indépendamment du fait qu'une telle activité soit rémunérée ou non. L'interdiction de principe de l'activité accessoire va donc plus loin que la règle d'incompatibilité inscrite à l'art. 46 LPD et englobe notamment les fonctions ou les emplois cantonaux et communaux.

5 La LPD ne définit pas la notion d'activité accessoire. Il ressort toutefois de la documentation que toute activité exercée par le préposé en plus de sa fonction ne doit pas être considérée comme illicite. Au lieu de cela, l'activité accessoire doit présenter une certaine qualité et intensité. Ne sont notamment pas considérées comme des activités accessoires les activités de loisirs ou les hobbies.

III. EXCEPTION : AUTORISATION DE L'ACTIVITÉ ACCESSOIRE (AL. 2)

6 Des exceptions à l'interdiction d'exercer une activité accessoire sont possibles aux conditions de l'art. 47 al. 2 LPD : la commission judiciaire peut autoriser le préposé à exercer une activité accessoire (cf. n. 11 ss), pour autant que ni l'exercice de la fonction, ni l'indépendance, ni la réputation du PFPDT ne soient compromis (cf. n. 7 ss). Les conditions mentionnées doivent être comprises comme cumulatives. Lors de l'octroi de l'autorisation, la commission judiciaire tient notamment compte du contenu de l'activité accessoire, du temps nécessaire et du montant d'une éventuelle indemnisation.

A. Conditions relatives au contenu

Premièrement, l'activité accessoire ne doit pas entraver l'exercice de la fonction du préposé. L'accomplissement des tâches ne doit pas être limité par l'absence ou l'indisponibilité du ou de la préposé(e). Il convient de noter que la fonction de préposé - contrairement à l'ancien droit qui ne prescrivait pas de taux d'occupation déterminé - ne peut être exercée qu'à plein temps (art. 8 de l'ordonnance de l'Assemblée fédérale du 17 juin 2022 sur les rapports de travail du chef du Préposé fédéral à la protection des données et à la transparence). Cela est lié aux exigences posées à l'office, qui ont augmenté notamment en raison de la numérisation, ainsi qu'aux nouvelles tâches et compétences que le PFPDT se voit attribuer dans le cadre de la révision totale de la LPD (p. ex. nouvelles compétences d'investigation et de décision selon les art. 49 ss LPD). 7

Deuxièmement, l'activité accessoire ne doit pas porter atteinte à l'indépendance du PFPDT. Un conflit d'intérêts ou la simple apparence d'un conflit d'intérêts doit être exclu en droit et en fait. 8

Troisièmement, l'activité accessoire ne doit pas nuire à la réputation du PFPDT. Ceci est d'autant plus vrai que la fonction du PFPDT est fortement personnifiée et qu'une perception négative du ou de la préposé(e) peut également avoir des répercussions sur l'autorité du PFPDT. 9

Exemples : 10

- L'activité de membre de la direction, du conseil d'administration ou de l'organe de révision d'une entreprise devrait en règle générale porter atteinte à l'indépendance du préposé (et, selon l'ampleur de l'activité, limiter sa disponibilité pour la fonction).
- En outre, les activités pour des associations dont les objectifs remettent en question la protection des données ou la surveillance exercée par le PFPDT ne seraient pas autorisées, car elles mettraient en danger la réputation du PFPDT.
- La question de savoir si une activité d'enseignement (p. ex. en tant que lecteur dans une université) pourrait être autorisée dépend des circonstances du cas d'espèce. En tout état de cause, seule une charge de travail réduite serait possible.

B. Compétence

11 La commission judiciaire est compétente pour autoriser l'activité accessoire (pour la genèse de l'art. 47 al. 2 LPD, cf. n. 2 s.).

12 La commission judiciaire examine au cas par cas, sur la base des informations fournies par le préposé, si les critères pour une exception à l'interdiction de principe de l'activité accessoire sont remplis. Compte tenu des exigences élevées en matière d'indépendance du préposé, un critère strict s'impose. Mais si les conditions de l'art. 47 al. 2 LPD sont manifestement remplies, il serait arbitraire que la commission judiciaire refuse l'autorisation exceptionnelle au préposé.

13 La décision de la commission judiciaire est publiée (art. 47 al. 2, deuxième phrase LPD). Cela contribue à la transparence de la fonction du préposé.

Les opinions exprimées reflètent l'opinion personnelle des auteurs et n'engagent pas l'Office fédéral de la justice.

BIBLIOGRAPHIE

Baeriswyl Bruno, Kommentierung zu Art. 47 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Huber René, Kommentierung zu Art. 47 DSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014.

Petermann Büttler Judith, Kommentierung zu Art. 47 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Datenschutzgesetz, Orell Füssli Kommentar, Zürich 2023.

MATÉRIAUX

Botschaft des Bundesrates vom 15.9.2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 S. 6941).

Bericht des Bundesamtes für Justiz von Oktober 2018 zum Bundesgesetz über die Umsetzung der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen

bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung.

Bericht der SPK-N vom 27.1.2022 zur parlamentarischen Initiative 21.443 «Verordnung über das Arbeitsverhältnis der Leiterin oder des Leiters des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten» (BBl 2022 S. 345).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 47a LPD

Un commentaire de Danielle Schneider / Carl Jauslin

PROPOSITION DE CITATION

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 47a DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Schneider/Jauslin, N. XXX zu Art. 47a DSG.

Art. 47a Récusation

Si la récusation du préposé est contestée, le président de la cour du Tribunal administratif fédéral compétente en matière de protection des données statue.

TABLE DES MATIÈRES

En bref 609
I. Historique 609
II. Motifs de récusation du préposé 610
III. Décision sur la récusation 610
Bibliographie 611
Matériaux 611

EN BREF

L'art. 47a LPD clarifie la question de savoir qui décide de la récusation du préposé en cas de litige. Cette tâche est confiée au président ou à la présidente de la section du Tribunal administratif fédéral compétente en matière de protection des données. Cette solution permet de préserver l'indépendance du préposé et le fait qu'il ne soit pas lié par des instructions.

I. HISTORIQUE

L'art. 47a LPD a été inséré dans la LPD totalement révisée dans le cadre de l'initiative parlementaire CIP-N 21.443. Lors de l'élaboration des dispositions d'exécution relatives aux rapports de travail du préposé, le Parlement a constaté qu'il n'était pas clair de savoir qui devait décider de la récusation du préposé en cas de litige. 1

Les compétences habituelles en vertu du droit du personnel de la Confédération (supérieur hiérarchique selon l'art. 94a, al. 3, OPers) et du droit de la procédure administrative (autorité de surveillance ou autorité collégiale excluant le membre concerné selon l'art. 10, al. 2, PA) n'entraient pas en ligne de compte en raison de la position particulière du ou de la mandataire. L'Assemblée fédérale (Chambres réunies) ou la Commission judiciaire, qui sont en principe compétentes pour les décisions de l'employeur à l'égard du préposé (cf. art. 2 de l'ordonnance de l'Assemblée fédérale du 17 juin 2022 sur les rapports de travail du chef du Préposé fédéral à la protection des données et à la transparence ; ci-après "ordonnance sur les rapports de travail du préposé"), n'entraient pas non plus en ligne de compte comme instances de décision en raison de l'indépendance ou du fait que le préposé n'est pas lié par des instructions. 2

Le Parlement a comblé cette lacune en confiant au président de la cour compétente en matière de protection des données du Tribunal administratif fédéral le soin de statuer sur une récusation litigieuse du préposé. Cette compétence est évidente, étant donné que le président de la Cour I du Tribunal administratif fédéral assumait déjà sous l'ancien droit des tâches particulières dans le domaine de la protection des données (cf. art. 30, al. 2, et art. 33, al. 2, aLPD). 3

II. MOTIFS DE RÉCUSATION DU PRÉPOSÉ

4 Les motifs de récusation du préposé sont en principe régis par le droit du personnel de la Confédération (art. 43 al. 3, première phrase LPD en relation avec l'art. art. 1 al. 2 de l'ordonnance concernant les rapports de travail du préposé). Selon l'art. 94a al. 1 OPers, le préposé se récuse s'il risque d'être partial en raison d'un intérêt personnel dans une affaire ou pour d'autres motifs. L'apparence de partialité suffit à cet égard (art. 94a, al. 1, OPers). L'art. 94a al. 2 OPers énumère (de manière non exhaustive) les motifs de partialité suivants :

- la proximité particulière de relations ou l'amitié ou l'inimitié personnelle avec des personnes physiques ou morales impliquées ou concernées par une affaire ou un processus décisionnel (let. a) et
- l'existence d'une offre d'emploi émanant d'une personne physique ou morale qui est impliquée ou concernée par une transaction ou un processus décisionnel (let. b).

5 En revanche, dans le cadre d'une enquête sur des violations de prescriptions en matière de protection des données, les prescriptions du droit de la procédure administrative et donc les motifs de récusation selon l'art. 10 al. 1 PA s'appliquent (art. 94a al. 4 OPers et art. 52 al. 1 LPD). Il s'agit entre autres de :

- un intérêt personnel dans l'affaire (art. 10 al. 1 let. a PA),
- le mariage, le partenariat enregistré ou la communauté de vie de fait avec une partie (art. 10 al. 1 let. b PA),
- le lien de parenté ou d'alliance avec une partie (art. 10 al. 1 let. bbis PA) ainsi que
- la représentation d'une partie ou le fait d'agir pour une partie dans la même affaire (art. 10 al. 1 let. c PA).

III. DÉCISION SUR LA RÉCUSATION

6 Les motifs de récusation sont de nature impérative. Le préposé doit donc les prendre en compte de sa propre initiative et les porter à la connaissance des

personnes impliquées. Si le/la mandataire se récuse, son/sa suppléant(e) reprend l'affaire.

En revanche, si la récusation du préposé est contestée, la décision est prise par le président ou la présidente de la cour du Tribunal administratif fédéral compétente en matière de protection des données (art. 47a LPD). Cette décision peut faire l'objet d'un recours en matière de droit public auprès du Tribunal fédéral (art. 82 ss. et art. 92 LTF). 7

Les opinions exprimées reflètent l'opinion personnelle des auteurs et n'engagent pas l'Office fédéral de la justice.

BIBLIOGRAPHIE

Baeriswyl Bruno, Kommentierung zu Art. 47*a* DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Petermann Büttler Judith, Kommentierung zu Art. 47*a* DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Datenschutzgesetz, Orell Füssli Kommentar, Zürich 2023.

MATÉRIAUX

Bericht der SPK-N vom 27.1.2022 zur parlamentarischen Initiative 21.443 «Verordnung über das Arbeitsverhältnis der Leiterin oder des Leiters des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten» (BBl 2022 S. 345).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 48 LPD

Un commentaire de Carl Jauslin / Danielle Schneider

PROPOSITION DE CITATION

Carl Jauslin/Danielle Schneider, Kommentierung zu Art. 48 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Jauslin/Schneider, N. XXX zu Art. 48 DSG.

Art. 48 Autocontrôle du PFPDT

Le PFPDT s'assure, par des mesures de contrôle appropriées portant notamment sur la sécurité des données personnelles, du respect et de la bonne application des dispositions fédérales de protection des données en son sein.

TABLE DES MATIÈRES

En bref 615
I. Généralités 615
II. Mesures de contrôle 617
A. Sécurité des données en particulier 617
B. Exécution conforme au droit des dispositions relatives à la protection des données en général 618
Bibliographie 619
Matériaux 619

EN BREF

Le respect des prescriptions en matière de protection des données par le PFPDT est une obligation légale qui découle déjà de la qualité d'organe fédéral du PFPDT. Comme aucune surveillance externe de la protection des données n'est prévue pour le PFPDT, le législateur l'oblige à s'autocontrôler : selon l'art. 48 LPD, le PFPDT doit s'assurer, par des mesures de contrôle appropriées, qu'une exécution conforme au droit est garantie. L'art. 40 OLPD concrétise le fait que le PFPDT doit établir un règlement de traitement pour tous ses traitements automatisés de données - et ce, indépendamment du fait qu'il traite des données personnelles sensibles ou qu'il procède à un profilage. Cela garantit que le respect des prescriptions en matière de protection des données est également contrôlé au sein du PFPDT, ce qui renforce la crédibilité du PFPDT en tant qu'autorité de surveillance vis-à-vis des tiers.

I. GÉNÉRALITÉS

L'art. 48 LPD s'adresse au PFPDT - non pas en tant qu'autorité de surveillance, mais en tant qu'organe fédéral traitant des données personnelles. Il oblige le PFPDT à assurer des mesures de contrôle appropriées afin de garantir la sécurité des données en particulier et l'exécution conforme au droit des prescriptions fédérales sur la protection des données en général, également au sein de son institution. Etant donné qu'aucune surveillance externe de la protection des données n'est prévue pour le PFPDT en tant qu'autorité de surveillance, le législateur oblige par cette disposition le PFPDT à s'autocontrôler lors du traitement de données personnelles. 1

Le PFPDT traite des données personnelles, y compris des données personnelles sensibles, dans les buts suivants (art. 39 OLPD) : 2

- pour exercer ses activités de surveillance (let. a),
- pour exercer ses activités de conseil (let. b),
- pour collaborer avec d'autres autorités (let. c),
- pour accomplir ses tâches dans le cadre des dispositions pénales de la LPD (let. d),

- pour accomplir ses tâches conformément à la loi sur la transparence (let. e-g),
- pour informer la surveillance parlementaire (let. h), pour informer le public (let. i) et pour exercer ses activités de formation (let. j).

Le PFPDT traite des données personnelles aussi bien dans sa fonction de préposé à la protection des données que dans celle de préposé à la transparence. Concrètement, il gère notamment une administration des affaires (art. 57h LOGA), un système de gestion du personnel, une liste des conseillers à la protection des données (art. 10, al. 3, let. d, LPD ; art. 10, al. 4, LPD en relation avec l'art. 27, al. 2, OLPD), le registre des activités de traitement des organes fédéraux (art. 12, al. 4, LPD) et un portail de notification des violations de la sécurité des données (art. 24 LPD). Dans le cadre de ses tâches légales, le PFPDT devrait notamment traiter des données personnelles de ses collaborateurs, des données personnelles d'autres employés de la Confédération, ainsi que des données de tiers, y compris des données de personnes morales (art. 57r LOGA).

3 Le PFPDT lui-même n'est pas soumis à une surveillance externe de la protection des données, c'est pourquoi il est tenu de s'autocontrôler. La disposition de l'art. 48 LPD montre clairement que le PFPDT, en tant qu'autorité de surveillance dans le domaine de la protection des données, n'est pas au-dessus de la loi sur la protection des données et qu'il doit garantir le respect des prescriptions, même au sein de sa propre autorité. Un contrôle externe du PFPDT limiterait de manière disproportionnée son indépendance par rapport au risque plutôt faible d'abus de données.

4 En tant qu'organe fédéral, le PFPDT est tenu de respecter, outre les dispositions générales des art. 5 à 13 et 16 à 29, les dispositions particulières relatives au traitement des données par des organes fédéraux, conformément aux art. 33 et suivants LPDS. LPD sont tenus de respecter. L'art. 48 LPDT prévoit que le PFPDT doit prévoir des mesures de contrôle appropriées pour le respect de ces obligations. Cette obligation d'autocontrôle est due au fait qu'il n'existe pas de surveillance externe correspondante de la protection des données pour le PFPDT. Les obligations primaires ne diffèrent donc pas de celles des autres organes fédéraux ; l'art. 48 LPDT concerne uniquement les obligations du PFPDT en matière de contrôle du respect de ces obligations primaires. Le PFPDT doit notamment prendre toutes les mesures de contrôle

qu'il applique habituellement dans le cadre de son activité de surveillance à l'égard d'autres organes fédéraux, dans la mesure où celles-ci s'avèrent également appropriées lors de l'autocontrôle. La crédibilité du PFPDT dans son activité de surveillance à l'égard des organes fédéraux et des particuliers s'en trouve ainsi renforcée.

La disposition de l'art. 48 LPD concernant l'autocontrôle du PFPDT a été introduite dans la loi fédérale sur la protection des données lors de la révision totale du 25 septembre 2020 (entrée en vigueur le 1er septembre 2023). 5

II. MESURES DE CONTRÔLE

A. Sécurité des données en particulier

L'art. 48 LPD oblige le PFPDT à mettre en place des mesures de contrôle appropriées afin de garantir la sécurité des données au sein de sa propre institution. Selon l'art. 5 let. h LPD, on entend par violation de la sécurité des données "toute violation de la sécurité entraînant accidentellement ou de manière illicite la perte, l'effacement, la destruction ou la modification de données personnelles, ou entraînant leur divulgation ou leur mise à disposition de personnes non autorisées". 6

L'obligation de garantir la sécurité des données pour le PFPDT découle déjà, de manière générale, de l'article 8 LPD. Conformément à cette disposition, les responsables du traitement et les personnes chargées du traitement sur mandat doivent garantir une sécurité des données adaptée au risque par des mesures techniques et organisationnelles appropriées. Les mesures mises en place doivent permettre non seulement de constater a posteriori les violations de la sécurité des données, mais aussi de les éviter de manière préventive. La sécurité des données est concrétisée dans le RGPD. L'art. 3 OLPD, en particulier, mentionne une série de mesures techniques et organisationnelles pour atteindre les objectifs de la sécurité des données selon l'art. 2 OLPD, comme par exemple le contrôle de l'accès, de l'accès, de l'utilisateur, de la saisie et de la communication. Le règlement de traitement pour les organes fédéraux selon l'art. 6 OLPD sert également de moyen pour assurer la sécurité des données. 7

Dans ce contexte, le Conseil fédéral a concrétisé l'obligation d'autocontrôle du PFPDT à l'art. 40 OLPD. Le PFPDT doit établir un règlement de traitement 8

pour tous les traitements automatisés - et ce, indépendamment du fait que, par exemple, des données personnelles sensibles soient traitées, qu'un profilage soit effectué ou que le but du traitement ou la manière dont les données sont traitées puissent conduire à une atteinte grave aux droits fondamentaux de la personne concernée. L'art. 40 OLPD déclare en effet l'art. 6 al. 1 OLPD et les conditions qu'il prévoit pour l'établissement d'un règlement de traitement inapplicables dans le cas du PFPDT.

9 L'art. 40 OLPD ne mentionne pas d'autres mesures que l'obligation d'établir un règlement de traitement dans le cadre de l'autocontrôle du PFPDT. Dans les explications relatives à l'art. 40 OLPD, l'Office fédéral de la justice précise que le PFPDT, à l'instar des autres organes fédéraux, doit également prévoir des processus internes appropriés pour mettre en œuvre le règlement de traitement et en vérifier le respect. La disposition légale de l'art. 48 LPD parle toutefois de manière plus générale de "mesures de contrôle appropriées, notamment en ce qui concerne la sécurité des données". L'élaboration, la mise en œuvre, la vérification et l'adaptation régulière du règlement de traitement conformément à l'art. 40 OLPD ne dispense donc pas le PFPDT de son obligation plus générale de prévoir des mesures de contrôle plus étendues conformément à l'art. 48 LPD, pour autant que celles-ci soient jugées appropriées et adéquates.

B. Exécution conforme au droit des dispositions relatives à la protection des données en général

10 L'art. 48 LPD oblige le PFPDT à mettre en place des mesures de contrôle qui garantissent une exécution conforme au droit des prescriptions fédérales en matière de protection des données. Cette obligation va au-delà de l'élaboration et de la mise en œuvre d'un règlement de traitement au sens de l'art. 40 OLPD. Elle exige notamment que les traitements de données prévus soient régulièrement contrôlés quant à leur conformité avec les prescriptions fédérales en matière de protection des données. C'est précisément dans le cadre du système de contrôle interne (SCI) que le PFPDT devrait prévoir d'autres mesures afin de garantir le respect des prescriptions de la LPD.

11 Contrairement à l'obligation d'établir un règlement de traitement, des mesures de contrôle allant au-delà ne sont toutefois exigées que dans la mesure où elles sont, d'une part, aptes à garantir le respect des prescriptions en matière de protection des données et, d'autre part, proportionnées au risque d'abus de

données et à la menace pesant sur les droits fondamentaux de la personne concernée. Concrètement, l'obligation du PFPDT ne doit pas avoir pour effet de rendre impossible ou de compliquer de manière disproportionnée ses tâches légales de surveillance et de conseil. Ceci étant dit, le PFPDT peut tenir compte des ressources en personnel nécessaires dans le cadre de l'autocontrôle dans le cadre de sa demande de budget.

L'avis exprimé reflète l'opinion personnelle des auteurs et n'engage pas l'Office fédéral de la justice.

BIBLIOGRAPHIE

Baeriswyl Bruno, Kommentierung zu Art. 48 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Petermann Büttler Judith, Kommentierung zu Art. 48 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Datenschutzgesetz, Orell Füssli Kommentar, Zürich 2023.

MATÉRIAUX

Botschaft des Bundesrates vom 15.9.2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 S. 6941).

Erläuternder Bericht des BJ zur Datenschutzverordnung DSV vom 31. 8.2022.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 49 LPD

Un commentaire de Michael Reinle

PROPOSITION DE CITATION

Michael Reinle, Kommentierung zu Art. 49 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Reinle, N. XXX zu Art. 49 DSG.

Section 2
Enquêtes concernant des violations des prescriptions de protection des données

Art. 49 Enquête

[1] Le PFPDT ouvre d'office ou sur dénonciation une enquête contre un organe fédéral ou une personne privée si des indices suffisants font penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données.

[2] Il peut renoncer à ouvrir une enquête lorsque la violation des prescriptions de protection des données est de peu d'importance.

[3] L'organe fédéral ou la personne privée fournit au PFPDT tous les renseignements et les documents qui lui sont nécessaires pour l'enquête. Le droit de refuser de fournir des renseignements est régi par

les art. 16 et 17 PA, pour autant que l'art. 50, al. 2, de la présente loi n'en dispose pas autrement.

[4] Si la personne concernée est l'auteur de la dénonciation, le PFPDT l'informe des suites données à celle-ci et du résultat d'une éventuelle enquête.

TABLE DES MATIÈRES

En bref 624
I. Généralités 624
A. But de la norme et contexte 624
B. Historique 624
II. Enquête 626
A. Différence par rapport au droit en vigueur 626
B. Ouverture de l'enquête (al. 1) 627
C. Renonciation à l'enquête (al. 2) 628
D. Obligation de collaborer (al. 3) 629
E. Information de la personne concernée (al. 4) 631
Bibliographie 632
Matériaux 632

EN BREF

Cette disposition est d'une importance capitale dans la perspective du renforcement des compétences du PFPDT. Les devoirs de coopération des organes fédéraux et des personnes privées dans le cadre de l'enquête sont particulièrement importants. Autre nouveauté importante : le PFPDT peut ouvrir une enquête à l'encontre de personnes privées s'il existe des indices suffisants d'une violation des prescriptions sur la protection des données. Sous l'empire de l'ancienne LPD, la compétence d'enquête à l'égard des personnes privées était plus limitée.

I. GÉNÉRALITÉS

A. But de la norme et contexte

1 Alors que l'art. 4 LPD stipule de manière générale que le PFPDT est chargé de surveiller l'application des prescriptions fédérales en matière de protection des données, l'art. 49 LPD règle l'une des principales compétences du PFPDT en rapport avec cette surveillance, à savoir l'enquête sur d'éventuelles violations de la protection des données par des organes fédéraux ou des personnes privées.

2 L'un des principaux objectifs de la révision de la LPD était de renforcer les compétences de contrôle du PFPDT. Ceci également parce que l'ancienne LPD était considérée comme édentée en ce qui concerne le contrôle des traitements de données effectués par des personnes privées (art. 29 aLPD).

3 En outre, les pouvoirs d'investigation dont disposait jusqu'ici le PFPDT étaient inférieurs aux exigences internationales, d'où la crainte que, sans un renforcement des compétences d'investigation du PFPDT, une décision positive de l'UE en matière d'adéquation ne soit mise en danger.

B. Historique

4 Dans le concept normatif relatif à la révision de la loi sur la protection des données, le renforcement des compétences du PFPDT était l'une des exigences centrales de la révision de la LPD et l'introduction d'une procédure

d'enquête préalable ainsi que le renforcement des pouvoirs d'investigation étaient notamment discutés.

L'art. 41 AP-LPD met en œuvre différentes mesures issues du concept normatif : ainsi, les compétences d'enquête à l'égard des organes fédéraux et des personnes privées, qui figuraient jusqu'alors aux art. 27 et 29 aLPD, ont été regroupées dans une seule disposition et la procédure informelle d'enquête préalable a été réglementée. Alors que l'art. 29 aLPD n'autorisait l'ouverture d'enquêtes à l'égard de personnes privées qu'à des conditions restreintes, ces restrictions devaient être supprimées à l'avenir. Cette décision a également été motivée par le fait que les restrictions actuelles de l'art. 29 aLPD ne répondaient pas aux exigences du P-SEV 108. Les nouveaux pouvoirs d'investigation du PFPDT seraient en outre un élément décisif au regard de l'art. 45 du règlement (UE) 2016/679, afin de garantir que la Commission européenne renouvelle ou maintienne la décision d'adéquation à l'égard de la Suisse. L'art. 41 AP-LPD a fait l'objet de discussions animées lors de la consultation. Alors que certains participants à la consultation ont salué le renforcement des compétences d'enquête, d'autres ont estimé que cela allait beaucoup trop loin. 5

Le contenu de l'art. 43 P-LPD s'inspire de l'art. 41 AP-LPD. On a toutefois renoncé à mentionner la procédure d'enquête préalable. De même, les mesures d'investigation explicitement mentionnées à l'art. 41, al. 3, AP-LPD ont été omises ou copiées dans une autre disposition. Le message relatif à la révision de la LPD soulignait à nouveau que la nouvelle réglementation des compétences d'enquête du PFPDT était importante, car ses compétences de surveillance à l'égard du secteur privé ne répondaient actuellement pas aux exigences du P-SEV 108. 6

L'art. 43 P-LPD a fait l'objet de débats parlementaires. Au Conseil national, la discussion s'est surtout concentrée sur les conditions d'ouverture d'une enquête. La minorité "Romano" souhaitait relever les exigences minimales pour l'ouverture d'une enquête. Le motif invoqué était que de simples indices de violation des dispositions sur la protection des données ne suffiraient pas à satisfaire aux exigences d'une procédure conforme à l'État de droit. On craignait également que le PFPDT ne soit surchargé de travail si les exigences étaient trop faibles. La majorité ne voulait en revanche pas "passer les menottes" au PFPDT. La conseillère fédérale Keller-Sutter, responsable du dossier, a fait remarquer que la proposition de la majorité - il doit y avoir 7

suffisamment d'indices et non pas seulement des signes d'une violation de la protection des données - ne constituerait pas une modification matérielle par rapport à l'art. 43 P-LPD. Elle se montre toutefois critique à l'égard d'une nouvelle augmentation des exigences. La proposition minoritaire "Romano" entraînerait une certaine insécurité juridique dans les procédures du PFPDT. En outre, l'augmentation des exigences en matière d'ouverture de procédure mettrait en péril l'adéquation du niveau de protection des données en Suisse dans un domaine particulièrement important pour l'UE. Ni la Convention 108+ ni les actes juridiques de l'UE ne prévoiraient une telle limitation des pouvoirs d'investigation des autorités de surveillance de la protection des données. Le Conseil national a suivi l'avis de la majorité.

8 Le Conseil des États s'est rallié à la décision du Conseil national concernant l'article 43, paragraphe 1, P-LPD. Le Conseil des États a surtout discuté de l'art. 43, al. 3, P-LPD. Le débat portait sur la protection du secret professionnel. Bien que l'art. 43 al. 3 P-LPD protège déjà le secret professionnel des avocats et des médecins par exemple, la commission du Conseil des États a proposé de mentionner à nouveau explicitement la réserve du secret professionnel. La CF Keller-Sutter a défendu la proposition du Conseil fédéral. Elle a souligné que le secret professionnel était déjà suffisamment protégé dans les lois de procédure applicables. De l'avis du Conseil fédéral, le fait de souligner une nouvelle fois le secret professionnel conduirait plutôt à une insécurité juridique. La question se poserait de savoir pourquoi d'autres motifs de refus importants du droit de procédure général ne sont pas également mentionnés une nouvelle fois de manière explicite. Le Conseil des Etats a toutefois suivi sa commission. Le Conseil national s'est rallié à cette décision du Conseil des États.

II. ENQUÊTE

A. Différence par rapport au droit en vigueur

9 Jusqu'à présent, les enquêtes menées à l'encontre d'organes fédéraux et de personnes privées étaient régies par des dispositions différentes (art. 27 et 29 aLPD). Les exigences pour l'ouverture d'une enquête étaient également différentes. L'art. 27, al. 2, aLPD ne prévoyait pas de seuil particulier pour l'ouverture d'enquêtes contre des organes fédéraux. Selon l'art. 29, al. 1, aLPD, le PFPDT ne pouvait en revanche ouvrir des enquêtes contre des personnes

privées que si les méthodes de traitement étaient susceptibles de porter atteinte à la personnalité d'un grand nombre de personnes (erreur de système), si des fichiers devaient être enregistrés ou s'il existait un devoir d'information selon l'art. 6, al. 3, aLPD. Or, ces exigences de l'art. 29 al. 1 aLPD ne répondaient pas aux normes internationales.

Désormais, les anciennes exigences relatives à l'ouverture d'une enquête à l'encontre de personnes privées sont supprimées. En outre, des règles uniformes s'appliquent à l'ouverture d'enquêtes contre des organes fédéraux et des personnes privées. Il en résulte un renforcement du PFPDT. 10

B. Ouverture de l'enquête (al. 1)

Selon l'art. 49, al. 1, LPD, le PFPDT ouvre une enquête, d'office ou sur dénonciation, lorsqu'il existe suffisamment d'indices qu'un traitement de données pourrait violer les prescriptions sur la protection des données. 11

La dénonciation peut être faite par un tiers ou par la personne concernée, c'est-à-dire en principe par toute personne. La personne qui dénonce n'a toutefois pas la qualité de partie dans la procédure (art. 52 al. 2 LPD e contrario). La dénonciation peut également se faire de manière anonyme. Comme le PFPDT ne doit désormais ouvrir une enquête qu'en présence d'indices suffisants d'une violation de la protection des données, une dénonciation anonyme peut avoir un effet négatif sur cette décision. Le fait qu'une dénonciation soit faite par exemple par une personne ayant un lien étroit avec le traitement de données dénoncé ou non est donc tout à fait pertinent pour cette évaluation. 12

Le PFPDT peut également intervenir lorsque des communiqués de presse font état d'éventuelles violations de la protection des données, ce qui correspond déjà à la pratique actuelle. 13

Les prescriptions de protection des données au sens de l'art. 4, al. 1, LPD ne concernent pas seulement les prescriptions de la LPD, mais aussi les prescriptions fédérales de protection des données spécifiques à un domaine. Sont donc concernées les dispositions relatives à la protection des données contenues dans d'autres actes législatifs fédéraux ainsi que les traités internationaux spécifiques au droit de la protection des données. Cette extension au-delà de la LPD concerne en premier lieu les organes fédéraux. 14

15 Une enquête ne peut être ouverte que s'il existe suffisamment d'indices d'une violation des dispositions relatives à la protection des données. Cette exigence a été introduite par le Parlement (voir n. 7 ci-dessus). Les débats parlementaires n'ont pas permis de définir clairement ce qu'il faut considérer comme un indice suffisant. Une minorité du Conseil national voulait aménager l'art. 43 P-LPD de la manière suivante : "En cas de soupçon fondé, le préposé ouvre, d'office ou sur dénonciation motivée, une enquête contre un organe fédéral ou une personne privée s'il existe des indices manifestes qu'un traitement de données pourrait enfreindre les prescriptions sur la protection des données". Ces exigences plus strictes - notamment l'exigence de disposer d'indices clairs - ont toutefois été rejetées. En cas d'indices suffisants, il ne doit donc s'agir ni d'indices clairs ni de soupçons fondés au sens du droit de procédure pénale. Selon la conseillère fédérale Keller-Sutter, il ne s'agit pas d'un changement matériel par rapport à la proposition du Conseil fédéral, qui parlait simplement d'indices. En fin de compte, le Conseil fédéral ne voulait pas non plus que le PFPDT épuise ses ressources avec des enquêtes générales. Il doit s'agir d'indices qui justifient l'engagement des ressources du PFPDT. Les débats parlementaires et en particulier les votes de la majorité montrent que l'on a voulu accorder au PFPDT une marge d'appréciation en la matière.

C. Renonciation à l'enquête (al. 2)

16 Selon l'art. 49 al. 2 LPD, le PFPDT peut renoncer à une enquête formelle si la violation des dispositions sur la protection des données est de peu d'importance. Selon le message, ce serait par exemple le cas si une association sportive ou culturelle envoyait un message électronique à tous ses membres sans dissimuler l'identité des destinataires. Selon le message, l'al. 2 peut également s'appliquer lorsque le PFPDT estime que les conseils prodigués au responsable suffisent pour remédier à une situation qui ne pose guère de problème en soi.

17 Selon Rosenthal, une renonciation doit également être possible lorsqu'il est clair, dans le cas des annonces de violation de données, que la violation n'est pas grave ou que le responsable a la situation en main.

18 En revanche, le fait que les traitements de données en question concernent un grand nombre de personnes et qu'ils présentent donc un intérêt général pour le public ne plaide pas en faveur d'une renonciation.

Le PFPDT doit agir lorsqu'il estime qu'il existe un intérêt public suffisant pour mener une enquête. En revanche, il doit renoncer à une enquête lorsque seule la sphère privée d'un individu est concernée. Dans ce dernier cas, la personne concernée a la possibilité de porter plainte contre la personne privée devant un tribunal civil ou de contester la décision de l'organe fédéral auprès de l'autorité de recours compétente. 19

L'art. 49, al. 1, en relation avec la. al. 2 LPD est une disposition "potestative" qui laisse au PFPDT une certaine marge de manœuvre pour décider d'ouvrir une enquête ou d'y renoncer. Le Parlement a laissé cette marge de manœuvre au PFPDT (voir n. 7 ci-dessus). Il appartient au PFPDT de décider de l'opportunité d'une telle enquête. Il n'existe donc toujours pas de droit du dénonciateur à l'exécution d'une enquête formelle. 20

Le PFPDT a déjà précisé qu'il continuera à effectuer des prises de contact informelles, c'est-à-dire des enquêtes préalables, comme il l'a fait jusqu'à présent. S'il s'avère, lors de ces prises de contact informelles, que le responsable reconnaît les lacunes sur lesquelles il a été rendu attentif et qu'il y remédie dans un délai raisonnable, le PFPDT renoncera à ouvrir une enquête formelle. En raison des ressources limitées du PFPDT, on peut partir du principe que, même après l'entrée en vigueur de la nouvelle LPD, il fixera des priorités dans le traitement des dénonciations en fonction du principe d'opportunité. 21

D. Obligation de collaborer (al. 3)

L'art. 49 al. 3 LPD règle les obligations de collaborer de la personne privée et de l'organe fédéral lors d'une enquête formelle du PFPDT, en reprenant pour la plupart les règles des art. 27 al. 3 et 29 al. 2 aLPD. 22

La partie à la procédure doit fournir au PFPDT tous les renseignements et documents dont celui-ci a besoin pour son enquête. Selon l'art. 49 al. 3 LPD, une partie n'est pas tenue de fournir plus que des renseignements et des documents. La collaboration peut être exigée de manière informelle. D'autres mesures dans le cadre de l'enquête sont régies par les articles 50 et 52 LPD. 23

Selon l'art. 49 al. 3 LPD, les organes fédéraux et la personne privée doivent collaborer. Comme dans le droit actuel, le PFPDT peut également obliger à collaborer les responsables principaux du traitement des données au sein de l'organe fédéral ou de la personne privée concernés, ainsi que les autres 24

collaborateurs, les personnes chargées d'exécuter des mandats, les auxiliaires et les tiers qui participent au traitement des données à examiner ou qui peuvent fournir des renseignements pertinents à ce sujet.

25 Les obligations de collaborer selon l'art. 49 al. 3 LPD peuvent porter sur des informations relatives à un cas concret, mais aussi être de nature fondamentale. Elles portent sur tous les documents qui peuvent être pertinents pour l'évaluation du PFPDT.

26 Afin que les personnes tenues de collaborer ne s'incriminent pas elles-mêmes, il existe également des droits de refus de fournir des renseignements lors de l'enquête du PFPDT. Les droits de refus d'informer sont régis par les PA 16 et 17.

27 L'art. 16 al. 1 PA renvoie, en ce qui concerne le droit de refuser de témoigner, à l'art. 42 al. 1 et 3 de la loi fédérale de procédure civile fédérale du 4 décembre 1947. Selon l'art. 42 al. 1 et 3 de la loi fédérale de procédure civile, les personnes interrogées peuvent refuser de témoigner si la réponse à la question peut les exposer au risque de poursuites pénales. Il s'agit ici de personnes soumises à une obligation légale de garder le secret en vertu des articles 321, 321bis et 321ter du Code pénal. Il en résulte que les médecins peuvent refuser de fournir au PFPDT des données personnelles sur leurs patients si ces derniers ne consentent pas à cette remise. Il en va de même pour les avocats et leur clientèle. L'art. 90 RGPD prévoit également la possibilité d'établir de tels droits de refus dans le droit national.

28 Une réglementation dérogatoire à l'art. 50 al. 2 LPD demeure réservée. Celui-ci stipule uniquement que le secret professionnel est réservé. Cette réserve a été introduite lors des débats parlementaires (voir n. 8 ci-dessus). Il s'agit d'une insistance qui n'aurait pas été nécessaire en soi, puisque les secrets professionnels légaux sont déjà pris en compte par la PA. La réserve du secret professionnel s'appliquait déjà sous l'ancien droit. Le secret professionnel ne peut toutefois être opposé au PFPDT que si la personne protégée par le secret professionnel ne libère pas la personne tenue de collaborer de son obligation de garder le secret.

29 Le secret de fonction n'est pas opposable au PFPDT.

Les personnes tenues de collaborer ne peuvent pas non plus invoquer des secrets d'affaires ou de fabrication ou des obligations contractuelles de garder le secret. 30

En cas d'enquête préalable informelle avant l'ouverture d'une enquête formelle, les personnes privées ne sont pas tenues de fournir des renseignements au PFPDT. L'art. 49 al. 3 LPD ne s'applique qu'après l'ouverture d'une procédure formelle. Il peut toutefois être judicieux pour les responsables de coopérer volontairement avec le PFPDT s'il existe une possibilité de clarifier ainsi l'affaire sans ouvrir une procédure formelle. 31

Il convient de noter que les documents fournis au PFPDT dans le cadre d'une enquête préalable informelle sont soumis à la loi sur la transparence. L'enquête préalable informelle ne tombe pas sous le coup de l'art. 3 LTrans. Selon ses propres dires, le PFPDT ne peut pas non plus garantir une limitation ou un refus de la consultation par des tiers selon l'art. 7 LTrans. Les informations particulièrement confidentielles ainsi que, par exemple, les données personnelles de tiers doivent donc être traitées avant d'être remises. En outre, dans le cas d'informations particulièrement confidentielles, p. ex. des informations sur les mesures de sécurité des données, il peut être recommandé de ne pas livrer les informations par écrit au PFPDT, mais de les lui présenter oralement sur place lors d'une visite ou de les lui montrer, p. ex. à l'occasion d'une vidéoconférence avec écran partagé. 32

E. Information de la personne concernée (al. 4)

La personne concernée n'est pas partie à la procédure (art. 52 al. 2 LPD e contrario). Cela vaut également lorsque la personne concernée a déposé une plainte. La personne concernée n'a donc pas le droit de consulter le dossier. 33

Selon l'art. 49 al. 4 LPD, le PFPDT doit tout de même informer la personne concernée, si elle a porté plainte, de la suite de sa démarche et du résultat d'une éventuelle enquête. 34

La personne concernée peut ensuite faire valoir ses droits par les voies de droit applicables, c'est-à-dire qu'elle peut porter plainte auprès d'un tribunal civil si le responsable est une personne privée ou qu'elle peut faire recours contre la décision de l'organe fédéral responsable. 35

BIBLIOGRAPHIE

Rudin Beat, Kommentierung zu Art. 2 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2022.

Baeriswyl Bruno, Kommentierung zu Art. 27 und Art. 29 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2022.

Waldmann Bernhard/Oeschger Magnus, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht – Grundlagen und öffentliches Recht, Bern 2011.

Bieri Adrian/Powell Julian, Die Totalrevision des Bundesgesetzes über den Datenschutz - Übersicht der wichtigsten Neuerungen für Unternehmen, Jusletter vom 16.11.2020.

Huber René, Kommentierung zu Art. 27 und Art. 29 DSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014.

Reudt-Demont Janine/Gordon Clara-Ann/Egli Luisa, Das revidierte Datenschutzgesetz, LSR 2021, S. 264–269.

Jöhri Yvonne, Kommentierung zu Art. 27 DSG, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Rosenthal David, Kommentierung zu Art. 29 DSG, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter vom 16.11.2020.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBI 2017 S. 6941 ff., abrufbar unter https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2017/2057/de/pdf-x/fedlex-data-admin-ch-eli-fga-2017-2057-de-pdf-x.pdf, besucht am 30.3.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 50 LPD

Un commentaire de Reto Fanger / Isabelle Oehri

PROPOSITION DE CITATION

Reto Fanger/Isabelle Oehri, Kommentierung zu Art. 50 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Fanger/Oehri, N. XXX zu Art. 50 DSG.

Art. 50 Pouvoirs

[1] Lorsque l'organe fédéral ou la personne privée ne respecte pas son obligation de collaborer, le PFPDT peut dans le cadre de la procédure d'enquête ordonner notamment:

a. l'accès à tous les renseignements, documents, registres des activités de traitement et données personnelles nécessaires pour l'enquête;

b. l'accès aux locaux et aux installations;

c. l'audition de témoins;

d. des expertises.

[2] Le secret professionnel demeure réservé.

[3] Pour l'exécution des mesures prévues à l'al. 1, le PFPDT peut faire appel à d'autres autorités fédérales ainsi qu'aux organes de police cantonaux et communaux.

TABLE DES MATIÈRES

I. But de la norme et genèse 636
II. Droit à l'information du PFPDT 638
A. Ordonner des mesures d'instruction 638
B. Champ d'application personnel et matériel 639
C. Limites, notamment la réserve du secret professionnel 640
III. Procédure 642
A. Aperçu 642
B. Terme "ordonner" 642
C. Voies de recours 645
D. Exécution 646
E. Pas d'émolument 647
Bibliographie 647
Matériaux 650

I. BUT DE LA NORME ET GENÈSE

1 Lorsque le PFPDT mène une enquête sur des violations présumées de la protection des données commises par un organe fédéral ou une personne privée, il doit en principe, conformément à l'art. 49 al. 3 LPD, lui fournir tous les renseignements et mettre à sa disposition tous les documents nécessaires à l'enquête. Afin que l'activité de surveillance puisse être exercée efficacement même si les responsables ne remplissent pas leur obligation de collaborer, l'art. 50 LPD confère au PFPDT certains pouvoirs d'investigation et d'intervention afin d'élucider les faits de manière complète, rapide et exacte.

2 L'art. 50 LPD vise à satisfaire aux exigences actuelles et futures du droit international public, auxquelles la Suisse doit se conformer en tant qu'Etat membre de la Convention STE 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et en tant qu'Etat Schengen. L'art. 15 al. 2 let. a du Protocole d'amendement du 18 mai 2018 à la Convention STE 108 exige que les États membres dotent leurs autorités de contrôle de la protection des données de pouvoirs d'investigation et d'intervention. De même, l'article 47 al. 1 de la directive (UE) 2016/680 dispose que les États de l'UE et de l'espace Schengen doivent prévoir des pouvoirs d'enquête effectifs pour leurs autorités de contrôle, notamment le pouvoir d'accéder à toutes les données à caractère personnel traitées et à toutes les informations nécessaires à l'accomplissement de leurs missions.

3 Eu égard à l'article 45 du règlement (UE) 2016/679 (règlement général sur la protection des données, RGPD), selon lequel un transfert de données à caractère personnel de l'UE vers des pays tiers ne peut être effectué que si le pays tiers en question offre un niveau de protection adéquat, conformément à la décision de la Commission européenne, le législateur suisse considère les nouveaux pouvoirs d'enquête du PFPDT comme un élément décisif pour garantir que l'UE maintient sa décision d'adéquation à l'égard de la Suisse.

4 Par rapport à la loi sur la protection des données de 1992 (aLPD), l'article 50 de la LPD clarifie et renforce la position du PFPDT. Ainsi, l'art. 27 al. 3 aLPD (dans le domaine de la surveillance des organes fédéraux) et l'art. 29 al. 3 aLPD (dans le domaine privé) prévoyaient certes déjà la possibilité, dans le cadre de l'établissement des faits, d'exiger la production de dossiers, de

demander des renseignements et de se faire présenter des traitements de données. Les responsables étaient alors tenus de collaborer, sous réserve du droit de refuser de témoigner applicable par analogie en vertu de l'art. 16 PA (cf. art. 27 al. 3 aLPD et art. 34 al. 2 let. b aLPD). Si les responsables ne coopéraient pas d'eux-mêmes, le PFPDT ne disposait toutefois pas de mesures de contrainte directes pour obtenir des informations (p. ex. la possibilité de saisir des informations ou de se procurer l'accès à des locaux, des installations ou des systèmes, même contre la volonté de l'ayant droit). En cas de refus de collaborer de la part d'un organe fédéral, le PFPDT ne pouvait s'adresser qu'à une unité supérieure ayant le droit de donner des instructions à cette dernière ; dans le domaine privé, il n'avait en fait que la possibilité de déposer une plainte pénale pour violation de l'obligation de collaborer (art. 34 al. 2, let. b aLPD). Dans les cas graves de refus de collaborer de la part d'un organe fédéral ou d'une personne privée, il pouvait en outre informer le public conformément à l'art. 30 al. 2 aLPD.

Les compétences d'investigation limitées du PFPDT sous l'aLPD ont parfois fait l'objet de critiques dans la doctrine et la pratique de la protection des données. Des suggestions visant à élargir les compétences du PFPDT en matière de recherche d'informations ont par exemple également été faites en 2014 par le groupe d'accompagnement de la révision de la LPD. Le renforcement de la position du PFPDT dans ses activités d'enquête est donc une réponse aux exigences internationales (cf. ci-dessus n. 2 s.) et aux points faibles identifiés par la doctrine et la pratique. 5

La pratique montrera si le nouveau régime des compétences d'investigation du PFPDT, associé à ses pouvoirs de recours, qui ont été développés avec retenue (cf. OK-Fanger/Oehri ad art. 51 LPD), garantit une activité de surveillance efficace. Outre la répartition des compétences, une surveillance efficace requiert également une dotation en ressources adéquate du PFPDT. A cet égard, diverses critiques ont été formulées dans la littérature à l'encontre des moyens jugés trop limités qui, malgré l'augmentation déjà intervenue, devraient continuer à contraindre le PFPDT à agir selon le principe de l'opportunité dans son activité de surveillance. Les évaluateurs Schengen 2018 se sont également montrés critiques à cet égard et ont recommandé d'allouer au PFPDT des ressources financières et humaines suffisantes pour qu'il puisse accomplir toutes ses tâches dans le contexte Schengen. 6

II. DROIT À L'INFORMATION DU PFPDT

A. Ordonner des mesures d'instruction

7 Lorsque le PFPDT ouvre une enquête contre un organe fédéral ou une personne privée conformément à l'art. 49 al. 1 LPD en raison d'une violation présumée de la protection des données, il appartient en principe à l'organe fédéral ou à la personne privée en question de fournir au PFPDT tous les renseignements et de mettre à sa disposition tous les documents nécessaires à l'enquête (art. 49 al. 3 LPD). Si le responsable ne respecte pas l'obligation de collaborer prévue à l'art. 49 al. 3 LPD, l'art. 50 al. 1 LPD donne au PFPDT la compétence d'ordonner des mesures de recherche d'informations. L'ordonnance de telles mesures est subsidiaire à la coopération du responsable et présuppose donc que le PFPDT ait ouvert une enquête et tenté en vain d'obtenir les renseignements et documents nécessaires dans le cadre de celle-ci.

8 La liste des mesures possibles pour obtenir des informations à l'art. 50 al. 1 LPD s'appuie sur celle de l'art. 12 PA et n'est pas exhaustive. Le PFPDT peut notamment exiger l'accès à tous les renseignements, documents, listes d'activités de traitement et données personnelles nécessaires à l'enquête (let. a) ainsi qu'aux locaux et installations (let. b) et ordonner l'audition de témoins (let. c) ainsi que des expertises (let. d).

9 Afin de permettre une enquête ciblée, la notion d'accès (art. 50 al. 1 let. a et let. b LPD) doit être comprise au sens large. Ainsi, l'accès aux documents ne comprend pas seulement leur examen, mais aussi, le cas échéant, leur saisie. En ce qui concerne les mesures d'accès de l'art. 50 al. 1 let. a et let. b LPD, la réglementation s'oriente essentiellement sur les dispositions concernées du RGPD (art. 58 al. 1 let. e et let. f RGPD). Dans ce contexte, les renseignements sont généralement recueillis au moyen d'un catalogue de questions et tous les documents utiles à l'enquête sont saisis avec les dossiers. Selon l'art. 12 al. 1 LPD, la liste des activités de traitement doit être établie et tenue par le responsable du traitement et le sous-traitant indépendamment d'une éventuelle enquête sur la protection des données, sauf dans les cas exceptionnels de l'art. 12 al. 5 LPD, qui sont toutefois très étendus dans le pays des PME qu'est la Suisse et qui constituent donc de fait la règle. Ici aussi, l'injonction de l'art. 50 al. 1 LPD se rapporte donc à l'examen et, le cas échéant, à la saisie, mais pas à la tenue correcte. Cette dernière peut, le cas

échéant, faire l'objet d'une décision basée sur les résultats de l'enquête, conformément à l'article 51 LPD. En cas de besoin, la communication des données personnelles nécessaires à l'enquête peut également être ordonnée en vertu de l'art. 50 al. 1 let. a LPD. L'accès aux locaux et aux installations peut s'avérer nécessaire lorsque des mesures techniques et organisationnelles (TOM) font l'objet d'une enquête. En mentionnant les auditions de témoins et les expertises, l'art. 50 al. 1 LPD va plus loin que le RGPD, qui ne contient pas de règles explicites à ce sujet.

Par rapport à l'aLPD, l'énumération exemplative des mesures d'enquête possibles à l'art. 50 al. 1 LPD représente une extension ponctuelle des pouvoirs d'information (cf. supra N. 4). L'extension essentielle de la position du PFPDT en matière de recherche d'informations réside toutefois en premier lieu dans le renforcement des mécanismes d'exécution (cf. n. 18 ss. ci-après). 10

B. Champ d'application personnel et matériel

Pour que le PFPDT puisse remplir ses tâches légales de surveillance, les droits de recherche d'informations qui lui sont conférés doivent être conçus de manière exhaustive. 11

D'un point de vue personnel, la collecte d'informations s'effectue en premier lieu auprès de l'organe fédéral ou de la personne privée concernés, mais peut également inclure d'autres services ou personnes impliqués dans le traitement de données en question (p. ex. collaborateurs, auxiliaires, mandataires, partenaires d'externalisation) ou des tiers susceptibles de fournir des renseignements pertinents (p. ex. personnes concernées, autorités, anciens collaborateurs, partenaires commerciaux). Sous l'aLPD, le cercle des personnes auprès desquelles le PFPDT peut se procurer des informations dans le cadre de ses enquêtes était déjà défini de manière large. Grâce à l'inclusion explicite des auditions de témoins et des expertises à l'art. 50 al. 1 LPD, l'implication possible de tiers apparaît désormais clairement dans le texte de loi. Alors que l'obligation de collaborer du responsable en tant que partie découle de l'art. 49 al. 3 LPD et de l'art. 13 al. 1 let. c PA, celle des tiers se fonde sur les art. 15 et 17 PA. Les droits de refus applicables dans des cas particuliers demeurent réservés (cf. à ce sujet n. 14 ss. ci-après). 12

13 Du point de vue matériel également, le droit à l'information du PFPDT doit être interprété de manière large. L'art. 50 al. 1 let. a LPD mentionne notamment tous les renseignements, documents, listes des activités de traitement et données personnelles qui sont nécessaires à l'enquête. Le droit à l'information s'étend donc à toutes les informations en rapport avec un cas concret ou de nature générale, qui sont pertinentes et nécessaires pour une appréciation juridique de l'infraction présumée à la protection des données. En font partie tous les documents et renseignements qui peuvent indiquer si, quand et comment les services responsables respectent les exigences légales en matière de protection des données, en particulier ceux qui permettent d'évaluer l'exactitude des données, la licéité de leur traitement et le respect des droits des personnes concernées. Sont également concernés les documents et renseignements relatifs aux mesures personnelles, techniques et organisationnelles, la documentation relative aux procédures, aux programmes et aux systèmes ainsi que toutes les bases juridiques (p. ex. instructions, directives, notices, contrats) qui ont un rapport avec l'exécution des dispositions relatives à la protection des données.

C. Limites, notamment la réserve du secret professionnel

14 Le droit à l'information du PFPDT et l'obligation de collaborer qui en découle pour les organes fédéraux et les personnes privées faisant l'objet d'une enquête, ainsi que, le cas échéant, pour les tiers, ne sont évidemment pas illimités. Elles trouvent leurs limites dans les droits de refus pertinents. A cet égard, l'art. 49 al. 3 LPD prévoit que le droit de refuser de fournir des renseignements des organes fédéraux et des personnes privées est régi par les art. 16 et 17 PA, à moins que l'art. 50 al. 2 LPD n'en dispose autrement. Les art. 16 et 17 PA s'appliquent également aux tiers.

15 Selon l'ordre ainsi applicable, qui résulte de l'interaction entre la LPD et la PA et du renvoi partiel qui y est fait à la PCF et au CP, les renseignements ainsi qu'une autre collaboration, par exemple sous la forme de la remise de documents, peuvent en tout cas être refusés :

- si le collaborateur s'expose ou expose un proche au danger d'une poursuite pénale ou d'une atteinte grave à l'honneur ou s'il cause un dommage

patrimonial direct à lui-même ou à ce proche (art. 16 al. 1 PA en relation avec l'art. 42 al. 1 let. a PCF) ;

- si le collaborateur peut se prévaloir de la protection des sources des journalistes (art. 16 al. 1 PA en relation avec l'art. art. 42 al. 1 let. abis PCF en relation avec. art. 28a CP) ;
- lorsque le collaborateur peut se prévaloir d'un secret professionnel au sens de l'art. 321 ch. 1 CP et que le détenteur du secret n'a pas consenti à la révélation du secret (art. 16 al. 1 PA en relation avec l'art. art. 42 al. 1 let. b PCF en relation avec l'art. art. 321 ch. 1 CP) ;
- lorsqu'il s'agit de la correspondance d'un avocat (art. 17 PA en relation avec l'art. 51a PCF).

16 En revanche, l'invocation de secrets de fabrication ou d'affaires, d'obligations contractuelles de garder le secret ou du secret de fonction ne dispense pas de collaborer à une enquête du PFPDT. De son côté, le PFPDT est tenu de respecter les dispositions légales en vigueur - notamment celles relatives à la protection des données et à la préservation des secrets de fabrication et d'affaires - et est soumis au secret de fonction conformément à l'art. 22 LPers, ce qui, selon le législateur, garantit le traitement confidentiel des informations obtenues dans le cadre de ses enquêtes.

17 Selon la pratique sous l'aLPD, les détenteurs d'autres secrets professionnels, c'est-à-dire par exemple les personnes soumises au secret bancaire (art. 47 LB), au secret professionnel en matière de recherche médicale (art. 321bis CP) ou au secret des postes et des télécommunications (art. 321ter CP), ne pouvaient pas non plus se prévaloir d'un droit de refus de collaborer selon l'art. 16 al. 2 PA en relation avec l'aLPD dans le cadre d'enquêtes relevant de la protection des données. l'art. 42 al. 2 PCF. On peut se demander si la réserve explicite du secret professionnel dans le nouvel art. 50 al. 2 LPD change quelque chose à cela. Celle-ci n'a été introduite que lors des débats parlementaires. Selon le point de vue défendu ici, les débats parlementaires en question suggèrent que la mention explicite du secret professionnel n'est qu'une clarification et n'implique aucune modification de la situation juridique et de la pratique.

III. PROCÉDURE

A. Aperçu

18 Alors que le droit à l'information du PFPDT selon l'art. 50 al. 1 LPD n'a subi que des extensions ponctuelles par rapport à l'ancien droit (cf. supra N. 7 ss), la position du PFPDT en matière d'exécution a été nettement renforcée. Sous le régime de l'aLPD, le PFPDT pouvait certes prévoir des mesures d'enquête, mais il ne pouvait pas les imposer si l'autre partie ne coopérait pas (cf. supra N. 4). Désormais, la recherche d'informations du PFPDT est réglée en trois étapes :

- En premier lieu, elle se fait par une demande informelle du PFPDT à l'organe fédéral ou à la personne privée contre laquelle une enquête a été ouverte. En vertu de l'art. 49 al. 3 LPD, le responsable est tenu, dans la mesure où l'enquête le requiert, de fournir des renseignements et de remettre des documents s'il ne peut pas faire valoir un droit de refus de collaborer.
- Subsidiairement, c'est-à-dire lorsque la recherche d'informations par le seul biais de la communication de renseignements et de la remise de documents par l'organe fédéral ou la personne privée concernée n'aboutit pas ou ne suffit pas, le PFPDT peut "ordonner" des mesures d'enquête conformément à l'art. 50 al. 1 LPD (cf. à ce sujet N. 19 ss. ci-après).
- Enfin, le PFPDT peut faire appel à d'autres autorités fédérales ainsi qu'aux organes de police cantonaux ou communaux pour exécuter les mesures ordonnées en vertu de l'art. 50 al. 1 LPD, conformément à l'art. 50 al. 3 LPD.

B. Terme "ordonner"

19 La loi et les documents ne précisent pas explicitement ce qu'il faut entendre par le terme "ordonner" ni sous quelle forme cet ordre doit être donné. Alors que dans le contexte des mesures administratives que le PFPDT peut prendre en vertu de l'art. 51 LPD au terme d'une enquête, la compétence du PFPDT de rendre des décisions est largement thématisée tant dans le message que dans la réception de la nouvelle disposition dans la littérature (cf. OK-Fanger/Oehri ad art. 51 LPD, n. 1 ss), la question de savoir si les mesures d'enquête selon

l'art. 50 LPD ont également un caractère de décision ou si elles doivent être qualifiées d'acte réel de l'autorité n'est pas abordée.

Les dispositions de la PA applicables à la procédure d'enquête selon l'art. 50 LPD en vertu du renvoi de l'art. 52 al. 1 LPD, en particulier les art. 12 à 19 PA, ainsi que les art. 37, 39 à 41 et 43 à 61 PA applicables en vertu du renvoi de l'art. 19 PA, qui sont tous pertinents pour l'établissement des faits dans les procédures administratives, ne déterminent pas non plus expressément sous quelle forme les mesures d'enquête doivent être ordonnées. 20

Selon l'opinion défendue ici et exposée en détail ci-après, l'ordonnance de mesures d'instruction doit prendre la forme d'une décision (incidente) de procédure. 21

Contrairement à ce qui se passe dans le domaine de la procédure civile, les ordonnances de preuve proprement dites ne sont pas courantes dans les procédures administratives où la maxime inquisitoire prévaut. Toutefois, dans de nombreux domaines administratifs, les mesures de preuve ou d'instruction sont généralement ordonnées sous forme de décision. Certes, la jurisprudence ne se penche guère en détail sur la nature juridique des ordonnances concernées, mais dans la plupart de ces décisions, le tribunal qui a rendu le jugement part sans autre du principe qu'il s'agit d'une décision dans les considérants relatifs à l'objet de la contestation. 22

Dans les arrêts où le Tribunal fédéral a eu à se pencher spécifiquement sur la question de savoir si l'ordonnance d'une mesure d'instruction dans un cas spécifique se qualifie ou non de décision (attaquable), l'image n'est pas uniforme : parfois, une telle ordonnance est classée comme décision incidente de procédure, parfois comme acte réel de l'autorité. Dans sa jurisprudence récente, le Tribunal fédéral semble admettre de plus en plus le caractère de décision. Il n'est toutefois pas possible d'en tirer des conclusions générales pour tous les domaines administratifs. 23

La doctrine plaide - à juste titre selon l'avis défendu ici - en faveur d'une qualification en tant que décision, en faisant remarquer que l'ordonnance de mesures de preuve sous obligation de collaborer crée toujours une obligation juridique. Certains font une distinction selon que l'exécution de l'obligation de collaborer peut être imposée par des sanctions (contrainte directe, amende, etc.). Dans la mesure où cela est prévu par la loi et qu'il faut donc partir du principe qu'il existe une véritable obligation juridique, une injonction de 24

coopérer y relative doit être conçue comme une décision incidente si la menace pour le cas d'omission est si concrète qu'elle peut être exécutée.

25 Si un acte administratif porte fortement atteinte à la position juridique du destinataire, une décision par voie de décision est indiquée afin que ce dernier puisse, si nécessaire, demander un examen par une instance de recours. L'organe fédéral ou la personne privée, en tant que partie à une enquête relevant du droit de la protection des données, ne devrait généralement pas être d'accord avec l'ordonnance de mesures d'instruction : Le responsable n'ayant pas voulu ou pas pu, dans le cadre de la demande informelle du PFPDT, lui fournir la base d'informations nécessaire à l'évaluation d'une éventuelle violation de la protection des données, il faut partir du principe qu'il ne pourra ou ne voudra pas soudainement coopérer suffisamment de lui-même, même en réponse à une injonction selon l'art. 50 al. 1 LPD. Il est donc d'autant plus important pour lui, eu égard au droit d'être entendu, de disposer d'une possibilité de faire examiner l'injonction contestée par un tribunal dans les conditions prévues par l'art. 52 al. 1 LPD en relation avec l'art. 46 PA. En outre, conformément à l'art. 50 al. 3 LPD, le PFPDT peut exécuter les mesures d'instruction ordonnées, dans la mesure où elles sont accessibles à une exécution forcée, avec l'aide d'autres autorités fédérales ainsi que des autorités de police cantonales et communales. La non-coopération est punissable en vertu de l'article 60 LPD. En d'autres termes, les mesures d'enquête au sens de l'art. 50 al. 1 LPD entraînent régulièrement de véritables obligations juridiques pour la partie à la procédure, raison pour laquelle elles doivent être ordonnées par voie de décision.

26 Il en va de même pour l'obligation de collaborer des tiers, qui peut être imposée par la force (art. 50 al. 3 LPD) et dont le non-respect peut également entraîner des conséquences pénales (art. 52 al. 1 LPD en relation avec l'art. 60 PA). S'ils sont cités comme témoins ou sommés d'éditer des documents ou d'accorder l'accès à des locaux et à des installations, il s'agit là d'une atteinte importante contre laquelle il faut disposer d'un moyen de recours avant une exécution forcée ou la sanction d'une non-collaboration.

27 Dans une perspective d'économie de procédure, on peut certes objecter que le fait d'ordonner des mesures d'instruction par voie de décision peut, selon les circonstances du cas d'espèce, conduire à des procédures d'instruction très longues et coûteuses. Cela doit toutefois être accepté pour des raisons liées à l'Etat de droit. La motivation des mesures d'enquête par le PFPDT ne doit pas

être soumise à des exigences excessives, de sorte qu'une décision sous forme de décision n'entraîne pas un surcroît de travail important par rapport à un acte purement réel. La procédure risque d'être retardée si un recours indépendant est possible (art. 52 al. 1 LPD en relation avec l'art. 46 al. 1 PA), ce qui ne sera qu'exceptionnellement le cas dans le présent contexte (voir en détail N. 28 ci-après). En outre, le PFPDT peut, le cas échéant, retirer l'effet suspensif à un recours (art. 52 al. 1 LPD en relation avec l'art. 55 al. 2 PA). Enfin, c'est précisément dans le cas d'enquêtes complexes dont la procédure dure longtemps que le prononcé de mesures administratives à titre provisionnel selon l'art. 51 LPD devrait parfois s'imposer (cf. OK-Fanger/Oehri ad art. 51 LPD, n. 22 ss).

C. Voies de recours

Si l'on accorde à l'ordonnance de mesures d'instruction le caractère d'une décision, elle peut faire l'objet d'un recours aux conditions de l'art. 52 al. 1 LPD en relation avec l'art. art. 46 al. 1 PA, elle peut être contestée de manière indépendante par un recours auprès du Tribunal administratif fédéral. 28

En premier lieu, la contestabilité devrait être donnée lorsque la décision peut entraîner un préjudice irréparable au sens de l'art. 46 al. 1 let. a PA. C'est le cas lorsque des griefs sont invoqués à l'encontre des mesures d'instruction ordonnées, griefs qui ne peuvent pas encore être soulevés sans préjudice en contestant la décision finale. L'art. 46 al. 1 let. b PA, selon lequel le recours est également recevable lorsque son admission entraînerait immédiatement une décision finale et permettrait ainsi d'économiser un temps considérable ou les frais d'une vaste procédure probatoire, ne sera guère pertinent en ce qui concerne les mesures d'instruction relevant du droit de la protection des données. 29

Lorsqu'un recours est recevable, la décision du Tribunal administratif fédéral peut ensuite faire l'objet d'un recours en matière de droit public au Tribunal fédéral (art. 82 let. a en relation avec l'art. 86 al. 1 let. a LTF). Dans ce cas, outre le destinataire de la décision, le PFPDT dispose également d'une qualité pour recourir (art. 52 al. 3 LPD). 30

D. Exécution

31 L'art. 50 al. 3 LPD prévoit que le PFPDT peut faire appel à d'autres autorités fédérales ainsi qu'aux organes de police cantonaux ou communaux pour l'exécution des mesures prévues à l'art. 50 al. 1 LPD. L'art. 54 al. 2 let. c LPD stipule en outre à ce sujet que le PFPDT peut communiquer aux autorités consultées les informations et les données personnelles nécessaires à l'accomplissement de leurs tâches légales.

32 L'art. 50 al. 3 LPD a été adapté au cours de la procédure législative. Dans le P-LPD de 2017 encore, la disposition en question conférait expressément au PFPDT le pouvoir d'ordonner des mesures provisionnelles pour la durée de l'enquête et de les faire exécuter par une autorité fédérale ou par les organes de police cantonaux ou communaux (art. 44, al. 2, P-LPD [2017]). La version finale de la disposition ne mentionne plus directement les mesures provisionnelles (cf. sur la possibilité d'ordonner des mesures provisionnelles pendant la durée d'une enquête en matière de protection des données, OK-Fanger/Oehri ad art. 51 LPD, n. 22 ss).

33 En ce qui concerne l'exécution, les règles de la PA, en particulier les art. 39 à 43 PA, s'appliquent également à titre complémentaire en vertu du renvoi de l'art. 52 al. 1 LPD, pour autant que l'art. 50 LPD n'en dispose pas autrement. L'exécution suppose donc qu'il n'existe plus de voie de recours avec effet suspensif contre la décision (art. 52 al. 1 LPD en relation avec l'art. 39 PA). En ce qui concerne les moyens de contrainte possibles (cf. art. 52 al. 1 LPD en relation avec l'art. 41 PA), l'obtention forcée d'un accès et la perquisition de locaux et d'installations ainsi que la saisie d'installations, de documents, de listes d'activités de traitement et de données personnelles joueront en premier lieu un rôle dans la pratique. La menace d'une peine peut également entrer en ligne de compte (cf. art. 60 LPD et art. 52 al. 1 LPD en relation avec l'art. 60 PA). En revanche, il est peu probable qu'il faille jamais envisager de contraindre les parties à fournir des renseignements ou les témoins à se présenter, d'autant plus que le principe de proportionnalité s'applique toujours aux moyens de contrainte utilisés (art. 52 al. 1 LPD en relation avec l'art. 42 PA).

E. Pas d'émolument

L'art. 59 al. 1 let. d LPD stipule que le PFPDT perçoit un émolument auprès des personnes privées pour l'adoption de mesures provisionnelles et de mesures (administratives) conformément à l'art. 51 LPD. En ce qui concerne la procédure d'enquête, cela signifie a contrario qu'en l'absence de base légale correspondante, aucun émolument ne doit en tout cas être imposé à un organe fédéral. En outre, conformément au message relatif à la P-LPD (2017), on devrait en déduire qu'aucun émolument n'est dû pour les enquêtes menées contre des personnes privées qui sont closes sans que des mesures provisionnelles ou administratives aient été ordonnées. 34

L'exemption d'émoluments prévue est convaincante pour les procédures d'enquête dans lesquelles, d'une part, l'établissement des faits est simple sur le plan formel, c'est-à-dire qu'il peut être effectué sans que des mesures d'enquête soient formellement ordonnées, par la seule collaboration d'un responsable qui coopère pleinement, et, d'autre part, le résultat est libératoire, c'est-à-dire qu'il n'entraîne pas de mesures administratives. De même, on peut soutenir que le fait d'ordonner des mesures d'enquête à des tiers, dans la mesure où celles-ci n'ont pas été rendues nécessaires par un manque de coopération de la part du responsable, ne doit pas entraîner de conséquences financières pour ce dernier. Toutefois, l'art. 50 LPD n'est pas uniquement conçu pour de tels cas de figure, mais s'applique également lorsque le responsable ne collabore pas suffisamment à la procédure d'enquête (cf. art. 50 al. 1 LPD). Selon le point de vue défendu ici, l'ordonnance de mesures d'enquête, rendue nécessaire par le seul fait que le responsable n'a pas respecté sans raison son devoir de collaboration, devrait en tout cas entraîner des conséquences financières dans le domaine privé, et ce même si, après l'exécution complète de l'enquête ouverte sur la base d'indices suffisants conformément à l'art. 49 al. 1 LPD, il s'avère qu'il n'y a pas eu de violation des prescriptions sur la protection des données et qu'il n'y a donc pas lieu d'ordonner des mesures administratives conformément à l'art. 51 LPD. 35

BIBLIOGRAPHIE

Auer Christoph/Binder Anja Martina, Kommentierung zu Art. 12 VwVG, in: Auer Christoph/Müller Markus/Schindler Benjamin (Hrsg.), VwVG –

Bundesgesetz über das Verwaltungsverfahren: Kommentar, 2. Aufl., Zürich 2019.

Auer Christoph/Binder Anja Martina, Kommentierung zu Art. 13 VwVG, in: Auer Christoph/Müller Markus/Schindler Benjamin (Hrsg.), VwVG – Bundesgesetz über das Verwaltungsverfahren: Kommentar, 2. Aufl., Zürich 2019.

Auer Christoph/Binder Anja Martina, Kommentierung zu Art. 15 VwVG, in: Auer Christoph/Müller Markus/Schindler Benjamin (Hrsg.), VwVG – Bundesgesetz über das Verwaltungsverfahren: Kommentar, 2. Aufl., Zürich 2019.

Baeriswyl Bruno, Kommentierung zu Art. 50 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Baeriswyl Bruno, Kommentierung zu Art. 27 aDSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, Bern 2015.

Baeriswyl Bruno, Kommentierung zu Art. 29 aDSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, Bern 2015.

Güngerich Andreas/Bickel Jürg, Kommentierung zu Art. 15 VwVG, in: Waldmann Bernhard/Weissenberger Philippe (Hrsg.), VwVG – Praxiskommentar Verwaltungsverfahrensgesetz, 2. Aufl., Zürich 2016.

Güngerich Andreas/Bickel Jürg, Kommentierung zu Art. 16 VwVG, in: Waldmann Bernhard/Weissenberger Philippe (Hrsg.), VwVG – Praxiskommentar Verwaltungsverfahrensgesetz, 2. Aufl., Zürich 2016.

Huber René, Kommentierung zu Art. 27 aDSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014.

Huber René, Kommentierung zu Art. 29 aDSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014.

Jöhri Yvonne, § 8 Aufgabe und Bedeutung der öffentlichen Datenschutzbeauftragten, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht, Basel 2015, S. 245–278.

Jöhri Yvonne, Kommentierung zu Art. 27 aDSG, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Reudt-Demont Janine/Gordon Clara-Ann/Egli Luisa, Das revidierte Datenschutzgesetz: Wichtigste Neuigkeiten mit Fokus auf Gesundheitsdaten, LSR 2021, S. 264–269.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16.11.2020 (zit. Rosenthal nDSG).

Rosenthal David, Der Entwurf für ein neues Datenschutzgesetz: Was uns erwartet und was noch zu korrigieren ist, Jusletter 27.11.2017 (zit. Rosenthal E-DSG).

Rosenthal David, § 7 Sanktionierung von Datenschutzverstössen, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht, Basel 2015, S. 203–244 (zit. Rosenthal Sanktionierung).

Rosenthal David, Kommentierung zu Art. 29 aDSG, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Rudin Beat, Verpasste Chance und Handlungsbedarf: Ein Blick auf die Datenschutzrechts-Reform(en) und die Wirksamkeit der Datenschutzaufsicht, digma 2020, S. 180–187.

Walter Jean-Philippe, «Vingt ans de législation sur la protection des données, rétrospectives et perspectives» – L'évolution du droit de la protection des données: perspectives, Jusletter 25.6.2012.

Wiederkehr René/Meyer Christian/Böhme Anna, Kommentierung zu Art. 13 VwVG, in: Wiederkehr René/Meyer Christian/Böhme Anna (Hrsg.), VwVG Kommentar, Zürich 2022.

Wiederkehr René/Meyer Christian/Böhme Anna, Kommentierung zu Art. 15 VwVG, in: Wiederkehr René/Meyer Christian/Böhme Anna (Hrsg.), VwVG Kommentar, Zürich 2022.

Wiederkehr René/Meyer Christian/Böhme Anna, Kommentierung zu Art. 55 VwVG, in: Wiederkehr René/Meyer Christian/Böhme Anna (Hrsg.), VwVG Kommentar, Zürich 2022.

MATÉRIAUX

Botschaft zur Genehmigung des Protokolls vom 10.10.2018 zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 6.12.2019, BBl 2020 S. 565 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2020/60/de/pdf-a/fedlex-data-admin-ch-eli-fga-2020-60-de-pdf-a.pdf, besucht am 28.6.2023.

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 S. 641 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2017/2057/de/pdf-a/fedlex-data-admin-ch-eli-fga-2017-2057-de-pdf-a.pdf, besucht am 28.6.2023.

Durchführungsbeschluss 7281/19 des Rates der Europäischen Union zur Festlegung einer Empfehlung zur Beseitigung der 2018 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes durch die Schweiz festgestellten Mängel vom 8.3.2019, abrufbar unter https://data.consilium.europa.eu/doc/document/ST-7281-2019-INIT/de/pdf, besucht am 28.6.2023.

Normkonzept zur Revision des Datenschutzgesetzes – Bericht der Begleitgruppe Revision DSG vom 29.10.2014, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/75506.pdf, besucht am 28.6.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 51 LPD

Un commentaire de Reto Fanger / Isabelle Oehri

PROPOSITION DE CITATION

Reto Fanger/Isabelle Oehri, Kommentierung zu Art. 51 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Fanger/Oehri, N. XXX zu Art. 51 DSG.

Art. 51 Mesures administratives

[1] Si des dispositions de protection des données sont violées, le PFPDT peut ordonner la modification, la suspension ou la cessation de tout ou partie du traitement ainsi que l'effacement ou la destruction de tout ou partie des données personnelles.

[2] Il peut suspendre ou interdire la communication de données personnelles à l'étranger si elle est contraire aux conditions des art. 16 ou 17 ou à des dispositions d'autres lois fédérales concernant la communications de données personnelles à l'étranger.

[3] Il peut notamment ordonner à l'organe fédéral ou à la personne privée:

a. de lui fournir les informations prévues aux art. 16, al. 2, let. b et c, et 17, al. 2;

b. de prendre les mesures prévues aux art. 7 et 8;

c. d'informer les personnes concernées conformément aux art. 19 et 21;

d. d'établir une analyse d'impact relative à la protection des données personnelles conformément à l'art. 22;

e. de le consulter conformément à l'art. 23;

f. de l'informer et, le cas échéant, d'informer les personnes concernées, conformément à l'art. 24;

g. de communiquer à la personne concernée les renseignements visés à l'art. 25.

[4] Il peut également ordonner au responsable du traitement privé ayant son siège ou son domicile à l'étranger de désigner un représentant conformément à l'art. 14.

[5] Lorsque l'organe fédéral ou la personne privée a pris, durant l'enquête, les mesures nécessaires au rétablissement d'une situation conforme aux prescriptions de protection des données, le PFPDT peut se limiter à prononcer un avertissement.

TABLE DES MATIÈRES

I. But de la norme et genèse 654
II. Mesures administratives 656
A. Mesures contre les traitements de données qui violent les prescriptions sur la protection des données (art. 51 al. 1, 2 et 4 LPD) 657
B. Mesures d'accompagnement en cas de violation de prescriptions d'ordre ou d'obligations envers les personnes concernées (art. 51 al. 3 LPD) 658
III. Droit procédural 660
A. Généralités 660
B. Mesures provisoires 661
Bibliographie 663
Matériaux 665

I. BUT DE LA NORME ET GENÈSE

1 L'art. 51 LPD décrit les mesures administratives que le PFPDT peut prendre en cas de violation des dispositions relatives à la protection des données. La compétence de décision accordée au PFPDT par l'art. 51 LPD constitue une nouveauté de la nouvelle loi sur la protection des données. En élargissant ainsi les compétences du PFPDT, le législateur répond aux suggestions des évaluateurs Schengen de 2014, qui avaient critiqué le fait que sous l'ancienne loi sur la protection des données de 1992 (aLPD), le PFPDT ne pouvait émettre que des recommandations. L'évaluation Schengen de 2018 recommandait également de renforcer les pouvoirs d'exécution du PFPDT afin qu'il puisse prendre directement des décisions juridiquement contraignantes. L'art. 51 LPD met en œuvre la majeure partie de l'art. 47 al. 2 de la directive (UE) 2016/680, spécifié à l'art. 58 al. 2 du règlement (UE) 2016/679 (règlement général sur la protection des données, RGPD). De même, les exigences de l'art. 15 al. 2 let. c du Protocole d'amendement du 18 mai 2018 à la Convention STE 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel sont ainsi largement satisfaites.

2 En revanche, la révision de la LPD a renoncé à étendre les pouvoirs de sanction du PFPDT au-delà de sa compétence de décision, malgré une recommandation en ce sens de l'Union européenne et malgré une mention correspondante à l'art. 15 al. 2 let. c du Protocole d'amendement du 18 mai 2018 à la Convention STE 108. Contrairement aux autorités de protection des données de différents autres pays - comme par exemple les autorités de surveillance dans le champ d'application territorial du RGPD - le PFPDT ne peut donc notamment toujours pas infliger de sanctions administratives aux organes fédéraux. En ce qui concerne les personnes privées, le PFPDT n'a pas non plus de pouvoir de sanction direct, mais divers manquements aux obligations sont tout de même sanctionnés au chapitre 8 de la LPD. Le PFPDT peut notamment assortir ses décisions de mesures administratives selon l'art. 51 LPD à l'encontre de personnes privées d'une menace de peine selon l'art. 63 LPD. De l'avis du législateur, cet ordre à deux niveaux correspond mieux à la tradition juridique suisse qu'une compétence directe du PFPDT en matière de sanctions et est suffisamment efficace.

Contrairement à ce qui se passe sous le nouveau régime, l'aLPD n'avait pas la compétence d'édicter des mesures juridiquement contraignantes. S'il constatait, dans le cadre d'une enquête menée contre un organe fédéral ou une personne privée, une violation des prescriptions en matière de protection des données, il pouvait uniquement émettre une recommandation au responsable de modifier le traitement des données ou d'y renoncer (art. 27 al. 4 aLPD [pour les organes fédéraux] ou art. 29 al. 3 aLPD [pour les personnes privées]). Si le responsable s'opposait à la recommandation du PFPDT en la rejetant formellement ou en ne la suivant tout simplement pas dans les faits, le PFPDT devait soumettre sa recommandation au département ou à la Chancellerie fédérale (dans le secteur public) ou directement au Tribunal administratif fédéral (dans le secteur privé) afin d'obtenir un jugement juridiquement contraignant. L'organe fédéral concerné et - depuis l'introduction d'un droit de recours correspondant lors de la révision de la LPD en 2006 - le PFPDT pouvaient alors également contester la décision rendue par la suite par le département ou la Chancellerie fédérale auprès du Tribunal administratif fédéral. En dernière instance, les décisions du Tribunal administratif fédéral, tant dans le domaine public que dans le domaine privé, pouvaient faire l'objet d'un recours en matière de droit public devant le Tribunal fédéral (art. 82 let. a en relation avec l'art. 86 al. 1 let. a LTF). Outre cette voie formelle à plusieurs niveaux passant par la recommandation et son éventuel recours, le PFPDT pouvait donner de facto du poids à ses injonctions non contraignantes en informant l'Assemblée fédérale et le Conseil fédéral et en les publiant avec l'effet de réputation correspondant (art. 30 aLPD). 3

Dans la pratique, sous le régime de l'aLPD, le PFPDT n'a émis que peu de recommandations, tant dans le secteur privé que dans le secteur public, et il a été encore plus rare qu'elles soient mises en œuvre par voie de plainte. Souvent, les responsables ont déjà pris les mesures nécessaires au cours de la procédure d'enquête, avec l'aide des conseils du PFPDT (art. 28 et art. 31 al. 1 let. aLPD), pour remédier aux irrégularités révélées. Si le PFPDT a néanmoins émis une recommandation, celle-ci a généralement été suivie sans autre. 4

Néanmoins, la doctrine et la pratique de la protection des données n'ont cessé de critiquer l'absence de compétence du PFPDT pour prendre lui-même des mesures efficaces et, le cas échéant, des sanctions. Les débats politiques et législatifs relatifs à l'aLPD ont également permis d'identifier des points faibles 5

et de discuter d'un éventuel renforcement de la position du PFPDT. Les avis divergeaient toutefois quant à la forme concrète de cette position renforcée, et notamment quant à la question de savoir si le PFPDT devait disposer de pouvoirs de sanction. En 2014, par exemple, une initiative parlementaire demandant l'introduction de pouvoirs de sanction administrative pour le PFPDT n'a pas été suivie. Le renforcement modéré de la position du PFPDT dans le cadre de la révision de la LPD reflète l'opinion des milieux politiques, de la doctrine et de la pratique, ainsi que la pression exercée par les exigences internationales (cf. ci-dessus n. 1 s.).

6 La pratique montrera si le nouveau régime, qui confère au PFPDT des pouvoirs de décision mais pas de pouvoir de sanction direct, garantit une activité de surveillance efficace. Outre la répartition des compétences, une surveillance efficace requiert également une dotation en ressources adéquate du PFPDT. A cet égard, la littérature spécialisée a émis diverses critiques à l'encontre des moyens jugés trop limités qui, malgré l'augmentation déjà intervenue, devraient continuer à contraindre le PFPDT à agir selon le principe de l'opportunité dans son activité de surveillance. Les évaluateurs Schengen 2018 se sont également montrés critiques à cet égard et ont recommandé d'allouer au PFPDT des ressources financières et humaines suffisantes pour lui permettre d'accomplir toutes ses tâches dans le contexte Schengen.

II. MESURES ADMINISTRATIVES

7 L'art. 51 LPD laisse au PFPDT une grande marge de manœuvre : en cas de violation des dispositions relatives à la protection des données, il peut ordonner des mesures visant à remédier à la situation illégale, mais il n'y est pas obligé. L'énumération des mesures n'est pas exhaustive. Le principe de proportionnalité s'applique pour décider si une décision doit être prise et, dans l'affirmative, laquelle : il convient d'ordonner les mesures nécessaires pour (re)garantir la licéité du traitement des données dans un cas concret. Le principe de proportionnalité est également ancré expressément à l'art. 51 al. 5 LPD : si l'organe fédéral ou la personne privée a déjà pris les mesures nécessaires pour rétablir le respect des prescriptions en matière de protection des données pendant l'enquête, l'art. 51 al. 5 LPD prévoit que le PFPDT peut se limiter à prononcer un avertissement. En outre, étant donné que l'art. 51 LPD est conçu comme une disposition potestative, il devrait être possible,

dans l'intérêt d'une pratique adéquate et ciblée au cas par cas, selon l'avis défendu ici, que le PFPDT se contente, en cas de manquements mineurs, de donner aux responsables des indications sur la manière de remédier aux manquements dans le cadre de son activité de conseil (art. 58 al. 1 let. a LPD), au lieu d'émettre une décision de mesure. Il faut s'attendre à ce que le PFPDT, ne serait-ce que pour des raisons d'efficacité, s'efforce de faire en sorte que les responsables prennent les mesures nécessaires pour rétablir la légalité du traitement des données, sans qu'il soit contraint de rendre une décision.

La compétence du PFPDT de rendre des décisions en vertu de l'art. 51 LPD est très large sur le plan du contenu. Elle n'est limitée que par le fait qu'elle dépend de la violation des prescriptions de protection des données : le PFPDT ne peut évidemment pas ordonner, par voie de décision, des choses différentes ou allant au-delà de ce que les dispositions légales de protection des données exigeraient de toute façon. 8

Les mesures énumérées à l'art. 51 LPD peuvent être divisées en deux catégories : Les al. 1, 2 et 4 prévoient des mesures contre les traitements de données qui violent les prescriptions sur la protection des données. L'al. 3 contient des mesures d'accompagnement en cas de violation de prescriptions d'ordre ou d'obligations envers la personne concernée. Le PFPDT peut, le cas échéant, assortir les mesures administratives ordonnées à l'encontre de personnes privées d'une menace de sanction conformément à l'art. 63 LPD (cf. supra, n. 2). 9

A. Mesures contre les traitements de données qui violent les prescriptions sur la protection des données (art. 51 al. 1, 2 et 4 LPD)

La première catégorie de mesures concerne les traitements de données contraires à la protection des données et vise à rétablir le respect des prescriptions violées. Selon la situation, le PFPDT peut ordonner les mesures nécessaires conformément à l'art. 51 al. 1, 2 ou 4 LPD. 10

Au sens d'une clause générale, l'art. 51 al. 1 LPD confère au PFPDT, en ce qui concerne les traitements de données qui violent les prescriptions en matière de protection des données, le pouvoir d'ordonner l'adaptation, l'interruption ou la suspension partielle ou totale ainsi que l'effacement ou la destruction partielle ou totale des données personnelles concernées. 11

12 L'art. 51 al. 2 et al. 4 LPD règle en outre séparément deux cas spécifiques de traitements de données contraires à la protection des données : la communication de données à l'étranger en violation des prescriptions et l'omission de désigner une représentation suisse pour les personnes étrangères traitant des données conformément à l'art. 14 LPD.

13 En cas de communication de données à l'étranger en violation des prescriptions, le PFPDT peut décider de la suspendre ou de l'interdire (art. 51 al. 2 LPD). Sont concernées d'une part les violations des art. 16 et 17 LPD, qui règlent l'exportation de données depuis la Suisse, et d'autre part les violations des dispositions relatives à la communication de données personnelles à l'étranger figurant dans d'autres lois fédérales. La prise en compte des violations d'autres lois fédérales n'a pas été modifiée malgré les critiques émises lors de la consultation. Dans la pratique, elle ne devrait toutefois pas avoir beaucoup d'importance en soi, car de telles exportations de données violent régulièrement le principe de la licéité du traitement des données (art. 6 al. 1 LPD) et pourraient donc également être soumises à la clause générale de l'art. 51 al. 1 LPD.

14 En cas de violation de l'art. 14 LPD, le PFPDT peut ordonner par voie de décision la désignation d'une représentation suisse par des responsables privés ayant leur domicile ou leur siège à l'étranger (art. 51 al. 4 LPD).

B. Mesures d'accompagnement en cas de violation de prescriptions d'ordre ou d'obligations envers les personnes concernées (art. 51 al. 3 LPD)

15 La deuxième catégorie de mesures vise les cas où les prescriptions d'ordre ou les obligations envers les personnes concernées ne sont pas respectées. Il n'est pas nécessaire qu'il y ait eu une violation de la protection des données. L'art. 51 al. 3 LPD contient à cet égard une liste non exhaustive d'injonctions possibles. Celles-ci doivent être lues en relation avec les obligations que la LPD impose aux organes fédéraux et aux personnes privées dans les deuxième et troisième chapitres.

16 La plupart des mesures énumérées à l'art. 51 al. 3 LPD sont des injonctions d'information et de consultation par lesquelles le responsable est invité à informer ou à consulter le PFPDT et/ou les personnes concernées par un traitement de données sur certaines opérations (art. 51 al. 3 let. a, c, e, f et g

LPD). Plus précisément, le PFPDT peut demander aux responsables de traitement de le faire par voie de décision,

- de lui communiquer préalablement les clauses ou garanties correspondantes, dans la mesure où une communication de données à l'étranger sans protection adéquate au sens de l'art. 16 al. 1 LPD est prévue et que la protection des données doit être assurée au moyen de clauses contractuelles de protection des données selon l'art. 16 al. 2 let. b LPD ou au moyen de garanties spécifiques élaborées par l'organe fédéral compétent (art. 16 al. 2 let. c LPD) (art. 51 al. 3 let. a LPD) ;
- de l'informer, conformément à l'art. 17 al. 2 LPD, des cas de communication de données à l'étranger qui relèvent des règles d'exception de l'art. 17 al. 1 let. b ch. 2, let. c et let. d LPD (art. 51 al. 3 let. a LPD) ;
- de respecter ses obligations d'information envers les personnes concernées lors de la collecte de données personnelles (art. 19 LPD) et lors de décisions individuelles automatisées (art. 21 LPD) (art. 51 al. 3 let. c LPD) ;
- de le consulter, conformément à l'art. 23 LPD, dans les cas où une analyse d'impact sur la protection des données effectuée révèle encore un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées, malgré les mesures de protection prévues (art. 51 al. 3 let. e LPD) ;
- de lui notifier, conformément à l'art. 24 LPD, les violations de la sécurité des données et, dans les conditions de l'art. 24 al. 4 et 5 LPD, d'en informer les personnes concernées (art. 51 al. 3 let. f LPD) ;
- de satisfaire à son obligation de renseigner les personnes concernées conformément à l'art. 25 LPD (art. 51 al. 3 let. g LPD).

Les autres mesures énumérées aux let. b et d de l'art. 51 al. 3 LPD sont des ordres d'action. Le PFPDT peut donc exiger des responsables qu'ils le fassent par voie de décision, 17

- de prendre les mesures techniques et organisationnelles (MTO) nécessaires au traitement des données, dans le respect des prescriptions sur la protection des données (art. 7 al. 1 et 2 LPD) et en garantissant une

sécurité appropriée des données conformément à l'art. 8 LPD et aux art. 1 ss. RGPD (art. 51 al. 3 let. b LPD) ;

- d'utiliser des préréglages favorables à la protection des données conformément à l'art. 7 al. 3 LPD (art. 51 al. 3 let. b LPD) ;
- de procéder à une analyse d'impact sur la protection des données conformément à l'art. 22 LPD (art. 51 al. 3 let. d LPD).

III. DROIT PROCÉDURAL

A. Généralités

18 Les mesures sont édictées par le PFPDT sous forme de décision : D'un point de vue procédural, les dispositions de la PA s'appliquent en principe aux mesures administratives selon l'art. 51 LPD (art. 52 al. 1 LPD). Conformément à l'art. 52 al. 2 LPD, seul l'organe fédéral ou la personne privée contre lequel/laquelle une enquête a été ouverte a qualité de partie. Les personnes concernées par un traitement de données ne sont donc pas parties à l'enquête, même si celle-ci a été déclenchée par leur dénonciation conformément à l'art. 49 al. 1 LPD. En principe, le PFPDT ne notifie ses décisions qu'aux destinataires. Ce n'est que dans les cas d'intérêt général qu'il informe le public (art. 57 al. 2 LPD). Le PFPDT doit motiver ses décisions de manière suffisante pour que les responsables soient en mesure d'évaluer et de mettre en œuvre les mesures ordonnées ou de recourir contre celles-ci. En d'autres termes, la décision doit contenir une instruction d'action concrète qui peut être exécutée en tant que telle. Des injonctions générales selon lesquelles le destinataire de la décision doit adapter son traitement de données de manière à satisfaire aux exigences de la LPD en matière de protection des données ne seraient donc pas suffisamment précises. Si aucune mesure n'est ordonnée après une enquête ou si seul un avertissement est prononcé au sens de l'art. 51 al. 5 LPD, la procédure d'enquête doit néanmoins être formellement close par le PFPDT.

19 Les décisions de mesures prises par le PFPDT en vertu de l'art. 51 LPD peuvent être contestées par l'organe fédéral ou la personne privée qu'elles visent, conformément aux règles générales de la procédure fédérale, par voie de recours auprès du Tribunal administratif fédéral (cf. art. 52 al. 1 LPD en relation avec les art. 44 ss PA). Les décisions sur recours du Tribunal

administratif fédéral sont soumises au recours en matière de droit public devant le Tribunal fédéral (art. 82 let. a en relation avec l'art. 86 al. 1 let. a LTF). Dans ce cas, outre le destinataire de la décision, le PFPDT a également qualité pour recourir (art. 52 al. 3 LPD). Faute de qualité de partie (cf. art. 52 al. 2 LPD et supra n. 18), les personnes concernées n'ont par contre pas qualité pour recourir contre les décisions du PFPDT et les décisions sur recours.

En ce qui concerne l'exécution des mesures administratives ordonnées, les art. 39 à 43 PA s'appliquent à titre complémentaire en vertu du renvoi de l'art. 52 al. 1 LPD. 20

Contrairement à ce qui se passait encore sous l'aLPD, selon laquelle aucun émolument ne pouvait être imposé au responsable du traitement pour l'émission d'une recommandation (cf. art. 33 aLPD), l'art. 59 al. 1 let. d LPD prévoit désormais qu'un émolument est perçu auprès des personnes privées pour l'adoption de mesures au sens de l'art. 51 LPD (cf. également art. 44 OLPD). En l'absence de base légale correspondante, il n'y a toujours pas d'émolument pour les décisions prises à l'encontre d'organes fédéraux (art. 59 al. 1 let. d LPD e contrario ; cf. message 2017, p. 7098). 21

B. Mesures provisoires

Dans le P-LPD de 2017, il était prévu d'habiliter expressément le PFPDT, par un alinéa dans l'article concernant la procédure d'enquête, à ordonner des mesures provisionnelles pour la durée de l'enquête et à les faire exécuter par une autorité fédérale ou par les organes de police cantonaux ou communaux (art. 44 al. 2 P-LPD [2017]). Toutefois, le Parlement ayant supprimé cet alinéa de l'art. 50 LPD, version finale de l'art. 44 P-LPD, la LPD ne confère plus directement au PFPDT la compétence de prendre des mesures provisionnelles pour la durée de ses enquêtes. Désormais, la compétence du PFPDT d'édicter des mesures provisionnelles ne résulte plus qu'indirectement de l'article sur les émoluments, qui déclare à l'art. 59 al. 1 let. d LPD que l'adoption de mesures provisionnelles par le PFPDT à l'encontre de personnes privées est soumise à émoluments. Mais, comme c'était déjà le cas sous l'aLPD, il doit en tout cas être possible d'ordonner des mesures provisoires, voire superprovisoires, dans le cadre d'enquêtes en matière de protection des données ; la suppression de la disposition en question doit être interprétée comme une inadvertance législative et non comme un silence qualifié. 22

23 Alors que sous l'ancien droit, le PFPDT devait s'adresser au Tribunal administratif fédéral pour prendre des mesures provisionnelles, faute de disposer d'une compétence décisionnelle propre (art. 33 al. 2 aLPD), il peut désormais les prendre lui-même.

24 L'art. 33 al. 2 aLPD, qui n'est plus en vigueur sous le nouveau droit, n'attribuait pas seulement au Tribunal administratif fédéral la compétence d'ordonner des mesures provisionnelles dans le cadre d'enquêtes en matière de protection des données, mais il réglait également les conditions et la procédure. Dans le premier contexte, l'art. 33 al. 2 aLPD exigeait que les personnes concernées soient menacées d'un préjudice difficilement réparable. Du point de vue de la procédure, cette disposition déclarait les art. 79-84 PCF applicables par analogie.

25 Après la suppression de l'art. 33 al. 2 aLPD, il n'existe plus de règles de condition et de procédure explicites pour la protection juridique provisoire. En fin de compte, l'appréciation du contenu des mesures provisionnelles dans les enquêtes en matière de protection des données ne devrait guère changer. La PA, applicable à la procédure d'enquête en vertu de l'art. 52 al. 1 LPD, contient uniquement des dispositions relatives à l'adoption de mesures provisionnelles dans la procédure de recours (cf. en particulier les art. 55 et 56 PA), mais pas dans la procédure administrative en amont. L'admissibilité de mesures provisionnelles dans la procédure administrative est toutefois reconnue, puisqu'elle découle directement du principe de l'application du droit matériel. Pour que le PFPDT puisse prendre des mesures provisionnelles dans le cadre d'une procédure d'enquête, il faut d'abord que l'on puisse s'attendre à un préjudice difficilement réparable. Contrairement à ce qui était encore le cas sous l'aLPD, ce préjudice ne doit pas nécessairement menacer les personnes concernées par le traitement des données, même si, dans la pratique, c'est à elles qu'il incombera le plus souvent. En outre, il doit y avoir une urgence correspondante pour l'ordonnance immédiate et celle-ci doit paraître appropriée, nécessaire et proportionnée à l'ensemble des circonstances pour la sauvegarde d'intérêts publics ou privés prépondérants. En tant que mesures provisoires, les mesures provisoires ne doivent pas préjuger de la situation qui sera finalement réglée, ni la rendre impossible. Au moment où les mesures provisoires sont discutées, l'issue de l'enquête relative à la protection des données est encore incertaine et seul un examen sommaire de la situation de fait et de droit peut être effectué. En

conséquence, il convient certes d'établir un pronostic principal au cours de l'examen des mesures provisoires, mais celui-ci ne fait obstacle à une ordonnance provisoire que s'il est clairement négatif.

Le contenu des ordonnances devrait s'orienter sur le catalogue des mesures 26
administratives selon l'article 51 LPD. Il s'agira souvent d'interdire, au moyen d'ordonnances provisoires, des traitements de données potentiellement contraires à la protection des données pendant la durée de la procédure, afin d'éviter des dommages supplémentaires qui pourraient résulter de la poursuite sans changement du traitement en question pendant une enquête parfois complexe et de longue haleine.

BIBLIOGRAPHIE

Baeriswyl Bruno, Kommentierung zu Art. 51 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Baeriswyl Bruno, Der «grosse Bruder» DSGVO und das revDSG: Ein vergleichender Überblick, SZW 2021, S. 8–15 (zit. Baeriswyl DSGVO-Vergleich).

Baeriswyl Bruno, Souveräner Rechtsschutz ist notwendig, digma 2017, S. 38–42 (zit. Baeriswyl Souveräner Datenschutz).

Baeriswyl Bruno, Kommentierung zu Art. 27 aDSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, Bern 2015.

Baeriswyl Bruno, Kommentierung zu Art. 29 aDSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, Bern 2015.

Brunner Stephan C., Mit rostiger Flinte unterwegs in virtuellen Welten? Leitgedanken zur künftigen Entwicklung des schweizerischen Datenschutzrechts, Jusletter 4.4.2011.

Huber René, Kommentierung zu Art. 27 aDSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014.

Huber René, Kommentierung zu Art. 29 aDSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz/Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014.

Huber René, Die Teilrevision des Eidg. Datenschutzgesetzes – ungenügende Pinselrenovation, recht 2006, S. 205–221.

Kugelmann Dieter/Buchmann Antonia, Kommentierung zu Art. 58 DSGVO, in: Schwartmann Rolf/Jaspers Andreas/Thüsing Gregor/Kugelmann Dieter (Hrsg.), Heidelberger Kommentar DS-GVO/BDSG, Heidelberg 2018.

Reudt-Demont Janine/Gordon Clara-Ann/Egli Luisa, Das revidierte Datenschutzgesetz: Wichtigste Neuigkeiten mit Fokus auf Gesundheitsdaten, LSR 2021, S. 264–269.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16.11.2020 (zit. Rosenthal nDSG).

Rosenthal David, Der Entwurf für ein neues Datenschutzgesetz: Was uns erwartet und was noch zu korrigieren ist, Jusletter 27.11.2017 (zit. Rosenthal E-DSG).

Rosenthal David, Kommentierung zu Art. 29 aDSG, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Rudin Beat, Verpasste Chance und Handlungsbedarf: Ein Blick auf die Datenschutzrechts-Reform(en) und die Wirksamkeit der Datenschutzaufsicht, digma 2020, S. 180–187.

Selmayr Martin, Kommentierung zu Art. 58 DSGVO, in: Ehmann Eugen/Selmayr Martin (Hrsg.), Datenschutz-Grundverordnung, München 2017.

Thür Hanspeter, Rolle der Datenschutzbeauftragten: Aufgabe und Instrumente der Datenschutzbehörde im Wandel, digma 2003, S. 80–82.

Walter Jean-Philippe, «Vingt ans de législation sur la protection des données, rétrospectives et perspectives» – L'évolution du droit de la protection des données: perspectives, Jusletter 25.6.2012.

MATÉRIAUX

Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9.12.2011, BBl 2012 S. 335 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2012/86/de/pdf-a/fedlex-data-admin-ch-eli-fga-2012-86-de-pdf-a.pdf, besucht am 28.6.2023.

Botschaft zur Genehmigung des Protokolls vom 10.10.2018 zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 6.12.2019, BBl 2020 S. 565 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2020/60/de/pdf-a/fedlex-data-admin-ch-eli-fga-2020-60-de-pdf-a.pdf, besucht am 28.6.2023.

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 S. 641 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2017/2057/de/pdf-a/fedlex-data-admin-ch-eli-fga-2017-2057-de-pdf-a.pdf, besucht am 28.6.2023.

Bundesgesetz über den Datenschutz, Änderung vom 24.3.2006, BBl 2006 S. 3547 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2006/373/de/pdf-a/fedlex-data-admin-ch-eli-fga-2006-373-de-pdf-a.pdf, besucht am 28.6.2023.

Durchführungsbeschluss 7281/19 des Rates der Europäischen Union zur Festlegung einer Empfehlung zur Beseitigung der 2018 bei der Evaluierung der Anwendung des Schengen-Besitzstands im Bereich des Datenschutzes durch die Schweiz festgestellten Mängel vom 8.3.2019, abrufbar unter https://data.consilium.europa.eu/doc/document/ST-7281-2019-INIT/de/pdf, besucht am 28.6.2023.

Normkonzept zur Revision des Datenschutzgesetzes – Bericht der Begleitgruppe Revision DSG vom 29.10.2014, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/75506.pdf, besucht am 28.6.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 52 LPD

Un commentaire de Nicolas Winkelmann

PROPOSITION DE CITATION

Nicolas Winkelmann, Commentaire de l'art. 52 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la loi fédérale sur la protection des données

Citation abrégée: OK-Winkelmann, art. 52 LPD N. XXX.

Art. 52 Procédure

[1] La procédure d'enquête et les décisions relatives aux mesures visées aux art. 50 et 51 sont régies par la PA.

[2] Seuls l'organe fédéral ou la personne privée contre lesquels une enquête a été ouverte ont qualité de partie.

[3] Le PFPDT a qualité pour recourir contre les décisions sur recours du Tribunal administratif fédéral.

TABLE DES MATIÈRES

En bref 669
I. Remarques générales sur la procédure 669
II. Renvoi à la PA (al. 1) 671
A. Procédure selon la PA contre des particuliers 671
B. Procédure selon la PA contre des organes fédéraux 671
C. Délimitations 674
1. À propos de l'« enquête préalable informelle » 674
2. L'« intervention à seuil bas » 675
3. À propos de la campagne 676
4. Information du public sur les constatations et les décisions 677
5. Conseil 678
D. Dispositions spéciales par rapport à la PA 679
III. Parties à la procédure (al. 2) 679
A. Aperçu 679
B. Les particuliers en tant que partie 680
C. Les organes fédéraux en tant que partie 681
IV. Droit de recours du PFPDT (al. 3) 682
Bibliographie 682
Matériaux 683

EN BREF

L'art. 52, al. 1, LPD définit les règles selon lesquelles le Préposé fédéral à la protection des données et à la transparence (PFPDT) mène les procédures formelles. Cette disposition est une norme de renvoi et stipule que les enquêtes au sens de l'art. 49 LPD ainsi que les décisions rendues en vertu des art. 50 et 51 LPD sont régies par les règles de la PA. A contrario, les autres activités du PFPDT ne sont pas soumises à la PA, notamment les clarifications préalables informelles, les interventions à seuil bas ou les activités de conseil et de surveillance. Il est à noter que la PA est également mentionnée pour les procédures contre des organes fédéraux et que le PFPDT peut « rendre des décisions » à l'encontre de ces derniers selon les règles de la PA. 1

Al. 2, précise que seul l'organe fédéral ou la personne privée contre lequel ou laquelle une enquête a été ouverte a la qualité de partie. Le cercle des parties possibles dans les procédures formelles de l'PFPDT est ainsi restreint par rapport aux dispositions de la PA. 2

Al. 3, constitue la base légale qui accorde à l'PFPDT un droit de recours devant le Tribunal fédéral contre les décisions du Tribunal administratif fédéral. 3

I. REMARQUES GÉNÉRALES SUR LA PROCÉDURE

En vertu de l'aDSG, le PFPDT a mené, de 1993 à 2023, des enquêtes factuelles qu'il a conclues par un rapport final et des recommandations. La PA n'était pas applicable à ces procédures, car le PFPDT n'était pas compétent pour rendre des décisions. Si une telle **recommandation du préposé** n'était pas suivie ou était rejetée, le PFPDT pouvait soumettre l'affaire au Tribunal administratif fédéral pour décision. 4

Avec la révision totale de la LPD, entrée en vigueur le 1er septembre 2023, le PFPDT a désormais une compétence décisionnelle, raison pour laquelle il clôture depuis l'entrée en vigueur de la LPD révisée une procédure formelle par une décision. À l'occasion de la Journée internationale de la protection des données, le PFPDT a publié en janvier 2025 son premier bilan intermédiaire chiffré. Selon ce bilan, le PFPDT a reçu, entre le 1er septembre 2024 et le 21 janvier 2025, 1406 communications pour violation de la LPD, 5

dont 479 étaient en cours de traitement au moment de la publication. Les **mesures de surveillance** se répartissaient comme suit :

- Interventions à bas seuil : 116
- dont environ 90 % ont été suivies volontairement par les responsables
- Enquêtes préliminaires : 16
- Enquêtes en cours / pendantes devant le TAF : 8 / 2
- Campagnes 2

6 Les chiffres publiés montrent que les activités de surveillance du PFPDT ne conduisent qu'à l'ouverture d'une enquête formelle dans des cas isolés et que l'**intervention à bas seuil constitue le principal instrument de surveillance**. Dans la pratique, le PFPDT intervient donc généralement après réception d'une plainte sans ouvrir d'enquête formelle.

7 Les conditions pour l'**ouverture d'une enquête** sont fixées à l'art. 49, al. 1, LPD. Selon cette disposition, le PFPDT ouvre d'office ou sur plainte une enquête lorsqu'il existe des indices suffisants qu'un traitement de données pourrait contrevenir aux dispositions sur la protection des données. Dès que le PFPDT ouvre une enquête en vertu de l'art. 49 LPD, la PA est applicable. C'est le cas dès qu'il a décidé en interne d'ouvrir une procédure. Cela peut intervenir avant, pendant ou après une intervention informelle du PFPDT.

8 Conformément à la pratique, l'ouverture de la procédure est communiquée à la partie par **lettre d'ouverture**. L'ouverture de la procédure ne constitue pas une décision susceptible de recours. Enfin, la procédure est close ou classée par une décision au sens de l'art. 51 LPD.

9 Du point de vue du responsable, il est important de savoir si une procédure a été ouverte ou non. Après l'ouverture de la procédure, les parties sont soumises à l'**obligation de collaborer** sous peine de sanctions pénales (art. 60, al. 2, LPD). A contrario, la collaboration n'est pas obligatoire avant l'ouverture d'une enquête. En cas de refus ou de coopération insuffisante des responsables dans le cadre d'une enquête préliminaire ou d'une intervention à bas seuil, les conditions prévues à l'art. 49 al. 1 LPD sont toutefois régulièrement remplies, de sorte que les faits peuvent être établis sur la base de l'obligation de collaborer (art. 49 al. 3 LPD) ou à l'aide de mesures de contrainte (art. 50 al. 1 LPD). Le PFPDT peut percevoir des émoluments pour

ces actes (art. 59 al. 1 let. d LPD), raison pour laquelle il est généralement dans l'intérêt du responsable de coopérer volontairement avec le PFPDT avant l'ouverture d'une enquête.

Le principe du **droit d'être entendu**, inscrit à l'art. 29, al. 2, Cst. et concrétisé aux art. 29 ss PA, garantit aux parties un droit de participation à la procédure lié à la personnalité. Elles doivent pouvoir s'exprimer sur le fond avant que la décision ne soit rendue, produire des preuves pertinentes, participer à l'administration des preuves ou, à tout le moins, s'exprimer sur le résultat de l'administration des preuves. En d'autres termes, la partie concernée doit avoir la possibilité de prendre position sur les points essentiels avant qu'une décision ne soit rendue. Cela comprend en premier lieu les faits pertinents prévus. En conséquence, les parties ne peuvent se prononcer que sur les faits prévus avant que la décision ne soit rendue ; l'appréciation juridique prévue n'est en revanche pas couverte par le droit d'être entendu. Ce n'est que dans des cas exceptionnels – par exemple lorsque le PFPDT prévoit d'appliquer des dispositions spéciales inattendues – que le droit d'être entendu peut également s'étendre aux dispositions applicables prévues et à la motivation juridique prévue. L'appréciation juridique du PFPDT est communiquée aux parties dans la décision motivée. Si une partie n'est pas d'accord avec la motivation juridique du PFPDT, elle peut former recours. 10

II. RENVOI À LA PA (AL. 1)

A. Procédure selon la PA contre des particuliers

La PA s'applique, en vertu de l'art. 1, al. 1 et al. 2, let. c, PA, aux procédures devant le PFPDT dans lesquelles celui-ci rend une décision en première instance. Il n'y a pas d'exception au sens des art. 2 ss PA. L'art. 52 al. 1 LPD constitue donc une **norme de renvoi déclaratoire** à l'égard des particuliers et sert à clarifier la situation. 11

B. Procédure selon la PA contre des organes fédéraux

Avant la révision totale de la LPD, la surveillance des organes fédéraux et des particuliers était régie par deux dispositions distinctes, qui différaient notamment en ce qui concerne les conditions d'ouverture d'une enquête. Dans la LPD révisée, l'enquête sur les violations des dispositions de la protection des données est désormais réglée dans une section (art. 49 ss) 12

commune aux organes fédéraux et aux particuliers. Il est à noter qu'à quelques exceptions près, **aucune règle différente n'a été légiférée pour la procédure contre les organes fédéraux ou les particuliers**.

13 Selon la jurisprudence constante et la doctrine, sont considérées comme des décisions au sens de l'art. 5 PA les décisions autoritaires, unilatérales, concrètes et individuelles rendues par une autorité en application du droit administratif, qui ont pour but de produire des effets juridiques et qui sont contraignantes et exécutoires. La procédure d'adoption d'une décision présuppose l'existence d'un rapport de souveraineté entre une autorité et un particulier. Les injonctions du PFPDT à l'égard d'autres organes fédéraux ne remplissent donc pas toutes les caractéristiques structurelles de la notion de décision, en raison de l'absence de rapport entre l'autorité et le particulier. Dans la mesure où le PFPDT mène une procédure contre un organe fédéral, la procédure « est régie » par la PA conformément à l'art. 49 LPD, l'art. 52 al. 1 LPD correspondant dans ce domaine à une **norme de renvoi constitutive** et les dispositions de la PA s'appliquant *par analogie*.

14 La **compétence du PFPDT de rendre des décisions à l'encontre d'organes fédéraux** découle, d'une part, du libellé de nombreuses dispositions légales qui visent expressément les organes fédéraux et les particuliers et établissent une distinction pertinente entre les organes fédéraux et les particuliers. D'autre part, le législateur a délibérément harmonisé les procédures à l'encontre des particuliers et des organes fédéraux, qui étaient encore différentes sous l'ancien droit. Enfin, le législateur a aligné les pouvoirs d'enquête et les mesures administratives sur les exigences européennes afin de garantir que la Commission européenne renouvelle ou maintienne sa décision d'adéquation à l'égard de la Suisse, ce qui revêt une importance capitale pour l'économie suisse en particulier.

15 Outre le PFPDT, aucune autre unité administrative ne semble pouvoir statuer sur d'autres unités administratives selon les règles de la PA. Le **Contrôle fédéral des finances**, en tant qu'autorité de surveillance comparable, peut certes demander et faire appliquer des mesures à l'encontre d'autres autorités fédérales qui ne lui sont pas subordonnées hiérarchiquement, mais pas selon les règles de la PA.

16 Selon l'avis défendu ici, une injonction du PFPDT au sens de l'art. 51 LPD à l'encontre d'organes fédéraux équivaut à une **« fausse décision »**, car si, d'une

part, les conditions matérielles d'une décision au sens de l'art. 5 PA ne sont pas remplies, d'autre part, les organes fédéraux se voient imposer *par analogie* les mêmes droits et obligations que les destinataires privés d'une décision. Avec cette norme de renvoi constitutive, le législateur a réglementé de manière pragmatique les règles de procédure que le PFPDT, en tant qu'autorité de surveillance, doit respecter lorsqu'il mène une enquête à l'encontre d'organes fédéraux et qu'il rend et fait exécuter des injonctions contraignantes.

17 Il est à noter que le **projet de révision de la loi sur la protection des données** de 2014 établissait encore une distinction entre les enquêtes menées à l'encontre de particuliers et celles menées à l'encontre d'organes de la Confédération. Il proposait un modèle selon lequel le PFPDT devait d'abord formuler une recommandation à l'organe de la Confédération concerné et ne pouvait rendre une décision qu'après le rejet ou le non-respect de cette recommandation. Cette variante ralentit la procédure en raison d'étapes intermédiaires inutiles. Le rapport explicatif relatif à l'avant-projet de révision totale de la LPD de 2016 ne fait déjà plus de distinction entre les procédures à l'encontre de particuliers et celles à l'encontre d'organes fédéraux.

18 Il convient de distinguer les procédures de PFPDT à l'art. 49 LPD à l'encontre d'organes fédéraux de l'**entraide administrative**. Les autorités fédérales qui collaborent dans le cadre de l'entraide administrative sont sur un pied d'égalité sur le plan organisationnel, de sorte qu'il n'existe aucun rapport de subordination entre elles et que la collaboration se fait dans un esprit de partenariat. Si le PFPDT ouvre une procédure contre un organe fédéral sur la base de l'art. 49 LPD et demande des documents à l'organe fédéral soumis à l'enquête, cela ne relève pas de l'entraide administrative, de sorte que l'art. 36a LTAF n'est pas applicable. Dans le cadre d'une procédure, les autorités fédérales qui font l'objet d'une enquête sont soumises à l'obligation de collaborer, ce qui crée un rapport de subordination dans de tels cas, car c'est le seul moyen pour le PFPDT de contrôler et de faire respecter efficacement les prescriptions en matière de protection des données par les autorités fédérales.

19 L'application par analogie des dispositions de la PA aux procédures contre les organes fédéraux conduit notamment aux différences suivantes par rapport aux procédures à l'encontre des particuliers :

20 La **violation de l'obligation de collaborer** n'est pas punissable pour les organes fédéraux selon le libellé de l'art. 60, al. 2, LPD, qui s'adresse expressément aux seuls particuliers. Cette exclusion est judicieuse, car une application aux organes fédéraux serait totalement contraire au système.

21 Le PFPDT ne peut percevoir **d'émoluments** auprès des organes de la Confédération, en particulier pour l'ordonnance de mesures provisionnelles et de mesures au sens de l'art. 51 LPD. Selon le libellé de l'art. 59, al. 1, LPD, la perception d'émoluments vise exclusivement les particuliers. Cette exclusion est également logique, car la perception d'émoluments auprès des organes de la Confédération serait là encore contraire au système.

22 Selon le texte de la loi, le PFPDT peut également faire appel à d'autres autorités fédérales ainsi qu'aux organes de police cantonaux ou communaux afin de pouvoir exécuter ou faire exécuter les mesures ordonnées en vertu de l'art. 50 al. 1 LPD. Étant donné que les autorités fédérales peuvent faire valoir les droits qui leur sont reconnus par la LPD et la PA et que le PFPDT peut informer le public de la constatation du non-respect de la loi par un organe fédéral en vertu de l'art. 57, al. 2, LPD, cette possibilité ne sera probablement utilisée que dans des situations exceptionnelles. En ce qui concerne le **recours à des moyens de contrainte** au sens de l'art. 50, al. 3, LPD, il n'y a donc aucune différence avec les particuliers, de sorte que, selon l'avis défendu ici, le PFPDT peut également recourir à des moyens de contrainte à l'encontre des organes fédéraux.

23 Concernant la **qualité en tant que partie** des organes fédéraux, voir les explications relatives à l'al. 2.

C. Délimitations

1. À propos de l'« enquête préalable informelle »

24 Avant d'ouvrir une enquête au sens de l'art. 49 LPD et d'appliquer les dispositions de la PA, le PFPDT intervient souvent de manière informelle dans un premier temps. Son intervention fait généralement suite à une plainte ou à des informations parues dans les médias, qui ne contiennent toutefois **pas suffisamment d'indices** pour justifier l'ouverture directe d'une enquête. C'est pourquoi le PFPDT peut, dans un premier temps, examiner s'il existe des indices suffisants pour ouvrir une enquête. Il peut pour cela recourir à

toutes les sources d'information possibles, par exemple examiner des sources publiques ou interroger le ou les responsables, les personnes concernées ou des tiers sur les faits. La phase d'enquête préliminaire relève de l'« activité administrative informelle », au cours de laquelle le PFPDT doit respecter les principes de l'État de droit (cf. art. 5 Cst.) et ne peut agir de manière arbitraire ou en violation du principe d'égalité. Pendant l'enquête préalable informelle, le responsable du traitement n'est soumis à aucune obligation de collaborer et la norme pénale de l'art. 60 al. 2 LPD n'est pas applicable – ces dispositions ne s'appliquent qu'après l'ouverture d'une enquête formelle au sens de l'art. 49 LPD.

L'enquête préalable informelle peut aboutir à la réfutation des indices d'une violation présumée de la protection des données, de sorte que le PFPDT n'a pas à intervenir davantage. C'est régulièrement le cas lorsque, par exemple, les faits ont été exposés de manière imprécise dans la plainte. À défaut, une intervention à seuil bas peut être lancée ou une enquête ouverte. 25

2. L'« intervention à seuil bas »

Il convient de distinguer l'enquête préalable informelle de l'instrument de l'« intervention à seuil bas ». Le terme « intervention à seuil bas » ne figure pas dans la loi, mais a été développé par le PFPDT. Alors que la clarification informelle vise à établir les faits afin de déterminer s'il existe des indices suffisants pour ouvrir une enquête au sens de l'art. 49 LPD, l'intervention à seuil bas poursuit un autre objectif. Elle vise à rétablir la **légalité au moyen de mesures économiques administratives**, telles qu'une simple lettre, en incitant le responsable à prendre volontairement les mesures nécessaires. Toutefois, comme dans le cas de l'enquête préalable informelle, aucune enquête au sens de l'art. 49 LPD n'est ouverte, de sorte que l'intervention à seuil bas doit également être qualifiée d'acte administratif informel et que les dispositions de la PA ne sont pas applicables. Selon l'expérience du PFPDT, les adaptations nécessaires seraient ainsi mises en œuvre en temps utile dans de nombreux cas. Il s'agit ainsi de privilégier une approche axée sur la recherche de solutions et économes en ressources. 26

Par exemple, le PFPDT peut être informé par une communication qu'un responsable n'a pas répondu à une demande de renseignements de la personne à l'origine de la communication. Sur la base d'une ou plusieurs dénonciations de ce type, le PFPDT peut contacter le responsable du 27

traitement et l'inviter à traiter la demande de renseignements concrète de la personne ayant porté plainte et à prendre position sur le déroulement général du traitement des demandes de renseignements. Si la réponse du responsable du traitement permet de conclure qu'à l'avenir, les demandes d'accès seront traitées correctement et dans les délais légaux, il n'est pas nécessaire d'ouvrir une enquête.

28 Si l'intervention à bas seuil ne permet pas de rétablir la conformité avec la protection des données, il existe généralement suffisamment d'indices pour ouvrir une enquête formelle. C'est le cas, par exemple, lorsque, après une intervention à seuil bas, le PFPDT reçoit à nouveau des signalements concernant les mêmes faits. Indépendamment d'une éventuelle intervention en dehors d'une enquête, le PFPDT peut ouvrir une enquête dès qu'il dispose d'indices suffisants.

3. À propos de la campagne

29 Outre la conduite d'enquêtes au sens de l'art. 49 LPD, le PFPDT exerce également des activités de surveillance en vertu de l'art. 4 al. 1 en relation avec l'art. 57 al. 1 let. a, c et g LPD. Le PFPDT qualifie ces activités de campagnes. Du point de vue des responsables, les **enquêtes sont menées en fonction des événements**, tandis que les prises de contact par l'autorité de protection des données peuvent avoir lieu dans le cadre de **campagnes sans événement particulier**. Dans le cadre de campagnes, le PFPDT n'intervient donc pas sur la base d'indices concernant une violation concrète de la protection des données chez un responsable concret, mais parce que des problèmes identiques ou similaires ont été constatés à plusieurs reprises dans un domaine relevant de la protection des données. Afin d'assurer un contrôle et une application efficaces des dispositions en matière de protection des données, le PFPDT peut s'adresser simultanément à plusieurs responsables, attirer leur attention sur les problèmes généraux constatés dans un domaine particulier et leur rappeler les exigences applicables. Il peut également annoncer ses futures mesures de surveillance dans un domaine donné.

30 Le PFPDT n'a encore annoncé aucune campagne. Un coup d'œil en Allemagne montre à quoi pourrait ressembler une telle campagne : dans le cadre de ses activités de surveillance, l'Office bavarois de contrôle de la protection des données (BayLDA) effectue divers contrôles ciblés de la protection des données, c'est-à-dire des contrôles sans motif particulier, mais

axés sur un domaine spécifique. Il a ainsi vérifié le respect des dispositions relatives à la protection des données lors de la recherche de locataires. À cette fin, **des responsables ont été sélectionnés au hasard** et contrôlés de manière ciblée quant au respect des conditions de protection des données lors de la recherche de locataires, en devant répondre à un questionnaire dans un délai légal. Cette intervention se fonde notamment sur l'art. 58, al. 1, let. a, RGPD, selon lequel toutes les informations nécessaires à l'exécution des tâches légales doivent être fournies.

L'activité de surveillance du BayLDA décrite au point précédent peut, selon sa forme concrète, être qualifiée d'**enquête préliminaire informelle ou d'intervention à bas seuil**, mais elle s'adresse **simultanément à plusieurs responsables** dans un domaine déterminé. 31

Contrairement aux autorités européennes de protection des données, qui peuvent, en vertu de l'art. 58, al. 1, let. a, RGPD, exiger toutes les informations nécessaires à l'accomplissement de leurs *tâches légales*, le PFPDT ne peut, en vertu de l'art. 50 al. 1 let. a LPD, ordonner l'accès à toutes les informations, documents, registres des activités de traitement et données personnelles dans la mesure où ceux-ci sont nécessaires à l'*enquête*. Bien que l'art. 50 LPD soit censé satisfaire aux exigences européennes, la **disposition de la LPD a été restreinte par rapport aux dispositions européennes**. Dans le cadre des activités de surveillance du PFPDT, les responsables ne sont pas soumis à l'obligation de collaborer sous peine de sanction prévue à l'art. 60 al. 2 en relation avec l'art. 49 al. 3 LPD et ne sont pas non plus tenus de payer des émoluments (art. 59 al. 1 LPD a contrario). 32

4. Information du public sur les constatations et les décisions

Conformément à l'art. 57 al. 2 LPD, le PFPDT informe le public de ses constatations et décisions dans les cas d'intérêt général. La procédure administrative étant close par la notification de la décision, les dispositions de la PA ne sont plus applicables en vertu de l'art. 52 al. 1 LPD. La **publication** officielle d'une **décision** relève de l'activité administrative proprement dite et n'est donc pas susceptible de recours en tant que **acte réel**. Si le PFPDT et la partie ne s'accordent pas sur la forme ou le mode de publication et que la partie est touchée dans un intérêt digne de protection, une décision susceptible de recours doit être rendue en application de l'art. 25a PA. Cette 33

décision de publication constitue alors une décision au sens de l'art. 5 al. 1 let. c PA, qui oblige la partie à tolérer la publication dans la mesure décidée.

34 Une partie est touchée dans ses **intérêts dignes de protection** lorsqu'elle fait valoir des **secrets d'affaires** ou des **secrets de fonction** qui, selon l'appréciation du PFPDT, n'en constituent pas et ne doivent donc pas, à son avis, être anonymisés ou publiés. Il convient de se référer à la définition de l'art. 7, al. 1, let. g, LTrans.

35 La **communication de données personnelles ou de données de personnes morales** est soumise aux conditions légales correspondantes.

5. Conseil

36 Dans la pratique, la distinction entre un conseil soumis à émolument au sens de l'art. 59 al. 1 let. e LPD et une clarification préalable informelle ou une intervention à seuil bas peut prêter à confusion. Si, dans le cadre d'une enquête préalable informelle ou d'une intervention à seuil bas, le PFPDT indique au responsable du traitement les mesures à prendre pour que l'on puisse conclure à l'absence de violation de la protection des données ou pour qu'il renonce à ouvrir une enquête, ces indications peuvent être qualifiées d'activités de conseil gratuites. D'un point de vue politico-juridique, une telle procédure devient discutable au plus tard lorsque les responsables sont contactés par le PFPDT après que des violations de la protection des données ont été portées à sa connaissance et qu'ils reçoivent des conseils sur la manière de se mettre en conformité avec la protection des données, et que la mise en conformité est ensuite effectuée volontairement et en temps utile, de sorte que le PFPDT renonce à ouvrir une enquête. Au lieu d'une sanction – sous la forme d'une amende par exemple –, les responsables ont ainsi bénéficié d'un conseil juridique gratuit après qu'une violation de la protection des données a été portée à la connaissance du PFPDT. D'un autre côté, cela correspond exactement au sens d'une intervention à bas seuil, raison pour laquelle cette procédure doit être limitée aux violations d'importance mineure au sens de l'art. 49, al. 2, LPD.

D. Dispositions spéciales par rapport à la PA

La LPD contient des **dispositions spéciales** qui, en tant que lex specialis, priment sur la PA. Les plus importantes sont les suivantes 37

- Restriction des parties (art. 52, al. 2, LPD)
- Information de la personne qui a porté plainte (art. 49, al. 4, LPD)
- Obligation de collaborer (art. 49, al. 3, LPD)
- Obtention des preuves (art. 50 al. 1 LPD)
- Obtention des preuves par la contrainte (art. 50 al. 3 LPD)
- Information du public (art. 57 al. 2 LPD)

Les dispositions spéciales de la LPD tiennent compte de la **position particulière du PFPDT** en tant qu'autorité de surveillance, raison pour laquelle les obligations de collaborer et les possibilités d'obtenir des preuves vont plus loin que dans la PA. Il convient de distinguer ces dispositions des droits de collaborer, qui sont régis par les dispositions générales de la PA.

III. PARTIES À LA PROCÉDURE (AL. 2)

A. Aperçu

Selon l'art. 52, al. 2, LPD, seule l'autorité fédérale ou la personne privée contre laquelle une enquête a été ouverte est partie. La qualité de partie est donc réglée différemment à l'art. 52, al. 2, LPD et à l'art. 6 PA. Alors que selon la réglementation de la PA, outre le destinataire de la décision, les organisations privées, les associations et les autorités ou les tiers concernés par l'acte administratif peuvent également être parties, la **qualité en tant que partie** dans la procédure d'enquête du PFPDT est **limitée aux** organes fédéraux ou aux personnes privées contre lesquels ou contre lesquels une enquête a été ouverte. 38

Une procédure peut être menée contre **plusieurs parties**, en particulier lorsque les faits à examiner concernent plusieurs parties. Si plusieurs parties sont impliquées dans un traitement, l'information d'une partie dans le cadre de la procédure peut avoir une incidence négative sur la situation de l'autre partie. Afin de garantir le droit d'être entendu dans de telles configurations, une jonction des procédures s'impose. De telles configurations se produisent 39

par exemple lorsque des traitements sont effectués pour le compte d'un responsable par un sous-traitant.

B. Les particuliers en tant que partie

40 Seule la personne privée contre laquelle une enquête a été ouverte est partie. La qualité de partie est ainsi limitée au destinataire matériel de la décision. La **personne concernée**, même si le PFPDT a ouvert l'enquête à la suite de sa plainte, n'est pas partie à la procédure. Sont considérées comme personnes privées tant les personnes physiques que les personnes morales de droit privé.

41 Toute personne privée peut être partie à une procédure lorsqu'il existe des indices suffisants d'une violation des dispositions sur la protection des données. En effet, dès qu'il ouvre une procédure, le PFPDT peut ordonner des mesures administratives en vertu de l'art. 51 LPD, ce qui affecte les droits et obligations de la partie et remplit les conditions prévues à l'art. 49 LPD et à l'art. 6 PA. Pour ouvrir une procédure à l'encontre d'une personne privée, **aucun traitement de données n'est nécessaire** de sa part. Cela découle des mesures administratives exemplaires prévues à l'art. 51 LPD, selon lesquelles les mesures prévues à l'art. 7 LPD ou une analyse des conséquences en matière de protection des données peuvent être ordonnées avant qu'un traitement de données n'ait lieu. Cela est possible, par exemple, sur la base de dénonciations ou dans le cadre de projets législatifs, ou lorsque le PFPDT a connaissance de projets d'envergure par le biais des médias.

42 Outre le responsable au sens de l'art. 5, let. j, LPD, **les personnes chargées d'un traitement** au sens de l'art. 5, let. k, LPD, un **conseiller à la protection des données** au sens de l'art. 10 LPD et la **représentation** au sens de l'art. 14 LPD peuvent être considérés comme parties à la procédure, pour autant que l'enquête porte sur une violation des dispositions de la protection des données par la personne privée faisant l'objet de l'enquête.

43 La question de la **légitimation passive** d'une partie se pose en particulier dans le cas des **groupes internationaux**, car le responsable du traitement est généralement une personne morale ayant son siège en Irlande. Par exemple, les directives sur la protection des données d'Instagram, Facebook et Threads désignent Meta Platforms Ireland Ltd (MPIL) comme responsable du traitement. MPIL a également désigné un représentant en Suisse et dispose d'une succursale dans ce pays (Facebook Switzerland GmbH). En principe, les

trois entités mentionnées peuvent être parties à la procédure. Selon l'avis exprimé ici, les trois entités mentionnées peuvent également être parties à une procédure, pour autant que l'objet de l'enquête relève de leurs responsabilités respectives.

Par exemple, une procédure contre la succursale de Meta en Suisse est possible. Même s'il est avancé que la succursale suisse n'a rien à voir avec le traitement en question, car elle agit uniquement en tant que laboratoire de recherche pour l'ensemble du groupe, que les droits de propriété intellectuelle appartiennent à une autre entité et que les demandes de suppression sont également traitées par cette dernière, une procédure contre la succursale en Suisse est possible. Selon l'avis défendu ici, un site en Suisse constitue toujours un lien avec le reste du groupe international et est donc responsable du respect des prescriptions suisses, et par conséquent également de la LPD. Même si le site suisse n'est pas habilité, sur le plan organisationnel, à adapter le traitement des données en question, le PFPDT peut au moins constater la violation et obliger la succursale, par voie de décision, à faire adapter le traitement en question pour les personnes concernées en Suisse par l'intermédiaire de l'organe compétent au sein du groupe, conformément à la protection des données. Les groupes internationaux ne doivent pas pouvoir se soustraire aux obligations suisses en matière de protection des données par le biais de leur organisation interne. 44

C. Les organes fédéraux en tant que partie

Un organe fédéral peut également être partie à une procédure en matière de protection des données. Selon l'art. 5, let. i, LPD, un organe fédéral est une autorité ou un service de la Confédération ou une personne chargée d'une tâche publique. La **notion d'organe fédéral** correspond à la définition donnée à l'art. 3, let. h, aDSG. Sont considérés comme organes fédéraux les départements et les offices fédéraux ainsi que leurs divisions et sections. En font également partie les établissements et entreprises fédéraux ainsi que les commandements militaires. Sont également considérées comme organes fédéraux toutes les personnes physiques et morales qui traitent des données pour le compte de la Confédération dans l'accomplissement de tâches de droit public. Les organes des cantons et des communes ne sont toutefois pas considérés comme des organes fédéraux, même s'ils accomplissent des tâches fédérales. 45

46 Dans les procédures qui ne relèvent pas de l'art. 49 LPD, les autorités ou les organes fédéraux n'ont pas qualité de partie au sens de l'art. 6 PA dans les procédures contre des particuliers, en raison du rapport de souveraineté qui les lie à ces derniers, mais ils disposent de compétences similaires et sont désignés comme « instance précédente » dans la procédure de recours. Si le PFPDT ouvre une procédure contre un organe fédéral en vertu de l'art. 49 LPD, cet organe fédéral a, en vertu de la norme de renvoi constitutive, la même position et les mêmes compétences que les particuliers en tant que destinataire matériel de la décision. Par conséquent, l'organe fédéral contre lequel une procédure a été ouverte est partie à la **procédure de recours** et le PFPDT est l'instance précédente.

IV. DROIT DE RECOURS DU PFPDT (AL. 3)

47 Les décisions du PFPDT sont susceptibles de recours conformément à l'art. 44 PA. L'instance de recours est le Tribunal administratif fédéral (art. 47, al. 1, let. b, PA en relation avec les art. 31 et 33, let. d, LTAF). En vertu de l'art. 52 al. 3 LPD, le PFPDT dispose d'un droit de recours contre les décisions du Tribunal administratif fédéral. Il existe ainsi une base légale spéciale au sens de l'art. 89 al. 2 let. d LTF. Pour de plus amples informations, il est renvoyé aux dispositions pertinentes.

L'avis exprimé reflète l'opinion personnelle de l'auteur et n'engage pas le PFPDT.

BIBLIOGRAPHIE

Auer Christoph/Müller Markus/Schindler Benjamin (éd.), VwVG Kommentar, 2e éd., Zurich 2019 (cit. : VwVG-Kommentar, collaborateur/collaboratrice).

Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (éd.), Datenschutzgesetz, Stämpflis Handkommentar, 2e éd., Berne 2022 (cit. SHK-DSG, collaborateur/collaboratrice).

Bieri Adrian/Powell Julian (éd.), Commentaire Orell Füssli sur la loi suisse sur la protection des données et autres dispositions, Zurich 2023 (cit. OFK-DSG, collaborateur/collaboratrice).

Blechta Gabor-Paul/Vasella David (éd.), Datenschutzgesetz/Öffentlichkeitsgesetz, DSG/BGÖ. Commentaire bâlois, 4e édition, Bâle 2024 (cit. BSK-LPD, auteur).

Da Molin Luca/Wesiak-Schmidt Kirsten (éd.), Datenschutz im Unternehmen, Praxishandbuch mit Beispielen und Checklisten, Zurich 2023 (cit. : Datenschutz im Unternehmen, auteur).

Lobsiger Adrian, Hohes Risiko – kein Killerargument gegen Vorhaben der digitalen Transformation, SJZ, 2023, p. 311-319 (cit. Lobsiger, hohes Risiko – kein Killerargument).

Métille Sylvain/Meier Philippe (éd.), Commentaire Romand Loi sur la protection des données (LPD), Bâle 2023 (cit. CR-LPD, auteur).

Rosenthal David, La nouvelle loi sur la protection des données, Jusletter, 16.11.2020 (cit. Rosenthal, nDSG).

Waldmann Bernhard/Krauskopf Patrick (éd.), Praxiskommentar Verwaltungsverfahrensgesetz (VwVG), 3e éd., Fribourg et Zurich 2022 (cit. PK VwVG, collaborateur/collaboratrice).

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 6941 ff., abrufbar https://www.fedlex.admin.ch/eli/fga/2017/2057/de (zit.: Botschaft DSG 2017).

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988 II 413 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/de,
(zit.: Botschaft DSG 1988).

Bundesamt für Justiz BJ, Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderungen weiterer Erlasse zum Datenschutzgesetz, 21.12.2016, abrufbar unter https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/archiv/datenschutzstaerkung.html, (zit.: Erläuternder Bericht Totalrevision DSG).

Bundesamt für Justiz BJ, Normkonzept zur Revision des Datenschutzgesetztes, Bericht der Begleitgruppe Revision DSG, 29.10.2014, abrufbar unter https://

www.bj.admin.ch/bj/de/home/staat/gesetzgebung/archiv/datenschutzstaerkung/berichte.html, (zit.: Normkonzept DSG).

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), 31. Tätigkeitsbericht 2023/2024, abrufbar unter https://www.edoeb.admin.ch/de/taetigkeitsbericht-des-edob, (zit.: EDÖB, 31. Tätigkeitsbericht 2023/2024).

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Untersuchungen von Verstössen gegen Datenschutzvorschriften durch den EDÖB, Anwendung von Art. 49-53 des revidierten Datenschutzgesetztes, Stand: Oktober 2024, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/grundlagen/verstoesse.html,
(zit.: EDÖB Untersuchungen).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 54 LPD

Un commentaire de Florian Roth / Simon Mazidi

PROPOSITION DE CITATION

Florian Roth/Simon Mazidi, Commentaire de l'art. 54 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la Loi fédérale sur la protection des données

Citation abrégée: OK-Roth/Mazidi, art. 54 LPD N. XXX.

Section 3 Assistance administrative

Art. 54 Assistance administrative en Suisse

[1] Les autorités fédérales et cantonales communiquent au PFPDT les informations et les données personnelles nécessaires à l'accomplissement de ses tâches légales.

[2] Le PFPDT communique les informations et les données personnelles nécessaires à l'accomplissement de leurs tâches légales:

a. aux autorités chargées de la protection des données en Suisse;

b. aux autorités de poursuite pénale compétentes, lorsqu'il s'agit de dénoncer une infraction conformément à l'art. 65, al. 2;

c. aux autorités fédérales ainsi qu'aux organes de police cantonaux et communaux, pour l'exécution des mesures prévues aux art. 50, al. 3, et 51.

TABLE DES MATIÈRES

En bref ... 688
I. Généralités ... 688
A. Objet de la réglementation ... 688
B. Historique ... 690
C. But de la norme ... 691
D. Formes de collaboration et importance ... 692
E. Délimitations ... 693
F. Limites ... 695
1. Secret de fonction ... 696
2. Exigences en matière de droits fondamentaux ... 697
3. Principe de finalité ... 698
4. Principe de spécialité ... 698
G. Mise en œuvre et protection juridique ... 698
II. Entraide administrative en faveur du PFPDT (al. 1) ... 702
III. Entraide administrative en faveur d'autres autorités (al. 2) ... 706
A. Assistance administrative aux autorités de protection des données (let. a) ... 707
B. Assistance aux autorités de poursuite pénale (let. b) ... 709
C. Entraide administrative avec les autorités fédérales et les organes de police cantonaux et communaux (let. c) ... 709
Bibliographie ... 711
Matériaux ... 715

EN BREF

L'art. 54 LPDT règle l'entraide administrative entre le PFPDT et les autres autorités fédérales et cantonales. L'entraide administrative revêt une importance considérable pour l'accomplissement des tâches légales du PFPDT. C'est elle qui permet la collaboration entre le PFPDT et les autres autorités fédérales et cantonales, contribuant ainsi de manière essentielle à l'application du droit de la protection des données. L'al. 1 règle l'entraide administrative en faveur du PFPDT, qui est nécessaire à l'exécution de la LPD. L'al. 2 oblige le PFPDT à accorder l'entraide administrative à d'autres autorités. Les autorités envers lesquelles le PFPDT est tenu d'accorder l'entraide administrative sont énumérées de manière exhaustive à l'al. 2.

I. GÉNÉRALITÉS

A. Objet de la réglementation

1 L'art. 54 LPDT règle l'entraide administrative entre le PFPDT et les autres autorités fédérales et cantonales. Cette disposition fait partie des compétences de droit administratif du PFPDT, qui servent à faire respecter la protection des données. Elle constitue en outre une concrétisation de l'art. 58 al. 1 let. b LPD. Elle règle à l'al. 1 l'entraide administrative en faveur du PFPDT, qui est nécessaire à l'exécution de la LPD. L'al. 2 oblige le PFPDT à accorder l'entraide administrative à d'autres autorités, ce qui doit permettre à ces autorités d'accomplir leurs tâches légales respectives dans le domaine d'application de la LPD.

2 L'art. 44, al. 2, 2e phrase, Cst. oblige la Confédération et les cantons à s'accorder l'entraide administrative. L'obligation d'assistance administrative est, d'une part, une manifestation du principe de la collaboration partenariale des autorités au sein de l'Etat fédéral, ancré à l'art. 44 al. 1 Cst. ; la disposition constitutionnelle oblige la Confédération et les cantons à se soutenir mutuellement et à collaborer dans l'accomplissement de leurs tâches. Elle est d'autre part un cas d'application de l'obligation d'assistance mutuelle de l'art. 44 al. 2 phrase 1 Cst. Avant l'entrée en vigueur de la Constitution fédérale totalement révisée de 1999, la Commission fédérale de la protection des données avait déjà désigné l'obligation fondamentale de toutes les autorités de

coopérer en matière d'information comme un principe constitutionnel non écrit du droit suisse. Ce principe constitutionnel trouve désormais son ancrage dans le droit positif à l'art. 44 al. 2 Cst.

La disposition constitutionnelle doit être concrétisée au niveau de la loi. L'art. 54 LPD constitue une telle concrétisation dans la mesure où l'entraide administrative entre le PFPDT et les autorités cantonales est abordée. Il convient de noter que l'art. 44 Cst. ne concerne que l'entraide administrative entre autorités de différentes collectivités publiques et non pas celle entre autorités d'une même collectivité publique. L'art. 54 LPDT constitue donc une base légale autonome en ce qui concerne l'assistance administrative entre le PFPDT et d'autres autorités fédérales. 3

La notion d'assistance administrative n'est pas clairement définie par la loi. L'entraide administrative est généralement comprise comme le soutien mutuel d'unités administratives (qui n'ont aucun lien de subordination entre elles) dans l'accomplissement de leurs tâches légales par des prestations d'aide qui ne sont pas régies par le droit de procédure (civile, pénale ou administrative) (voir N. 15 ss). Elles peuvent être liées à une procédure administrative de première instance, mais pas nécessairement. Les prestations d'aide en dehors ou en amont d'une procédure administrative font également partie de l'assistance administrative. 4

D'une manière générale, toutes les prestations d'aide par lesquelles une autorité administrative de la Confédération ou des cantons soutient une autre autorité administrative de la Confédération ou des cantons dans l'accomplissement de ses tâches légales sont couvertes par l'assistance administrative. En font partie, outre la fourniture d'informations et de données (assistance administrative en matière d'information), la mise à disposition de ressources physiques ou techniques (véhicules, locaux, moyens techniques, etc.). La notion d'autorité administrative doit ici être comprise de manière fonctionnelle et englobe toutes les personnes morales et physiques chargées directement de l'exécution de tâches de droit public de la Confédération, des cantons ou des communes. Dans le cadre de l'art. 54 LPD, l'entraide administrative en matière d'information est au premier plan (voir N. 13). 5

B. Historique

6 L'art. 54 LPD n'a pas donné lieu à des discussions lors du processus législatif. L'entraide administrative en tant que condition nécessaire à l'accomplissement des tâches légales du PFPDT n'était pas contestée. Ainsi, l'avant-projet (art. 46 AP-LPD) contenait déjà une disposition matériellement identique. Sous l'empire de l'ancienne LPD, l'article sur l'entraide administrative n'obligeait le PFPDT qu'à collaborer avec les autorités de protection des données suisses et étrangères (art. 31, al. 1, let. c, aDSG). L'extension de l'entraide administrative à toutes les autorités suite à la révision de la LPD s'inscrit dans le cadre de l'élargissement multiple des compétences du PFPDT sous la LPD révisée.

7 Lors de la procédure de consultation, certains cantons ont critiqué le fait que la charge de travail supplémentaire qui en résulte pour les autorités cantonales et communales n'est pas claire et que les informations à fournir devraient être précisées dans l'ordonnance. Plusieurs participants issus de l'économie ont fait valoir que les secrets d'affaires ou de fabrication ne devaient pas être communiqués dans le cadre d'une procédure d'assistance administrative.

8 La disposition relative à l'assistance administrative nationale (art. 48 P-LPD) ne présentait dans le projet d'acte que quelques modifications rédactionnelles par rapport à l'avant-projet. Ainsi, le libellé de l'al. 1 a été adapté de manière à ce que les autorités fédérales et cantonales communiquent désormais au PFPDT les informations et les données personnelles nécessaires à l'accomplissement de ses tâches légales. Dans l'avant-projet, cette disposition obligeait encore les autorités à communiquer les informations et les données personnelles nécessaires à l'exécution de la présente loi. L'al. 2 let. a a également subi une légère modification rédactionnelle, le PFPDT communiquant désormais aux autorités chargées de la protection des données en Suisse les informations et les données personnelles nécessaires à l'accomplissement de leurs tâches légales. L'avant-projet limitait encore le libellé aux autorités cantonales compétentes en matière de protection des données. Lors des délibérations qui ont suivi au sein des Chambres fédérales, l'assistance administrative nationale n'a plus donné lieu à des discussions ; la disposition a été adoptée dans la version du projet d'acte législatif sans modification matérielle ou rédactionnelle.

Le fait que l'assistance administrative nationale n'ait pas fait l'objet de controverses approfondies peut être attribué à plusieurs facteurs. D'une part, l'utilité de l'assistance administrative nationale pour l'accomplissement des tâches légales est incontestée. En conséquence, Poltier formule simplement et pertinemment : "[...] l'entraide relève de l'évidence [...]". Grâce aux formes de coopération et de collaboration rendues possibles par l'assistance administrative, la protection des données peut être mise en œuvre de manière plus efficace. D'autre part, la disposition relative à l'assistance administrative nationale constitue également une disposition que l'on retrouve dans de nombreuses autres lois fédérales, où elle a également pour but de permettre aux autorités concernées d'accomplir leurs tâches légales. Le fait que le Conseil fédéral parle dans son message d'une disposition standard qui se trouve également dans de nombreuses autres lois fédérales peut tout au plus être compris comme le fait que l'assistance administrative est un instrument largement reconnu dans l'Etat fédéral. Il n'existe en tout cas pas de formulation uniforme dans les différentes lois sectorielles (voir n. 14). Les différentes dispositions règlent la portée de l'assistance administrative de manière trop différente. 9

C. But de la norme

La structure fédéraliste de l'Etat et l'organisation de l'administration en fonction des tâches résultent en une grande spécialisation technique des différentes autorités. Il en résulte une limitation matérielle et géographique de la compétence, qui menace constamment d'entraver l'accomplissement des tâches légales. L'entraide administrative permet de surmonter de telles restrictions de compétence au moyen de prestations d'aide. Ainsi, le PFPDT surveille de manière globale l'application des prescriptions fédérales en matière de protection des données. Des questions de droit de la protection des données se posent également dans le cadre de domaines techniques et juridiques particuliers, dans lesquels une autre autorité fédérale (FINMA, COMCO, etc.) est chargée de la surveillance et de l'exécution. L'entraide administrative est également indispensable en raison de la répartition verticale des compétences entre la Confédération et les cantons : Ainsi, pour faire appliquer les décisions du PFPDT selon l'art. 50 f. LPD, il est généralement fait appel aux autorités cantonales d'exécution (voir art. 50 al. 3 LPD). L'entraide administrative permet l'échange d'informations nécessaire et la collaboration entre les autorités, ce qui permet de garantir l'exécution des 10

mandats légaux malgré la différenciation matérielle et géographique de l'activité des autorités.

11 L'assistance administrative a pour but d'accomplir les tâches publiques de la manière la plus optimale et la plus efficace possible et vise ainsi à permettre et à favoriser une action efficace de l'État. Sur la base de l'art. 54 LPD, le PFPDT peut recourir aux connaissances spécialisées et à l'expérience d'autres autorités pour l'accomplissement de ses tâches légales. Comme le PFPDT peut être confronté à une multitude de questions spécifiques à un domaine, il a souvent besoin d'informations et du soutien d'autres autorités pour mener ses enquêtes de manière correcte et efficace. L'art. 54 LPDT garantit cette collaboration en faveur du PFPDT et contribue ainsi à l'application du droit de la protection des données.

12 Une autre fonction importante de l'entraide administrative est l'obtention de preuves. Dans le cadre de la procédure administrative de première instance menée par le PFPDT, les informations et les documents que le PFPDT a obtenus d'autres autorités suite à l'entraide administrative pour établir les faits pertinents peuvent être utilisés comme moyens de preuve.

D. Formes de collaboration et importance

13 Dans la pratique, les formes de collaboration dans le cadre de l'assistance administrative sont multiples. Dans le cadre de la LPD, l'entraide administrative en matière d'information est au premier plan. Celle-ci comprend la communication de données matérielles et personnelles à d'autres autorités dans le but de soutenir le PFPDT et, inversement, par le PFPDT ; elle est expressément mentionnée à l'art. 54, al. 1 et 2, LPD. En principe, tous les actes de procédure servant à l'établissement des faits (y compris les mesures d'instruction) ou aux actes d'exécution entrent en ligne de compte comme mesures d'entraide administrative. Dans le cadre de l'établissement des faits, les prestations d'aide internes à l'administration telles que la fourniture de renseignements, la consultation de dossiers officiels, la présentation ou l'obtention de documents officiels ou d'autres documents nécessaires, la participation à l'établissement de faits pertinents ou l'accès à une banque de données sont au premier plan. Des interrogatoires ou une inspection peuvent également être effectués à titre de mesures probatoires. L'entraide administrative dans le cadre des mesures d'exécution concerne les mesures qui servent à faire respecter une décision administrative. L'art. 50 al.

3 LPD mentionne expressément les mesures d'entraide administrative en matière de preuve et d'exécution du PFPDT.

Avec l'entraide judiciaire (voir n. 15 ss), l'assistance administrative constitue une condition indispensable pour garantir l'uniformité de l'espace juridique en Suisse. L'assistance administrative revêt une importance considérable pour l'accomplissement des tâches légales du PFPDT. Néanmoins, la constatation de Bellanger, selon laquelle l'assistance administrative nationale "[...] apparaît comme un parent pauvre du droit [...]", n'a rien perdu de sa validité aujourd'hui. Cela s'explique notamment par le fait que l'entraide administrative nationale n'est pas réglementée de manière uniforme au niveau fédéral. La PA évoque certes l'assistance administrative à l'art. 43. Il s'agit toutefois uniquement de l'assistance à l'exécution de décisions des autorités fédérales qui ne visent pas le paiement d'une somme d'argent ou la fourniture de sûretés. En revanche, l'entraide administrative dans le domaine de l'établissement des faits ne relève pas de l'art. 43 PA. Il n'existe pas de réglementation générale régissant aussi bien la procédure que les droits et obligations des parties. Par conséquent, l'entraide administrative est réglée au niveau des différentes lois spéciales. L'étendue de l'obligation d'assistance administrative diffère dans chaque cas, selon la loi spéciale qui s'applique matériellement. Dans le cas présent, l'étendue de l'obligation d'assistance administrative est déterminée en premier lieu par la LPD, en particulier par l'art. 54 al. 1 et 2 ainsi que par l'art. 50 al. 3 en relation avec la LPD. al. 1 LPD. Le champ d'application et les modalités de l'entraide administrative restent à concrétiser dans le détail. 14

E. Délimitations

L'assistance administrative entre autorités suisses (ci-après : assistance administrative) doit être distinguée d'une part de l'entraide judiciaire et d'autre part de l'assistance administrative internationale. Il n'est guère possible de distinguer nettement l'assistance administrative de l'entraide judiciaire. Néanmoins, la délimitation est essentielle en raison des effets juridiques qui y sont liés. Tant le choix du droit applicable - et donc de la procédure - que les limites des mesures et l'organisation concrète de la protection juridique peuvent dépendre de la classification. Au niveau de l'entraide administrative et judiciaire internationale, les différences et leurs conséquences sont marquées : ainsi, l'entraide judiciaire internationale en matière pénale peut, 15

dans des circonstances particulières, entrer dans le champ d'application de l'art. 6 CEDH. Un recours au Tribunal fédéral n'est admissible que pour l'entraide judiciaire internationale en matière pénale et pour l'entraide administrative en matière fiscale, qui présente généralement un objectif de poursuite pénale. A l'exception de l'entraide administrative en matière fiscale, le recours au Tribunal fédéral n'est pas admis contre les décisions prises dans le domaine de l'entraide administrative internationale.

16 Pour délimiter l'entraide administrative et l'entraide judiciaire, la doctrine et la jurisprudence se basent sur différents critères, une combinaison de critères étant parfois utilisée pour la qualification. En particulier, les critères suivants peuvent être mentionnés :

- Le type ou la fonction des autorités impliquées : Si des autorités judiciaires sont impliquées, on parle d'entraide judiciaire. L'assistance administrative, en revanche, concerne les autorités administratives.
- Nature de la procédure soutenue (procédure non contentieuse ou contentieuse ou procédure de décision ou procédure de recours) : L'entraide judiciaire couvre les formes de coopération qui se rapportent à des procédures externes à l'administration. Ces dernières ont lieu devant une autorité extérieure à l'administration et institutionnellement indépendante de celle-ci. L'entraide judiciaire concerne donc principalement des prestations d'assistance en matière de droit procédural (civil, pénal ou administratif) dans le cadre de procédures judiciaires. L'exemple classique est l'exécution de jugements. L'assistance administrative, en revanche, comprend les prestations d'aide entre les autorités administratives de la Confédération et des cantons, qui sont fournies en dehors des procédures définies par le droit de procédure. Elle intervient donc dans le cadre de procédures internes à l'administration ou en dehors d'une procédure administrative et est effectuée à la demande d'une autorité administrative ou spontanément.

17 Si l'on suit ces critères, on peut parler d'entraide administrative lorsque des prestations d'aide sont fournies entre autorités administratives dans le cadre d'une procédure interne à l'administration ou d'une procédure ne relevant pas d'une procédure administrative. En revanche, il y a entraide judiciaire lorsque l'aide est fournie dans le cadre ou à l'appui de procédures - souvent judiciaires - régies par le droit procédural.

La procédure devant le PFPDT étant régie par les art. 49 ss. LPD, il s'agit d'une procédure administrative de première instance non contentieuse - et non d'une procédure (judiciaire) régie par le droit de procédure -, la collaboration des autorités prend la forme d'une entraide administrative. C'est pourquoi l'entraide judiciaire n'est pas non plus abordée à l'art. 54 LPD. L'exécution des mesures (provisionnelles) que le PFPDT peut ordonner dans le cadre d'une enquête relève également de l'entraide administrative. 18

L'art. 54 LPD ne couvre que l'assistance administrative entre autorités suisses. Les prestations d'assistance transfrontalières relèvent de la réglementation sur l'assistance administrative internationale (art. 55 LPD). 19

En outre, toutes les prestations d'aide fournies dans le cadre d'une procédure interne à l'administration ou en dehors d'une procédure administrative ne sont pas couvertes par l'assistance administrative. L'aide fournie dans le cadre de l'assistance administrative sert à l'accomplissement des tâches légales de l'autorité requérante. Les formes générales de coopération ou certains régimes de coopération entre les autorités ne constituent pas une assistance administrative. De telles coopérations existent lorsque différentes autorités sont matériellement compétentes pour traiter une affaire donnée. Dans le champ d'application de la LPD, la coopération est régie par l'art. 53 LPD. 20

Enfin, l'assistance administrative s'adresse toujours à d'autres autorités. Elle ne concerne pas les personnes. Si, dans le cadre d'une enquête, le PFPDT demande l'assistance d'un fonctionnaire disposant de connaissances spécifiques, les dispositions relatives à l'expertise s'appliquent. Sur la base de l'art. 52 al. 1 LPD, ce sont les art. 12 let. e PA en relation avec l'art. art. 57 ss. PCF s'appliquent. 21

F. Limites

L'art. 54 LPD consacre une obligation juridique d'assistance administrative pour les autorités concernées. Les informations et les données personnelles ne peuvent toutefois être échangées que dans la mesure où le secret de fonction le permet et où les exigences de la protection des droits fondamentaux, de la protection des données et de l'assistance administrative, qui se recoupent partiellement, sont respectées. 22

1. Secret de fonction

23 Le secret de fonction est la première limite à l'entraide administrative. Le secret de fonction a été fortement relativisé par le principe de transparence : Sous le régime de la LTrans, les informations doivent soit être explicitement qualifiées de secrètes, soit des intérêts majeurs doivent s'opposer au principe de transparence. Les autorités peuvent désormais transmettre à d'autres autorités toutes les informations qu'elles auraient également dû mettre à la disposition de particuliers en vertu du principe de transparence. Néanmoins, les obligations légales de garder le secret peuvent constituer un obstacle à la communication d'informations en faveur d'autres autorités (art. 36 al. 6 let. b LPD). De telles obligations de garder le secret résultent d'une part du secret de fonction protégé par le droit pénal (art. 320 CP), du secret professionnel (art. 321 CP), du secret de fabrication et d'affaires (art. 162 CP) ou encore du secret fiscal (art. 110 LIFD). D'autre part, le droit du personnel interdit aux employés de la fonction publique de révéler des affaires professionnelles et commerciales qui doivent être tenues secrètes de par leur nature ou en vertu de dispositions légales ou d'instructions (art. 22 LPers en relation avec l'art. 94 OPers). Le secret de fonction s'applique également aux fonctionnaires d'autres services officiels tenus au secret : Il y a donc violation du secret de fonction lorsque le fonctionnaire révèle un secret à un autre office au sein ou en dehors de son département ou à un supérieur hiérarchique auquel il n'est pas directement subordonné. Il n'y a pas de violation du secret de fonction en présence d'un motif justificatif. C'est le cas lorsqu'une loi sectorielle autorise expressément la communication des informations ou que la révélation du secret est autorisée par le consentement écrit des autorités supérieures.

24 L'art. 54 LPD ne se prononce pas expressément sur la question de savoir si cette disposition permet de déroger à l'obligation légale de garder le secret. A notre avis, la disposition ne peut pas être comprise comme une autorisation en blanc de communiquer des obligations légales de garder le secret par le biais de l'entraide administrative, sans quoi l'obligation de garder le secret pourrait être levée par la seule demande d'une autre autorité. En l'absence d'une réglementation légale concrétisante, on peut, selon l'avis défendu ici, se référer à l'art. 36 LPD - par analogie en ce qui concerne les informations autres que les données personnelles. Selon l'al. 6 let. b, les organes fédéraux refusent la communication, la limitent ou l'assortissent de conditions si des obligations légales de garder le secret l'exigent. A notre avis, l'autorité requise

doit donc également procéder à une pesée des intérêts dans le cadre de l'octroi de l'assistance administrative. Si, comme nous l'avons vu, l'art. 54 LPD ne constitue pas à lui seul une base légale suffisante pour la communication d'informations et de données personnelles, la communication n'est autorisée, conformément à l'art. 36 al. 2, que si elle est indispensable à l'accomplissement des tâches légales (let. a) ou s'il existe d'autres motifs tels que le consentement de la personne concernée (let. b). Il convient toujours de mettre en balance l'intérêt à l'entraide administrative et les intérêts contraires au maintien du secret (voir également l'art. 36 al. 6 let. a LPD). Dans le cadre de cette pesée des intérêts ou pour protéger des obligations légales de garder le secret (art. 36 al. 6 let. b LPD), il peut également être indiqué de lier la communication de données personnelles à des conditions ou de rendre les données personnelles anonymes. L'assistance administrative doit en outre être autorisée lorsqu'il existe un autre motif justificatif au sens de l'art. 320 CP, par exemple l'autorisation de l'autorité supérieure (art. 320, ch. 2, CP).

2. Exigences en matière de droits fondamentaux

La protection des droits fondamentaux constitue une autre limite à l'entraide administrative. Ainsi, l'art. 13 al. 2 Cst. protège les données personnelles et les données relatives aux personnes, le domaine matériel de protection comprenant également la communication de telles données à des tiers. Il y a donc généralement atteinte aux droits fondamentaux des personnes concernées lorsque des données personnelles sont communiquées à d'autres autorités. Les prestations d'aide qui, dans le cadre de l'assistance administrative, portent atteinte aux droits fondamentaux de personnes privées doivent satisfaire aux conditions de l'art. 36 Cst. Il découle de l'art. 36 al. 1 Cst. l'exigence d'une base légale suffisante pour l'entraide administrative dans ces cas. Alors que les autorités fédérales - tout comme le PFPDT - doivent respecter la LPD lors de l'entraide administrative, les autorités cantonales qui accordent l'entraide administrative au PFPDT sont soumises aux lois cantonales respectives sur la protection des données. Les autres conditions d'intervention sous forme d'intérêt public prépondérant et de respect de la proportionnalité doivent également toujours être respectées lors de la communication de données personnelles à d'autres autorités. Enfin, même dans le cas d'actes d'entraide administrative qui ne portent pas atteinte aux droits fondamentaux, les autorités sont tenues de respecter les principes de l'action de l'Etat de droit (art. 5 Cst.). Il s'agit par exemple du principe de

25

légalité, de l'exigence de l'intérêt public et du principe de proportionnalité. Le législateur fédéral a repris les conditions constitutionnelles pour la communication de données personnelles dans la loi sur la protection des données et les a encore concrétisées.

3. Principe de finalité

26 En plus de l'exigence d'une base légale en cas de communication de données personnelles, la LPD prévoit une limitation de la finalité (art. 6 al. 3 LPD). La réutilisation de données personnelles suite à l'entraide administrative ne devrait souvent pas être conforme à la finalité de la collecte et du traitement initial des données au regard de la protection des données. Cela n'exclut toutefois pas que des données personnelles soient utilisées ultérieurement à d'autres fins, pour autant qu'il existe une base juridique ou un motif justificatif. L'article 54 LPD, en liaison avec l'article 36 LPD, constitue une telle base légale qui permet aux autorités de s'écarter de la finalité initiale lors de la communication des données personnelles.

4. Principe de spécialité

27 Une autre expression du principe de finalité s'est développée dans le cadre de l'entraide judiciaire et administrative internationale. Tout comme la limitation de la finalité dans le droit de la protection des données, il sert au traitement proportionné des informations et des données personnelles. Cette exigence, connue sous le nom de principe de spécialité, exige que les informations et les données personnelles ne puissent être utilisées par l'autorité requérante qu'aux fins pour lesquelles elles ont été transmises par l'autorité requise. Pour ce faire, l'autorité requérante doit indiquer la finalité pour laquelle les informations ou les données personnelles demandées sont nécessaires. Même si le principe de spécialité n'est souvent abordé que dans le contexte de l'assistance administrative internationale, il est tout aussi pertinent pour l'assistance administrative nationale. La finalité de l'entraide administrative a donc un effet restrictif sur la transmission d'informations et de données personnelles.

G. Mise en œuvre et protection juridique

28 La nature de l'assistance administrative en tant que collaboration partenariale entre autorités implique que les autorités sont placées sur un pied d'égalité sur

le plan organisationnel et qu'il n'existe donc pas de rapport de subordination entre elles. Le PFPDT ne peut pas faire valoir sa demande d'assistance administrative auprès des autorités fédérales ou cantonales par le biais d'une directive ou d'un ordre interne à l'administration. Il ne peut pas non plus imposer la manière dont l'entraide administrative doit être fournie, ni jusqu'à quand et dans quelle mesure ; il en va de même, a contrario, pour l'entraide administrative du PFPDT en faveur d'autres autorités. Les modalités de l'assistance administrative doivent être fixées d'un commun accord entre les autorités impliquées. La situation est différente lorsque le PFPDT ordonne des mesures d'enquête à l'égard d'organes fédéraux conformément à l'art. 50 al. 3 LPD, ces mesures ne relevant alors pas de l'assistance administrative. Dans ce cas, l'organe fédéral ne fournit pas de prestations d'aide au PFPDT, mais est tenu de coopérer en tant que destinataire de l'enquête.

L'entraide administrative a lieu entre les autorités. Si, après examen d'une demande, l'autorité requise refuse de communiquer les informations ou les données personnelles, l'autorité requérante ne peut pas contester la décision. La LPD ne confère pas au PFPDT ou aux autres autorités mentionnées à l'al. 2 un droit de recours particulier au sens de l'art. 48 al. 2 PA. Il est néanmoins concevable que l'autorité requérante, en cas de refus persistant de l'autorité requise, s'adresse à son service supérieur ou à l'autorité de surveillance supérieure par le biais d'un recours en matière de surveillance. Il appartient alors à l'autorité de surveillance de faire respecter l'obligation d'assistance administrative en cas de résistance non fondée et, le cas échéant, de donner les instructions nécessaires à l'autorité requise. Pour les autorités qui n'appartiennent pas à la même collectivité, le recours au Tribunal fédéral est ouvert sur la base de l'art. 120 al. 1 let. b LTF. S'il existe un litige entre le PFPDT et une autorité cantonale d'exécution concernant l'existence et l'étendue de l'obligation d'entraide administrative au sens de l'art. 54 LPD, il est possible de recourir à la voie judiciaire. 29

Même si l'entraide administrative a lieu entre autorités et peut donc être qualifiée d'"[...] acte interne à l'autorité [...]", elle peut avoir un effet réflexe sur les particuliers. Les actes accomplis par les autorités dans le cadre de l'assistance administrative peuvent affecter des positions juridiques ou des intérêts dignes de protection des parties à la procédure ou de tiers. On pense par exemple à la transmission de données personnelles dans le cadre de l'entraide administrative en matière d'information ou à l'application de 30

mesures de contrainte dans le cadre de l'exécution. L'art. 54 LPD ne précise pas si les autorités sont tenues de mener une procédure administrative dans le cadre de l'assistance administrative. Conformément à l'art. 52 al. 1 LPD, la procédure d'enquête est régie par la PA. Il s'ensuit que - si le PFPDT demande l'assistance administrative dans le cadre de la procédure d'enquête - et que cela a des conséquences sur les droits et obligations des personnes concernées, les droits procéduraux garantis par la PA s'appliquent. La décision de l'autorité requise de fournir l'assistance administrative doit être considérée comme une décision lorsque des intérêts dignes de protection de personnes privées sont concernés. Dans ce cas, les personnes privées doivent avoir la possibilité d'intervenir dans la procédure. A cet effet, la personne privée a la qualité de partie et doit être entendue conformément à l'art. 30 PA. La décision d'accorder l'assistance administrative constitue ensuite une décision au sens de l'art. 5 PA, qui doit être motivée et indiquer les voies de recours (art. 35 PA).

31 Selon la doctrine et la jurisprudence, différentes différenciations peuvent être faites en ce qui concerne le moment de l'exercice des droits procéduraux :

- L'autorité requérante n'est pas tenue d'entendre les parties à la procédure ou les tiers lorsqu'elle demande l'assistance administrative à d'autres autorités. La renonciation à une procédure administrative peut être justifiée par la protection juridique accordée ultérieurement dans la procédure principale. Ainsi, la partie à la procédure peut faire valoir ses droits devant le PFPDT en tant qu'autorité requérante à une date ultérieure. Si, dans le cadre de la procédure d'enquête, le PFPDT fonde sa décision sur les informations obtenues par voie d'entraide administrative, il doit en informer la partie à la procédure et lui permettre de consulter le dossier. Sur cette base, la partie à la procédure peut contester l'exactitude des informations ou l'admissibilité de la collecte et de la communication des informations.
- La décision de l'autorité requise d'accorder l'assistance administrative prend en général la forme d'une décision si des intérêts dignes de protection de personnes privées sont concernés. Elle n'est toutefois pas tenue de rendre une décision si elle est tenue de fournir l'assistance administrative et qu'elle ne dispose d'aucune marge d'appréciation. La mise en œuvre d'une procédure administrative est toutefois souvent indiquée. C'est notamment le cas lorsque la disposition légale relative à

l'assistance administrative ouvre une marge d'appréciation, ce qui est envisageable dans un grand nombre de constellations : une telle marge d'appréciation peut se présenter lorsque l'autorité requise doit décider si la communication des informations et des données personnelles est effectivement nécessaire à l'accomplissement de la tâche légale des autorités requérantes. Lors de la communication de données personnelles, il convient en outre, en raison de l'atteinte à l'art. 13 al. 2 Cst., de toujours vérifier la proportionnalité de la transmission et, le cas échéant, d'imposer des conditions ou d'autres restrictions (p. ex. caviardage). Enfin, comme l'art. 54 LPD ne se prononce pas sur les obligations légales de garder le secret, il peut être nécessaire, dans certains cas, de procéder à une pesée des intérêts entre l'indispensabilité de l'aide selon l'art. 36 al. 2 let. a LPD et un éventuel intérêt au maintien du secret qui s'y opposerait. Toutefois, étant donné qu'une protection juridique a posteriori existe également dans ces cas pour les personnes impliquées dans la procédure, la doctrine fait valoir que la mise en œuvre d'une procédure administrative n'est nécessaire que si, au-delà de la marge d'appréciation, il existe un risque de préjudice irréparable. Si ces deux conditions sont remplies, la partie à la procédure devrait se voir offrir le droit d'être entendue, et donc une protection juridique, avant même la décision de l'autorité requise d'accorder l'assistance administrative.

- Enfin, l'autorité requise doit également tenir compte de la position juridique des tiers. Dans la mesure où des données personnelles sont transmises dans le cadre de l'assistance administrative et qu'elles ont une incidence sur les droits et obligations de personnes qui ne sont pas parties à la procédure principale, celles-ci doivent se voir accorder la qualité de partie. Comme il n'existe pas de possibilité de protection juridique a posteriori pour les tiers, les droits procéduraux doivent être respectés dès le moment où les données personnelles sont communiquées. Cela n'est possible que si elles sont entendues au préalable et qu'une décision motivée et susceptible de recours est rendue.

La procédure de recours est régie par la PA. Conformément à l'art. 44 PA, les décisions sont soumises à un recours auprès du Tribunal administratif fédéral. En dernière instance, un recours en matière de droit public peut être déposé auprès du Tribunal fédéral conformément aux art. 82 et suivants LTF. LTF ; les décisions concernant l'assistance administrative interne peuvent faire 32

l'objet d'un recours illimité. Seules les décisions dans le domaine de l'assistance administrative internationale, à l'exception de l'assistance administrative en matière fiscale, sont exclues du recours en matière de droit public. En outre, l'exception de l'art. 83 let. v LTF ne concerne que les décisions du Tribunal administratif fédéral relatives à des divergences d'opinion entre autorités dans le cadre de l'assistance administrative interne. Les recours de parties privées à la procédure ne sont pas concernés.

33 Les actes d'exécution eux-mêmes constituent des actes réels, raison pour laquelle ils ne peuvent en principe pas faire l'objet d'un recours. Dans ce contexte, seul un recours en matière de surveillance est possible. Celui-ci peut être déposé soit auprès de l'autorité de surveillance cantonale compétente, soit auprès du PFPDT. Ce dernier, en tant qu'autorité fédérale requérante, reste compétent pour l'exécution, raison pour laquelle il doit également surveiller la bonne exécution de l'entraide en matière d'exécution par les cantons.

II. ENTRAIDE ADMINISTRATIVE EN FAVEUR DU PFPDT (AL. 1)

34 L'al. 1 pose le principe selon lequel les autorités fédérales et cantonales communiquent au PFPDT les informations et les données personnelles nécessaires à l'accomplissement de ses tâches légales. L'al. 1 a une double nature, puisqu'il autorise d'une part le PFPDT à demander l'assistance administrative à d'autres autorités. D'autre part, il oblige les autorités requises à fournir l'assistance administrative.

35 Les autorités requises sont les autorités fédérales et cantonales. Les autorités communales ne sont pas expressément mentionnées à l'art. 54 al. 1 LPD. Baeriswyl en déduit que les autorités communales ne sont pas tenues d'accorder l'entraide administrative au PFPDT. Une interprétation systématique plaide en faveur de ce point de vue : Les autorités communales sont expressément mentionnées à l'al. 3, mais pas à l'al. 1. En outre, selon une opinion largement répandue, les communes ne sont pas destinataires de l'art. 44 Cst. qui règle les principes de l'assistance administrative dans l'Etat fédéral. Il existe toutefois de bonnes raisons de penser le contraire : d'une part, rien dans les matériaux n'indique que l'assistance administrative nationale de l'art. 54 LPD doive être comprise comme excluant les autorités communales de la

notion d'"autorités cantonales". D'autre part, il semble douteux que l'exclusion des autorités communales soit pertinente au regard de la fonction de l'entraide administrative - à savoir permettre au PFPDT d'accomplir ses tâches dans le cadre d'une application conséquente de la protection des données -, d'autant plus que l'étendue de la délégation de tâches publiques aux communes est laissée à l'appréciation des cantons et que les autorités dont les domaines d'activité sont étendus seraient donc exclues de l'obligation d'entraide administrative. Compte tenu précisément de l'objectif poursuivi, il est logique de supposer que les communes doivent également fournir une assistance administrative au PFPDT.

36 Le contenu et l'étendue des informations à fournir ne sont pas décrits plus précisément à l'al. 1. La disposition parle d'informations et de données personnelles nécessaires à l'accomplissement des tâches légales du PFPDT. En mentionnant expressément les données personnelles, l'al. 1 précise au moins que toutes les informations qui se rapportent à une personne physique identifiée ou identifiable peuvent être communiquées au PFPDT dans le cadre de l'assistance administrative. Cette disposition est complétée par l'art. 39 let. c OLPD, selon lequel le PFPDT peut traiter des données personnelles, y compris des données personnelles sensibles, dans le cadre de la collaboration avec les autorités de la Confédération, des cantons et de l'étranger. La référence aux informations indique clairement que l'art. 54 LPD se réfère à l'assistance administrative en matière d'information. Outre la communication de données personnelles expressément mentionnée, elle vise la transmission de données matérielles (voir n. 13). L'entraide administrative dans le cadre des actes d'exécution est mentionnée à l'art. 50 al. 3 LPD. En raison de la formulation large de l'al. 1, une concrétisation du contenu de la nature des informations et des données personnelles résulte en premier lieu d'une interprétation sur la base des tâches légales du PFPDT.

37 Les tâches légales du PFPDT sont multiples et sont énumérées au chapitre 7 de la LPD. On pense tout d'abord à l'enquête sur les violations des prescriptions de protection des données selon les art. 49 ss. LPD. D'autres tâches du PFPDT consistent à tenir un registre des activités de traitement des organes fédéraux (art. 56 LPD) et à présenter un rapport annuel à l'Assemblée fédérale (art. 57 LPD). L'art. 58 LPD énumère ensuite, de manière non exhaustive, des tâches supplémentaires. Il n'est pas clair d'emblée pour quelles tâches et dans quelle mesure le PFPDT a besoin d'informations et de

données personnelles d'autres autorités. C'est donc la pratique qui montrera dans quelles situations et pour quels actes le PFPDT a besoin de telles informations ou données personnelles pour accomplir une tâche légale. Il est toutefois évident que le PFPDT demandera l'assistance administrative des autorités fédérales ou cantonales lors d'enquêtes sur des violations des prescriptions en matière de protection des données. L'entraide administrative est un instrument central, tant pour l'établissement des faits que pour l'exécution des mesures administratives selon l'art. 51 LPD. Le PFPDT peut par exemple demander aux organes de police cantonaux de l'assister dans l'exécution des mesures d'enquête.

38 La communication d'informations ou de données personnelles mentionnée à l'al. 1 peut se faire spontanément ou sur demande. Le libellé de cette disposition est toutefois beaucoup moins clair que celui de l'art. 112 al. 1 LIFD, par exemple, qui se réfère expressément aux deux formes d'assistance administrative. Il y a entraide administrative spontanée lorsqu'une autorité est légalement tenue d'informer d'office une autre autorité de faits dont elle a connaissance. D'autres autorités peuvent par exemple attirer spontanément l'attention du PFPDT sur le fait qu'un traitement de données effectué par un organe fédéral ou une personne privée pourrait enfreindre les prescriptions en matière de protection des données. En revanche, l'assistance administrative peut également être accordée à la demande du PFPDT. L'assistance administrative sur demande constitue la conception classique de l'assistance administrative.

39 Comme les autres autorités sont tenues de communiquer les informations ou les données personnelles, il s'agit dans ce cas d'une assistance obligatoire qui n'est en principe pas laissée à la discrétion de l'autorité requise. Du point de vue de la formulation ("communiquent"), cette disposition est comparable à l'art. 32, al. 1, LPGA et à l'art. 87, al. 1, LPP, qui prescrivent également une assistance obligatoire. Il convient toutefois de noter qu'une obligation d'assistance administrative n'existe que dans la mesure où la communication des informations et des données personnelles est nécessaire. Cela suppose que l'autorité requise soit habilitée à vérifier la nécessité de la communication. L'entraide administrative ne peut être accordée que si et dans la mesure où le PFPDT ne pourrait pas remplir son mandat légal respectif sans les informations ou les données personnelles, ou seulement au prix d'un surcroît de travail considérable. Par conséquent, Kerboas/Lennman précisent

également qu'une simple amélioration ou une meilleure efficacité dans l'accomplissement de la tâche légale ne peut pas servir de justification à la communication. Si la nécessité n'est pas donnée, il n'y a pas non plus d'obligation de communiquer les informations ou les données personnelles. Tant pour la communication de données personnelles (art. 36 al. 3 Cst.) que pour celle d'informations (art. 5 al. 2 Cst.), cela découle déjà du principe de proportionnalité (voir N. 25). En outre, un refus de l'assistance administrative ou, le cas échéant, une communication assortie de conditions ou de restrictions (p. ex. caviardage) peut se justifier (voir n. 24).

Contrairement aux dispositions relatives à l'assistance administrative contenues dans d'autres lois matérielles (art. 32 al. 1 LPGA, art. 45 al. 1 LN ou art. 87 al. 1 LPP), l'art. 54 LPD ne prévoit pas expressément que l'autorité requérante doit adresser une demande écrite et motivée à l'autorité requise. Une demande écrite et motivée s'impose par exemple lorsqu'il existe un besoin accru de légitimation pour la communication des informations concernées. C'est par exemple le cas en droit des assurances sociales, car la communication de données constitue une dérogation au principe du secret professionnel ; dans la procédure de naturalisation, les données nécessaires à l'appréciation de l'acquisition ou de la perte de la nationalité suisse sont souvent des données personnelles sensibles au sens de l'art. 5 let. c LPD. Un tel besoin de légitimation n'existe pas pour toutes les collectes d'informations du PFPDT. En renonçant à l'exigence d'une demande écrite à l'al. 1, on exprime le fait que les possibilités d'action du PFPDT ne doivent pas être restreintes de manière excessive et qu'il existe un intérêt à ce que l'application de la protection des données soit aussi simple et efficace que possible. Une demande écrite n'est pas obligatoire, notamment lorsque le PFPDT demande des renseignements simples à d'autres services administratifs. Si le PFPDT demande la communication de données personnelles ou si les informations doivent être utilisées dans le cadre d'une enquête sur des violations des prescriptions en matière de protection des données, la demande devrait, selon le point de vue défendu ici, être formulée par écrit - également dans l'optique des droits de protection juridique des personnes concernées (voir N. 30 s.). 40

L'art. 54 LPD ne constitue pas une base pour des renseignements de masse concernant un grand nombre de personnes. Ainsi, sous l'empire de l'ancienne LPD, le PFPDT a déclaré dans une prise de position : "Les communications de 41

données plus étendues, par exemple au moyen de listes (électroniques), et la reprise dans d'autres fichiers exigent une base légale expresse, dans laquelle doivent également être réglées les limites nécessaires des traitements de données et la sécurité". En l'absence d'une autorisation explicite à l'art. 54 LPD, il faut partir du principe que le PFPDT ne peut pas demander ou communiquer des renseignements de masse en rapport avec des données personnelles. De même, il faut partir du principe que les demandes sans motif précis ou question concrète (appelées "fishing expeditions") ne sont pas autorisées dans le cadre de l'entraide administrative sur demande. En se référant à l'art. 19 al. 1 let. a LPD (qui correspond aujourd'hui à l'art. 36 al. 2 let. a LPD), le Tribunal administratif fédéral a par exemple retenu que "[l]'autorité requérante [...] doit exposer les faits pertinents au service sollicité, désigner concrètement les renseignements et documents souhaités et indiquer le motif de la demande [...]". A notre avis, cela vaut également dans le contexte de l'article 54 LPD.

42 Une motivation doit toujours être indiquée, même si cette exigence ne découle pas expressément de l'al. 1 : D'une part, l'autorité requise doit pouvoir évaluer la nécessité de la communication des informations et des données personnelles. D'autre part, le principe de la finalité de l'entraide administrative (principe de spécialité) exige une indication du but dans lequel les informations ou les données personnelles demandées sont nécessaires (voir N. 27). Si l'entraide administrative est accordée à la demande du PFPDT, celui-ci doit donc toujours justifier dans quelle mesure il a besoin des informations ou des données personnelles pour accomplir ses tâches légales dans un cas concret.

III. ENTRAIDE ADMINISTRATIVE EN FAVEUR D'AUTRES AUTORITÉS (AL. 2)

43 Le PFPDT communique des informations et des données personnelles à certaines autorités, dans la mesure où cela est nécessaire à l'accomplissement de leurs tâches légales. L'al. 2 énumère de manière exhaustive les autorités pour lesquelles le PFPDT est tenu de fournir l'assistance administrative.

44 L'art. 54 LPD sert de base légale à l'entraide administrative. Il est donc possible de renvoyer aux explications données à l'al. 1 pour ce qui est du contenu et de l'étendue des données ("informations et données

personnelles"), de la nécessité de les communiquer et des autres modalités. Comme à l'al. 1, l'assistance administrative peut avoir lieu spontanément ou à la demande des autorités mentionnées à l'al. 2. Dans le cadre d'une demande, il s'agit d'une aide obligatoire fournie par le PFPDT. En d'autres termes, la communication d'informations et de données personnelles ne relève pas de son pouvoir d'appréciation. Il faut toutefois que la communication soit nécessaire et qu'aucun autre obstacle ne s'y oppose. Ainsi, le PFPDT est également soumis au secret de fonction selon l'art. 22 LPers.

A. Assistance administrative aux autorités de protection des données (let. a)

L'al. 2, let. a, établit une réciprocité avec les autres autorités de protection des données pour la transmission d'informations et de données personnelles : de même que le PFPDT peut demander à ces autorités des informations et des données personnelles en vertu de l'al. 1, les autres autorités de protection des données peuvent demander des renseignements au PFPDT. Par autorités compétentes en matière de protection des données en Suisse, on entend les autorités dont le mandat légal consiste également à surveiller et à faire respecter la protection des données. Cela découle des bases légales correspondantes au niveau fédéral, cantonal ou communal. 45

Pour concrétiser la notion d'autorités de protection des données, on peut se référer aux exigences de l'article 15 de la Convention 108+. L'art. 15 al. 5 de la Convention 108+ prévoit notamment que l'autorité de contrôle agit en toute indépendance et impartialité dans l'exercice de ses fonctions et de ses compétences et qu'elle n'est pas soumise à des instructions. Dans ce contexte, les autorités indépendantes de protection des données au sens de l'art. 15 al. 5 de la Convention 108+ peuvent être des autorités cantonales et communales indépendantes de protection des données ou d'autres organisations de droit public. 46

Les conseillers à la protection des données des organes fédéraux (art. 10 al. 4 LPD) exercent certes leur fonction vis-à-vis de l'organe fédéral de manière professionnellement indépendante et en étant soumis à des directives, 47

conformément à l'art. 26 al. 1 let. b OLPD. Ils n'ont toutefois pas le statut d'autorité.

- Outre la communication d'informations et de données personnelles à la demande d'une autre autorité dans un cas particulier, un échange d'informations a lieu par le biais des mécanismes et forums institutionnalisés suivants. Ceux-ci assurent un flux d'informations réciproque entre le PFPDT et les autorités cantonales et communales de protection des données et permettent aux autorités de faire part de leurs préoccupations et de leurs connaissances spécialisées.
- Au sein de l'association privatim, les autorités indépendantes de protection des données des collectivités de droit public de Suisse se regroupent pour former la Conférence suisse des Commissaires à la protection des données. Celle-ci encourage la collaboration entre les cantons, les communes et la Confédération dans le domaine de la protection des données par un échange d'informations permanent. L'association s'exprime sur des thèmes liés à la protection des données dans le cadre de prises de position, de réponses à des consultations, de guides ou de fiches techniques. Ainsi, privatim a publié une fiche d'information sur les risques et les mesures spécifiques au cloud et s'est exprimée sur la décision de plusieurs gouvernements cantonaux d'utiliser "Microsoft 365" dans l'administration. De même, l'association a actualisé, en collaboration avec le PFPDT, son guide sur l'application du droit de la protection des données au traitement numérique de données personnelles dans le cadre d'élections et de votations en Suisse. Il s'agit d'une forme générale de collaboration entre les autorités.
- Sur la base de l'art. 111g LIA, de l'art. 102d LAsi et de l'art. 8b LSIP, les autorités cantonales de protection des données et le PFPDT collaborent, dans le cadre de leurs compétences respectives, en vue d'une surveillance coordonnée du traitement des données personnelles dans le cadre de la coopération de Schengen/Dublin. A cette fin, le PFPDT a créé un groupe de coordination des autorités suisses de protection des données dans le cadre de la mise en œuvre des accords d'association. Le groupe de coordination se consacre à l'échange d'informations nécessaires à une surveillance efficace du traitement des données, discute des difficultés d'interprétation et d'application de la législation, analyse les problèmes qui peuvent se poser dans l'exercice de la surveillance ou en rapport avec les

droits des personnes concernées et élabore des propositions et des avis harmonisés en vue de trouver des solutions communes.

B. Assistance aux autorités de poursuite pénale (let. b)

Selon l'art. 65 al. 2 LPD, le PFPDT dispose d'un droit de dénonciation en cas d'infractions présumées aux dispositions pénales du chapitre 8 de la LPD. En revanche, les communications concernant des violations de la sécurité des données au sens de l'art. 24 LPD ne peuvent être utilisées dans une procédure pénale contre la personne soumise à l'obligation de communiquer qu'avec l'accord de cette dernière. 49

Dans l'intérêt d'une mise en œuvre efficace de la protection des données, le PFPDT peut, grâce à ce droit de dénonciation, œuvrer à une application uniforme de la LPD. Il peut se constituer partie civile dans le cadre d'une procédure pénale cantonale. En outre, il peut également contester les décisions de classement et faire appel des décisions cantonales. 50

La dénonciation de l'infraction présumée auprès de l'autorité cantonale de poursuite pénale compétente s'accompagne en général de la communication de données personnelles. Il s'agit de données personnelles sensibles au sens de l'art. 5 let. c ch. 5 LPD. Pour la communication de données personnelles, l'art. 54 al. 2 let. b LPD constitue la base juridique nécessaire. 51

C. Entraide administrative avec les autorités fédérales et les organes de police cantonaux et communaux (let. c)

Selon l'art. 50 al. 3 LPD, le PFPDT peut faire appel à d'autres autorités fédérales ainsi qu'aux organes de police cantonaux ou communaux pour exécuter les mesures prévues à l'art. 50 al. 1 LPD. Les mesures consistent en ce que le PFPDT peut ordonner l'accès à tous les renseignements, documents, listes d'activités de traitement et données personnelles nécessaires à l'enquête (let. a), l'accès à des locaux et installations (let. b), l'audition de témoins (let. c) ou des expertises par des experts (let. d). Cela n'est toutefois possible que s'il a ouvert une enquête et que la personne privée ou l'organe fédéral ne remplit pas son obligation de collaborer. L'entraide administrative par les organes de police cantonaux ou communaux prend la forme d'actes d'exécution qui servent à faire respecter la décision de l'autorité du PFPDT. Cette entraide administrative se fait en faveur du PFPDT et relève donc de l'art. 54 al. 1 LPD. 52

L'art. 54 al. 2 let. c LPD offre la base légale nécessaire pour que le PFPDT puisse transmettre aux autorités mentionnées les informations et les données personnelles nécessaires à l'exécution efficace de ses injonctions.

53 Pour l'exécution des mesures prévues à l'art. 51 LPD, le PFPDT peut également communiquer aux autorités fédérales ainsi qu'aux organes de police cantonaux et communaux les informations et les données personnelles qui sont nécessaires à l'accomplissement de leurs tâches légales. L'art. 51 prévoit des mesures administratives et confère au PFPDT des compétences de décision. Ainsi, selon l'al. 1, il peut décider, en cas de violation des prescriptions de protection des données, d'adapter, d'interrompre ou d'annuler tout ou partie du traitement et d'effacer ou de détruire tout ou partie des données personnelles.

54 A la différence de l'exécution des mesures ordonnées en vertu de l'art. 50 LPD, l'exécution des décisions prises par le PFPDT en vertu de l'art. 51 LPD n'est pas expressément réglée par la LPD. C'est la PA qui s'applique en la matière. Du moins à l'égard des personnes privées, cela découle déjà du fait que le PFPDT a des compétences en matière de décisions, ce qui le soumet à la PA conformément à l'art. 1 al. 2 let. c PA. La PA s'applique déjà, en l'absence de dispositions d'exception applicables selon l'art. 2 f. PA, sont applicables aux procédures administratives du PFPDT. L'art. 52 al. 1 LPD confirme une nouvelle fois expressément l'applicabilité de la PA à la procédure administrative du PFPDT. Cette disposition sert avant tout de clarification.

55 Pour l'exécution des décisions, l'art. 41 PA constitue la base légale nécessaire. Le PFPDT peut recourir à la liste - certes non exhaustive - des mesures d'exécution contenues dans cette disposition. Le PFPDT doit se conformer à la procédure prévue à l'art. 41 PA, qui comprend la menace d'exécution avec fixation d'un (nouveau) délai, la fixation et l'exécution des mesures de contrainte. En cas de péril en la demeure, il peut renoncer à la menace de la mesure de contrainte et à l'octroi d'un délai d'exécution.

56 Si le PFPDT ordonne l'effacement partiel ou total, voire la destruction, et que la personne privée ou l'organe fédéral s'y refuse, il peut, conformément à l'art. 41 al. 1 let. a et let. b PA, faire procéder lui-même à l'effacement ou à la destruction.

57 Pour l'exécution, le PFPDT peut faire appel aux autorités fédérales ainsi qu'aux organes de police cantonaux et communaux. En vertu de l'art. 54 al. 2

let. c LPD, le PFPDT peut transmettre à ces autorités les informations et les données personnelles nécessaires pour qu'elles puissent procéder à l'acte d'exécution.

BIBLIOGRAPHIE

Baeriswyl Bruno, Kommentierung zu Art. 52 DSG: in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2022.

Baeriswyl Bruno, Kommentierung zu Art. 54 DSG: in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2022.

Baeriswyl Bruno, Kommentierung zu Art. 6 DSG: in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2022.

Bellanger François, L'entraide administrative en Suisse, in: Bellanger François/Tanquerel Thierry (Hrsg.), L'entraide administrative, Zürich/Basel 2005, S. 9–28.

Biaggini Giovanni, BV Kommentar, 2. Aufl., Zürich 2017.

Bickel Jürg/Wyssling Markus, Kommentierung zu Art. 41 KG, in: Zäch Roger/Arnet Ruth/Baldi Marino/Kiener Regina/Schaller Olivier/Schraner Felix/Spühler Adrian (Hrsg.), Kommentar, Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen (KG), Zürich 2018.

Bigler-De Mooij Olivier, Kommentierung zu Art. 44 BV, in: Martenet Vincent/Dubey Jacques (Hrsg.), Commentaire Romand, Constitution fédérale, Basel 2021.

Blöchlinger Karin, Amtsgeheimnis und Behördenkooperation, Zum Spannungsfeld von Geheimnisschutz und Verwaltungstätigkeit, Zürich 2015.

Breitenmoser Stephan/Weyeneth Robert, Amts- und Rechtshilfe ist nicht gleich Amts- und Rechtshilfe, in: Fankhauser Roland/Widmer Lüchinger Corinne/Klingler Rafael/Seiler Benedikt (Hrsg.), Das Zivilrecht und seine Durchsetzung, Festschrift für Professor Thomas Sutter-Somm, Zürich 2016, S. 1063–1084.

Diggelmann Oliver, Kommentierung zu Art. 13 BV, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar, Bundesverfassung, Basel 2015.

Egli Patricia, Kommentierung zu Art. 44 BV, in: Ehrenzeller Bernhard/Egli Patricia/Hettich Peter/Hongler Peter/Schindler Benjamin/Schmid Stefan G./Schweizer Rainer J. (Hrsg.), St. Galler Kommentar, Bundesverfassung, 4. Aufl., Zürich 2023.

Gächter Thomas/Egli Philipp, Informationsaustausch im Umfeld der Sozialhilfe, in: Jusletter 6.9.2010.

Gächter Thomas/Egli Philipp, Kommentierung zu Art. 41 VwVG, in: Auer Christoph/Müller Markus/Schindler Benjamin (Hrsg.), Kommentar, Bundesgesetz über das Verwaltungsverfahren (VwVG), 2. Aufl., Zürich 2019.

Gächter Thomas/Egli Philipp, Kommentierung zu Art. 43 VwVG, in: Auer Christoph/Müller Markus/Schindler Benjamin (Hrsg.), Kommentar, Bundesgesetz über das Verwaltungsverfahren (VwVG), 2. Aufl., Zürich 2019.

Gerschwiler Stefan, Kommentierung zu Art. 54 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar, DSG, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023.

Häberli Thomas, Kommentierung zu Art. 83 BGG, in: Niggli Marcel Alexander/Uebersax Peter/Wiprächtiger Hans/Kneubühler Lorenz (Hrsg.), Basler Kommentar, Bundesgerichtsgesetz, 3. Aufl., Basel 2018.

Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich 2020.

Harrendorf Stefan/König Stefan/Voigt Lea, Kommentierung zu Art. 6 EMRK, in: Meyer-Ladewig Jens/Nettesheim Martin/von Raumer Stefan (Hrsg.), Handkommentar, Europäische Menschenrechtskonvention, 5. Aufl., Baden-Baden 2023.

Jaag Tobias, Die Rechtsstellung der Kantone in der Bundesverfassung, in: Thürer Daniel/Aubert Jean-François/Müller Jörg Paul (Hrsg.), Verfassungsrecht der Schweiz, Zürich 2001, S. 473–489.

Jaag Tobias/Häggi Furrer Reto, Kommentierung zu Art. 41 VwVG, in: Waldmann Bernhard/Weissenberger Philippe (Hrsg.), Praxiskommentar, Verwaltungsverfahrensgesetz, 2. Aufl., Zürich 2016.

Jaag Tobias/Häggi Furrer Reto, Kommentierung zu Art. 43 VwVG, in: Waldmann Bernhard/Weissenberger Philippe (Hrsg.), Praxiskommentar, Verwaltungsverfahrensgesetz, 2. Aufl., Zürich 2016.

Kerboas Cécile/Lennman Catherine, Kommentierung zu Art. 54, in: Meier Philippe/Métille Sylvain (Hrsg.), Commentaire Romand, Loi fédérale sur la protection des données, Basel 2023.

Kiener Regina/Rütsche Bernhard/Kuhn Mathias, Öffentliches Verfahrensrecht, 2. Aufl., Zürich 2015.

Kieser Ueli, Kommentar zum Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts ATSG, 4. Aufl., Zürich 2020.

Kölz Alfred/Häner Isabelle/Bertschi Martin, Verwaltungsverfahren und Verwaltungsrechtspflege des Bundes, 3. Aufl., Zürich 2013.

Mayhall Nadine, Kommentierung zu Art. 1 VwVG, in: Waldmann Bernhard/Weissenberger Philippe (Hrsg.), Praxiskommentar, Verwaltungsverfahrensgesetz, 2. Aufl., Zürich 2016.

Mund Claudia, Kommentierung zu Art. 36 DSG: in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2022.

Oberholzer Niklaus, Kommentierung zu Art. 320 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafrecht, 4. Aufl., Basel 2019.

Plüss Kaspar, Kommentierung zu § 7 VRG, in: Griffel Alain (Hrsg.), Kommentar zum Verwaltungsrechtspflegegesetz des Kantons Zürich (VRG), 3. Aufl., Zürich 2014.

Poltier Etienne, L'entraide administrative interne, in: Poltier Etienne/Favre Anne-Christine/Martenet Vincent (Hrsg.), L'entraide administrative, Évolution ou révolution?, Zürich 2019, S. 61–102.

Raselli Niccolò, Amts- und Rechtshilfe durch Informationsaustausch zwischen schweizerischen Straf- und Steuerbehörden, ZStrR 1993, S. 26–55.

Reinhardt Klaus, Über Amtsgeheimnis und Amtshilfe in kantonalen Verwaltungssachen, in: Regierungsrat des Kantons Solothurn (Hrsg.), Festgabe Alfred Rötheli zum fünfundsechzigsten Geburtstag, Solothurn 1990, S. 527–558.

Rosenthal David, Der Entwurf für ein neues Datenschutzgesetz, Jusletter 27.11.2017.

Schweizer Rainer J., Anforderungen der EGMR-Rechtsprechung an die internationale Amts- und Rechtshilfe, in: Lorandi Franco/Staehelin Daniel, Innovatives Recht, Festschrift für Ivo Schwander, Zürich 2011, S. 985–1010.

Schweizer Rainer J., Kommentierung zu Art. 44 BV, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J./Vallender Klaus A. (Hrsg.), St. Galler Kommentar, Bundesverfassung, 3. Aufl., Zürich 2014.

Simon Jürg Walter, Amtshilfe, Allgemeine Verpflichtungen, Schranken und Grundsätze, Chur/Zürich 1991.

Thurnherr Daniela, Verfahrensgrundrechte und Verwaltungshandeln, Zürich/St. Gallen 2013.

Tschannen Pierre/Müller Markus/Kern Markus, Allgemeines Verwaltungsrecht, 5. Aufl., Bern 2022.

Vest Hans, Kommentierung zu Art. 32 BV, in: Ehrenzeller Bernhard/Egli Patricia/Hettich Peter/Hongler Peter/Schindler Benjamin/Schmid Stefan G./Schweizer Rainer J. (Hrsg.), St. Galler Kommentar, Bundesverfassung, 4. Aufl., Zürich 2023.

Waldmann Bernhard/Kraemer Raphael, Kommentierung zu Art. 44 BV, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar, Bundesverfassung, Basel 2015.

Wermelinger Amédéo, Informationelle Amtshilfe: Verunmöglicht Datenschutz eine effiziente Leistungserbringung durch den Staat? Analyse des eidgenössischen und des luzernischen Rechts, ZBl 105 (2004) S. 173–205.

Wiederkehr René/Meyer Christian/Böhme Anna, Orell Füssli Kommentar, VwVG Kommentar, Bundesgesetz über das Verwaltungsverfahren und weiteren Erlassen, Zürich 2022.

Zobl Martin/Roth Florian/Mazidi Simon, Kommentierung zu Art. 52 DSG, in: Blechta Gabor/Vasella David (Hrsg.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz (im Erscheinen).

MATÉRIAUX

Botschaft über die Anpassung und Harmonisierung der gesetzlichen Grundlagen für die Bearbeitung von Personendaten in den Sozialversicherungen, BBl 2000 255 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2000/99/de/pdf-a/fedlex-data-admin-ch-eli-fga-2000-99-de-pdf-a.pdf, besucht am 29.9.2023.

Botschaft über eine neue Bundesverfassung vom 20.11.1996, BBl 1997 I 1 ff., abrufbar unter https://www.amtsdruckschriften.bar.admin.ch/viewOrigDoc/10054111.pdf?id=10054111&action=open, besucht am 28.9.2023.

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2017/2057/de/pdf-a/fedlex-data-admin-ch-eli-fga-2017-2057-de-pdf-a.pdf, besucht am 28.9.2023.

Botschaft zur Totalrevision des Bundesgesetzes über das Schweizer Bürgerrecht (Bürgerrechtsgesetz, BüG), BBl 2011 2825 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2011/422/de/pdf-a/fedlex-data-admin-ch-eli-fga-2011-422-de-pdf-a.pdf, besucht am 29.9.2023.

Bundesamt für Justiz, Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016, abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf.download.pdf/vn-ber-d.pdf, besucht am 1.8.2023 (zit. als Erl. Bericht VE).

Bundesamt für Justiz, Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens vom 10.8.2017, abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/

ve-ber-d.pdf.download.pdf/ve-ber-d.pdf, besucht am 9.7.2023 (zit. als Ergebnisse Vernehmlassungsverfahren DSG).

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, 28.1.1998, in: VPB 62 (1998) Nr. 43, S. 376 ff.

Urteil der Eidgenössischen Datenschutzkommission vom 10.1.1997, in: VPB 62 (1998) Nr. 40, S. 328 ff.

Urteil der Eidgenössischen Datenschutzkommission vom 9.5.1996, in: VPB 62 (1998) Nr. 39, S. 318 ff.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 55 LPD

Un commentaire de Florian Roth / Simon Mazidi

PROPOSITION DE CITATION

Florian Roth/Simon Mazidi, Commentaire de l'art. 55 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (édit.), Commentaire en ligne de la Loi fédérale sur la protection des données

Citation abrégée: OK-Roth/Mazidi, art. 55 LPD N. XXX.

Art. 55 Assistance administrative avec des autorités étrangères

[1] Le PFPDT peut échanger des informations ou des données personnelles avec des autorités étrangères chargées de la protection des données personnelles pour l'accomplissement de leurs tâches légales respectives en matière de protection des données, pour autant que les conditions suivantes soient réunies:

a. la réciprocité en matière d'assistance administrative est garantie;

b. les informations et les données personnelles échangées ne sont utilisées que dans le cadre de la procédure liée à la protection des données personnelles qui a donné lieu à la demande d'assistance administrative;

c. l'autorité destinataire s'engage à ne pas divulguer les secrets professionnels, d'affaires ou de fabrication;

d. les informations et les données personnelles ne sont communiquées à des tiers qu'avec l'accord préalable de l'autorité qui les a transmises;

e. l'autorité destinataire s'engage à respecter les charges et les restrictions d'utilisation exigées par l'autorité qui lui a transmis les informations et les données personnelles.

2 Pour motiver sa demande d'assistance administrative ou pour donner suite à une demande d'assistance administrative de l'autorité requérante, le PFPDT peut communiquer notamment les indications suivantes:

a. l'identité du responsable du traitement, du sous-traitant ou de tout autre tiers participant au traitement;

b. les catégories de personnes concernées;

c. l'identité des personnes concernées lorsque:

celles-ci ont donné leur consentement, ou que
la communication de l'identité des personnes concernées est indispensable à l'accomplissement des tâches légales du PFPDT ou de l'autorité étrangère;

d. les données personnelles ou les catégories de données personnelles traitées;

e. la finalité du traitement;

f. les destinataires ou les catégories de destinataires;

g. les mesures techniques et organisationnelles.

3 Avant de transmettre à une autorité étrangère des informations susceptibles de contenir des secrets professionnels, de fabrication ou d'affaires, il informe les personnes physiques ou morales détentrices de ces secrets et les invite à prendre position, à moins que cela ne s'avère impossible ou ne nécessite des efforts disproportionnés.

TABLE DES MATIÈRES

En bref ... 720
I. Généralités ... 720
A. Objet de la réglementation ... 720
1. Base ... 720
2. Contexte international ... 721
B. Genèse ... 723
C. But de la norme ... 724
D. Délimitations ... 725
1. Assistance administrative nationale ... 725
2. Distinction par rapport à l'entraide judiciaire ... 726
3. Simple coopération administrative ... 727
E. Formes de coopération ... 728
1. Formes de coopération ... 728
2. Coopération multilatérale ... 729
3. Traités internationaux ... 730
F. Limites ... 730
G. Protection juridique ... 733
II. Conditions (al. 1) ... 736
A. Généralités ... 736
1. Autorités compétentes ... 736
2. Étendue et contenu ... 737
3. Nature juridique ... 737
B. Conditions de recevabilité ... 737
1. Réciprocité (let. a) ... 738
2. Principe de spécialité (let. b) ... 738
3. Principe de confidentialité (let. c) ... 740
4. Principe de la longue main (let. d) ... 741
5. Respect des conditions et des restrictions (let. e) ... 742
III. Communication de données personnelles (al. 2) ... 743
IV. Obligation d'informer et prise de position (al. 3) ... 744
Bibliographie ... 746
Matériaux ... 751

EN BREF

L'art. 55 LPD régit l'entraide administrative internationale entre le PFPDT et les autorités étrangères chargées de la protection des données. Cette disposition permet la coopération transfrontalière entre les autorités de protection des données et contribue ainsi de manière significative à l'application du droit en matière de protection des données. L'al. 1 régit les conditions dans lesquelles le PFPDT peut échanger des informations ou des données personnelles avec des autorités étrangères. L'al. 2 détermine les informations que le PFPDT est autorisé à communiquer dans le cadre d'un tel échange. L'al. 3 définit les droits de certaines personnes susceptibles d'être concernées par une mesure d'entraide administrative.

I. GÉNÉRALITÉS

A. Objet de la réglementation

1. Base

1 L'entraide administrative internationale a pour but l'assistance **réciproque et transfrontalière des autorités compétentes en matière de protection des données** (ci-après : autorités de protection des données) dans l'accomplissement de leurs tâches légales, par le biais d'une aide fournie en dehors d'une procédure régie par le droit procédural. L'art. 55 LPD régit l'entraide administrative internationale entre le PFPDT et les autorités étrangères de protection des données.

2 L'art. 55 est une **nouvelle disposition** de la LPD. La disposition précédente (art. 31, al. 1, let. c, aLPD) obligeait uniquement le PFPDT à collaborer avec les autorités étrangères chargées de la protection des données. Il s'agissait notamment d'un échange technique sur des thèmes spécifiques ou d'une collaboration régulière au sein d'organes, de groupes de travail ou de conférences. Cette disposition n'offrait toutefois pas une base légale suffisante au PFPDT pour coopérer avec les autorités étrangères et échanger des informations dans le cadre de la surveillance et du contrôle du droit fédéral en matière de protection des données. Néanmoins, le PFPDT a déjà coopéré pleinement avec les autorités étrangères de protection des données dans le

cadre de l'aDSG. À l'époque, l'échange transfrontalier de données était largement régi par les règles générales de l'entraide administrative, qui se fondaient principalement sur les obligations découlant du droit international public (art. 13 ss de la Convention 108).

L'art. 55 LPD établit désormais **de véritables règles de procédure** en régissant les conditions de l'échange d'informations ou de données personnelles avec les autorités étrangères (al. 1) ainsi que les données pouvant être transmises (al. 2). L'al. 3 accorde ensuite aux détenteurs d'un secret professionnel, d'affaires ou de fabrication le droit d'être informés et la possibilité de prendre position lorsque le PFPDT communique à une autorité étrangère des informations susceptibles de contenir de tels secrets. 3

L'art. 55 LPD s'inscrit dans le cadre de l'**harmonisation avec le droit européen**. L'art. 50 de la directive (UE) 2016/680 exige que les autorités de contrôle se prêtent mutuellement assistance. Parallèlement, cette disposition satisfait aux exigences de l'art. 61 DSGVO et des art. 16 à 21 de la Convention 108+. 4

2. Contexte international

L'objectif de la Convention 108+ est de créer un niveau uniforme de protection des données et de renforcer les **mécanismes d'application**. Cela inclut notamment la coopération transfrontalière entre les autorités de contrôle. La Suisse a ratifié la Convention 108+ le 7 septembre 2023. Pour entrer en vigueur, la Convention 108+ doit être ratifiée par 38 États contractants. Au printemps 2025, ce nombre n'était pas encore atteint. Lors des références ultérieures à la Convention 108+, il convient donc de tenir compte du fait qu'elle n'est pas encore entrée en vigueur. Son entrée en vigueur prochaine semble toutefois probable. 5

La Convention 108+ oblige les parties contractantes à coopérer et à s'entraider dans la mise en œuvre de la convention. Elle prévoit différentes formes de coopération, sans que cette liste soit exhaustive. En premier lieu, les autorités de contrôle se prêtent mutuellement assistance, notamment en échangeant toutes les **informations pertinentes et utiles**. Il peut s'agir de deux types d'informations : 6

- L'**échange général d'informations et de documents** sur le droit et la pratique administrative dans le domaine de la protection des données. Cet

échange ne devrait poser aucun problème, car les informations peuvent être échangées librement et rendues publiques.

- L'**échange d'informations confidentielles**, y compris de données à caractère personnel. En ce qui concerne les données à caractère personnel, la Convention 108+ prévoit qu'elles ne peuvent faire l'objet d'un traitement que si elles sont d'une importance cruciale pour la coopération (c'est-à-dire si, sans leur fourniture, la coopération serait inefficace) ou si la personne concernée a donné son consentement explicite, libre et éclairé, en se référant au cas concret. Dans le cas contraire, l'échange de données à caractère personnel issues d'un traitement concret est exclu.

7 Outre l'échange d'informations pertinentes et utiles, les objectifs de la coopération peuvent également être atteints par des **enquêtes concertées**, telles que des enquêtes ou des opérations coordonnées, ainsi que par la mise en œuvre de mesures communes.

8 Les autorités de contrôle sont tenues de donner suite aux demandes qui leur sont adressées par d'autres autorités de contrôle. L'art. 20 de la Convention 108+ prévoit de manière exhaustive le **refus d'une demande** uniquement si celle-ci n'est pas compatible avec les compétences de l'autorité de contrôle (let. a), si elle n'est pas conforme aux dispositions de la Convention 108+ (let. b) ou si l'exécution de la demande n'est pas compatible avec la souveraineté, la sécurité nationale ou l'ordre public (par exemple pour garantir la confidentialité des enquêtes policières) de la partie contractante ou avec les droits et libertés fondamentaux des personnes relevant de la juridiction de cette partie contractante (let. c).

9 Au niveau du droit de l'Union, il existe deux actes juridiques pertinents en matière de protection des données. Le **DSGVO** est le texte fondamental en matière de protection des données et régit la protection des données traitées dans le cadre du marché intérieur. Son article 61 régit en détail l'assistance administrative entre les autorités de contrôle des États membres de l'UE ou de l'EEE, sans qu'il soit nécessaire de conclure des accords particuliers entre les États membres dans des cas individuels. L'assistance administrative internationale est régie par l'art. 50, let. b, DSGVO. La DSGVO ne fait pas partie de l'acquis de Schengen et n'est donc pas contraignant pour la Suisse.

10 La **directive (UE) 2016/680** vise à protéger les données à caractère personnel traitées à des fins de prévention, de recherche, de détection ou de poursuite

d'infractions pénales ou à des fins d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de celles-ci. Étant donné que la directive (UE) 2016/680 s'inspire de la DSGVO, les deux actes juridiques contiennent des dispositions largement similaires. La directive fait partie de l'acquis de Schengen. En tant qu'État associé à Schengen, la Suisse est tenue d'accepter, de transposer et d'appliquer les développements de l'acquis de Schengen, la transposition en Suisse ayant été effectuée dans le cadre de la révision totale de la LPD en ce qui concerne l'autorité de contrôle. L'obligation d'assistance mutuelle des autorités de contrôle est prévue à l'art. 50 de la directive (UE) 2016/680.

B. Genèse

Dans l'**avant-projet** de LPD, la disposition relative à l'entraide administrative internationale (art. 47 AP-LPD) était encore divisée en deux alinéas, le premier régissant les demandes d'entraide administrative adressées par le PFPDT aux autorités étrangères et le second l'entraide administrative fournie par le PFPDT aux autorités étrangères. Le premier paragraphe définissait les informations que le PFPDT était autorisé à communiquer aux autorités étrangères afin d'obtenir leur assistance administrative ; le second paragraphe fixait les conditions dans lesquelles le PFPDT pouvait fournir une assistance administrative aux autorités étrangères. 11

Dans le cadre de la **procédure de consultation**, certains participants ont fait valoir que la systématique de l'art. 47 était lacunaire. Ainsi, les conditions applicables à la communication d'informations ne seraient pas les mêmes selon que le PFPDT est l'autorité requérante ou l'autorité requise. Plusieurs participants se sont finalement prononcés en faveur de l'interdiction de communiquer des informations constituant des secrets d'affaires ou de fabrication dans le cadre d'une procédure d'entraide administrative entre le PFPDT et une autorité étrangère de protection des données, sans que la protection de ces secrets soit garantie ou que le détenteur du secret ait donné son accord. 12

La systématique de la disposition a subi une modification fondamentale dans le **projet de** LPD et après la consultation (art. 49 P-LPD). Au lieu de soumettre les demandes d'entraide administrative du PFPDT aux autorités étrangères et l'entraide administrative du PFPDT en faveur des autorités étrangères à des réglementations différentes, les conditions préalables à 13

l'échange d'informations ou de données personnelles avec les autorités étrangères ont été harmonisées à l'al. 1 et la communication de données personnelles à l'al. 2. L'al. 2 régit ainsi de manière uniforme les informations que le PFPDT est autorisé à communiquer à l'autorité étrangère pour motiver sa demande d'entraide administrative ou pour donner suite à la demande d'une autorité étrangère. Les modifications ont également entraîné un durcissement : le projet a ainsi été complété par l'exigence de réciprocité (art. 49, al. 1, let. a, P-LPD) et un nouvel al. 3 a été ajouté concernant les secrets professionnels, d'affaires ou de fabrication. Les réserves émises lors de la consultation concernant la systématique et la communication des secrets d'affaires et de fabrication semblent ainsi avoir été entendues.

14 Lors des **débats qui ont suivi** au sein des Chambres fédérales, l'entraide administrative internationale n'a plus donné lieu à discussion ; la disposition a été adoptée dans la version du projet de loi avec seulement quelques modifications rédactionnelles mineures.

C. But de la norme

15 Compte tenu du caractère **de plus en plus transfrontalier du traitement des données**, la coopération internationale entre les autorités de protection des données revêt une importance croissante. L'augmentation quantitative du traitement transfrontalier des données personnelles a accru le risque d'atteintes à la vie privée et à la protection des données en général. Pour parer à ce risque, une coopération efficace et étroite sous la forme d'une entraide administrative internationale est indispensable. L'accent est mis sur l'assistance mutuelle des autorités chargées de la protection des données : Dans le cadre de leurs activités de surveillance et de conseil, elles ont pour mission de garantir le respect des dispositions applicables en matière de protection des données, y compris dans un contexte transfrontalier, et de préserver ainsi efficacement les droits des personnes concernées.

16 L'art. 55 LPD constitue la **base légale** permettant au PFPDT de collaborer avec les autorités étrangères de protection des données et d'échanger des informations et des données personnelles dans le cadre de ses activités de surveillance. Cela permet au PFPDT d'exercer son activité de surveillance également dans le cas de traitements transfrontaliers de données par des organes fédéraux et des personnes privées et ainsi de remplir ses tâches légales. Dans le cadre de sa surveillance et de son conseil en matière de

traitements transfrontaliers de données par des organes fédéraux et des personnes privées, il peut ainsi, si nécessaire, prendre contact avec l'autorité de protection des données de l'État destinataire concerné. Cela s'avère notamment utile lorsqu'il doit, faute de connaissances spécialisées sur place, recourir aux connaissances et aux informations d'une autorité étrangère de protection des données afin d'évaluer dans quelle mesure les exigences en matière de protection des données sont respectées lors de l'échange de données.

La coopération internationale sous forme d'entraide administrative sert toujours à **préserver la souveraineté**. En vertu de la souveraineté territoriale prévue par le droit international public, un État dispose en principe d'une souveraineté exclusive sur son propre territoire. Les autres États doivent respecter cette souveraineté. Les autorités d'un État étranger ne peuvent donc pas effectuer d'actes officiels sur le territoire d'un autre État sans le consentement de celui-ci. Elles n'ont donc pas non plus d'accès direct aux données et informations qui se trouvent sur le territoire étranger. L'entraide administrative permet de surmonter cette barrière souveraine dans le cadre d'une procédure ordonnée, dans laquelle le PFPDT, qui dispose des données et informations nécessaires, peut fournir une assistance administrative aux autorités étrangères chargées de la protection des données. Les autorités étrangères chargées de la protection des données peuvent ainsi être renvoyées à la voie de l'entraide administrative. Cela permet en fin de compte d'empêcher les autorités étrangères chargées de la protection des données de prendre de leur propre chef des mesures (d'enquête) extraterritoriales. Cela vaut bien sûr également dans le cas inverse, lorsque le PFPDT a besoin d'informations et de données personnelles dont disposent les autorités étrangères chargées de la protection des données. 17

D. Délimitations

1. Assistance administrative nationale

À la différence de l'assistance administrative nationale, l'assistance administrative internationale comprend l'aide fournie à des autorités étrangères ou internationales ou celle que le PFPDT reçoit d'autorités étrangères ou internationales. Elle concerne donc l'**assistance transfrontalière** entre le PFPDT et les autorités étrangères chargées de la 18

protection des données. Il s'agit toujours d'une assistance en faveur d'un autre État. L'entraide administrative nationale entre le PFPDT et d'autres autorités fédérales ou cantonales dans le cadre de l'accomplissement de leurs tâches légales respectives, qui est régie par l'art. 54 LPD, n'est pas concernée.

2. Distinction par rapport à l'entraide judiciaire

19 La distinction entre entraide administrative et entraide judiciaire dans le contexte international est difficile à établir. Alors qu'il existe au moins des critères de délimitation dans le contexte national – même si, là aussi, une distinction nette n'est pas toujours facile à établir –, la situation juridique est encore plus confuse dans le contexte international. Souvent, les deux institutions juridiques ne sont plus distinguées, mais font l'objet d'un **traitement commun**. Une partie de la doctrine demande donc que l'entraide administrative et l'entraide judiciaire soient regroupées sur le plan dogmatique. Certaines lois regroupent alors les deux types d'assistance dans le même paragraphe.

20 À notre avis, la distinction est toutefois essentielle en raison des **effets juridiques** qui y sont liés. Tant le choix du droit applicable (base juridique) – et donc les règles de procédure et de recours – que les conditions et les limites respectives des mesures peuvent varier : Ainsi, l'entraide judiciaire internationale en matière pénale peut, dans des circonstances particulières, relever du champ d'application de l'art. 6 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH ; RS 0.101). Un recours devant le Tribunal fédéral n'est recevable que dans le cas de l'entraide judiciaire internationale et de l'assistance administrative en matière fiscale, qui ont généralement un but répressif.

21 Les **critères** suivants, qui peuvent parfois être combinés, peuvent en principe être utilisés pour déterminer s'il s'agit d'une entraide administrative ou judiciaire :

- **Nature ou fonction des autorités concernées :** l'entraide judiciaire internationale s'effectue entre les autorités judiciaires. L'entraide administrative, en revanche, est fournie entre les autorités administratives de l'État requérant et de l'État requis.
- **Nature de la procédure soutenue** : d'un point de vue procédural, il y a entraide judiciaire internationale lorsqu'une aide est accordée à une

autorité étrangère ou internationale dans le cadre d'une procédure pénale, administrative ou civile. Elle est généralement fournie dans le cadre d'une procédure externe à l'administration (c'est-à-dire judiciaire). L'assistance administrative internationale, en revanche, désigne l'assistance fournie entre les autorités de l'État requérant et de l'État requis en dehors d'une procédure (judiciaire) régie par le droit procédural, dans le but d'accomplir des tâches légales.

Étant donné que la coopération au sens de l'art. 55 LPD consiste en une assistance transfrontalière entre autorités administratives (PFPDT et autorités étrangères de protection des données) et que celle-ci est fournie en dehors d'une procédure régie par le droit procédural, la coopération administrative prend la **forme d'une assistance administrative**. L'art. 55 LPD ne régit donc que l'assistance administrative internationale ; la LPD ne régit en revanche pas l'entraide judiciaire internationale. 22

3. Simple coopération administrative

Toutes les aides transfrontalières entre le PFPDT et les autorités étrangères de protection des données qui sont fournies en dehors d'une procédure régie par le droit procédural ne constituent pas une assistance administrative. L'assistance administrative transfrontalière concerne toujours des personnes déterminées ou déterminables et s'inscrit donc dans le cadre d'un cas concret. Ainsi, l'al. 1 se réfère clairement à **des cas individuels concrets** dans lesquels des informations et des données personnelles sont communiquées à une autorité de protection des données afin que celle-ci puisse remplir son mandat légal. 23

La coopération administrative à des fins d'échange général d'informations et d'expériences (par exemple sur les *bonnes pratiques*) relève de la simple **coopération administrative**. À cette fin, le PFPDT peut établir des contacts avec des autorités étrangères de protection des données, indépendamment d'un cas particulier et de l'activité de surveillance concrète qui y est liée. Cela permet d'échanger sur des questions pertinentes qui se posent dans le cadre du traitement transfrontalier des données et d'élaborer des prises de position ou des recommandations. La simple coopération administrative peut se fonder sur l'art. 58, al. 1, let. b, LPD. 24

E. Formes de coopération

25 En l'absence d'une loi générale sur l'entraide administrative internationale, les différentes dispositions relatives à l'entraide administrative sont dispersées dans les différentes **lois spécialisées** et les bases conventionnelles internationales. Elles présentent une grande hétérogénéité, ce qui rend difficile toute catégorisation globale. L'approche sectorielle permet en revanche de tenir compte de manière ciblée des particularités du domaine concerné ainsi que des intérêts et des besoins des autorités impliquées et des personnes concernées. Le contenu et l'étendue de la coopération formelle avec les autorités étrangères de protection des données dans le domaine de la LPD sont donc principalement régis par l'art. 55 LPD. Les formes de coopération doivent toutefois encore être concrétisées dans le détail.

1. Formes de coopération

26 L'art. 55 LPD ne précise pas la forme que doit prendre la coopération. La disposition stipule simplement que le PFPDT peut échanger des informations ou des données personnelles avec des autorités étrangères afin de remplir leurs tâches respectives prévues par la loi dans le domaine de la protection des données. Il appartient donc au PFPDT de **décider** de l'intensité et de la forme de la coopération avec les autorités étrangères de protection des données.

27 Le libellé de l'art. 55 LPD, selon lequel le PFPDT peut échanger des informations et des données personnelles avec les autorités étrangères, montre clairement que l'**assistance administrative en matière d'information** est au cœur des échanges avec les autorités étrangères de protection des données. Celle-ci comprend la communication de données factuelles et personnelles dans le but d'aider le PFPDT et, inversement, par le PFPDT à d'autres autorités étrangères de protection des données afin qu'elles puissent remplir leurs tâches légales respectives. Cette forme de coopération peut être liée à l'enquête sur des violations présumées des dispositions des lois respectives sur la protection des données.

28 L'art. 55 LPD ne se prononce pas expressément sur la possibilité de **mener des enquêtes coordonnées**. Néanmoins, le PFPDT est habilité, en vertu de l'art. 55 LPD, à s'engager dans de telles formes de coopération. Le libellé de l'art. 55 LPD peut tout à fait être interprété comme signifiant que la conduite

d'enquêtes coordonnées fait partie de l'échange d'informations et de données personnelles. Enfin, la coopération dans le cadre d'enquêtes concertées repose en fin de compte sur un échange d'informations. Les documents ne contiennent en outre aucune indication laissant supposer que les formes de coopération se limitent à l'échange d'informations. L'art. 55 LPD laisse au contraire ouvertes les formes de coopération, ce qui plaide en faveur d'une interprétation aussi large que possible de l'entraide administrative internationale. Compte tenu de l'objectif de l'entraide administrative internationale, qui est de garantir le plus efficacement possible le respect des règles de protection des données dans un contexte transfrontalier, il va de soi que toutes les formes de coopération – pour autant que les conditions énoncées à l'al. 1 soient remplies – relèvent de l'entraide administrative internationale. En conclusion, la fourniture d'une aide à l'enquête et la conduite d'enquêtes concertées sont également couvertes par l'art. 55 LPD.

Il n'existe actuellement aucune base juridique spécifique pour la **reconnaissance et l'exécution** des décisions des autorités étrangères chargées de la protection des données. Même les mesures d'assistance administrative accordées par le PFPDT en vertu de l'art. 55 LPD ne vont pas jusqu'à couvrir l'exécution en Suisse des décisions des autorités étrangères chargées de la protection des données, notamment les sanctions. Compte tenu de la divergence entre les normes pénales de la LPD et du DSGVO, l'exécution des sanctions prononcées par les autorités étrangères chargées de la protection des données échouerait souvent en raison de l'exigence de la double incrimination. Cela revêt une importance particulière dans la mesure où les responsables du traitement et les sous-traitants en Suisse peuvent être soumis au champ d'application territorial du DSGVO et donc aux sanctions prévues par celui-ci. 29

2. Coopération multilatérale

Le caractère de plus en plus transfrontalier du traitement des données entraîne un renforcement de la surveillance transfrontalière, qui se traduit par une mise en réseau des autorités de surveillance, à laquelle participe également le PFPDT. Ainsi, l'échange général d'informations transfrontalières, qui vise notamment à favoriser l'élaboration de normes transfrontalières, a souvent lieu au sein d'**instances multilatérales** et de réseaux internationaux. 30

Ceux-ci présentent un degré d'institutionnalisation plus ou moins élevé et constituent une forme de simple coopération administrative (cf. N. 23 s.).

3. Traités internationaux

31 Au-delà de l'art. 55 LPD, le Conseil fédéral est libre de réglementer spécifiquement la coopération entre le PFPDT et les autorités étrangères de protection des données dans le cadre de traités internationaux. Le PFPDT aurait préféré que l'art. 55 LPD soit complété de manière à lui permettre de réglementer de manière autonome les modalités de la coopération avec les autorités étrangères dans le cadre d'un accord. L'art. 67, let. a, LPD prévoit toutefois que le **Conseil fédéral** peut conclure de manière autonome des traités internationaux relatifs à la coopération internationale entre autorités de protection des données.

32 L'art. 55 LPD constitue déjà une base suffisante pour permettre l'échange de données personnelles et, par exemple, de secrets professionnels, commerciaux et de fabrication, sous réserve des conditions prévues à l'al. 1. Un traité international n'est pas nécessaire à cet effet. Un tel traité est toutefois utile lorsqu'une **coopération à long terme** exige un degré de coopération plus élevé et que celle-ci doit être formalisée. La délimitation des compétences des différentes autorités de protection des données peut également être réglée dans le cadre d'un traité international. Enfin, un traité international est nécessaire si l'on veut établir des droits et des obligations pour les autorités de protection des données qui vont au-delà de l'art. 55 LPD. On peut penser, en dehors du champ d'application de la Convention 108+ et de la directive (UE) 2016/680, à une obligation d'assistance administrative ou à la réglementation de la communication à des tiers (voir N. 8 et N. 10).

F. Limites

33 Dans le cadre de l'entraide administrative internationale, il faut toujours tenir compte du fait que deux relations juridiques sont concernées. Celles-ci peuvent parfois être en **conflit** l'une avec l'autre. D'une part, il existe une relation de droit international entre l'État requérant et l'État requis. Cette relation est principalement régie par les conditions préalables à la fourniture d'une assistance administrative, telles que prévues à l'al. 1. La question centrale est de savoir dans quelle mesure la coopération avec l'État requérant est autorisée en matière de protection des données sur la base de l'al. 1.

D'autre part, il existe également une relation juridique entre l'État requis et la personne concernée par les informations ou les données personnelles transmises dans le cadre de l'entraide administrative. Dans cette relation, le droit constitutionnel à la protection de la sphère privée s'oppose à la tâche de l'État de garantir le respect des dispositions en matière de protection des données dans un contexte transfrontalier, dans la mesure où des données personnelles sont concernées. Pour ces deux relations, la protection des droits fondamentaux et le droit en matière de protection des données imposent certaines exigences qui doivent être respectées lors de la communication transfrontalière d'informations et de données personnelles.

34 L'art. 13, al. 2, de la Constitution fédérale de la Confédération suisse (Cst. ; RS 101) protège les données personnelles et les données à caractère personnel. L'**autodétermination informelle** garantit qu'une personne peut décider de manière autonome à qui et quand elle divulgue des informations sur sa vie privée et si et à quelles fins des informations la concernant peuvent être traitées. Le champ d'application matériel n'est donc pas seulement concerné lorsqu'un traitement de données personnelles est effectué de manière abusive. Un traitement sans le consentement des personnes concernées suffit déjà à cet effet. La communication de données personnelles à des tiers est donc également couverte par l'art. 13, al. 2, Cst. La communication de données personnelles à une autorité étrangère de protection des données constitue donc généralement une atteinte aux droits fondamentaux des personnes concernées.

35 Les atteintes aux droits fondamentaux protégés sont admissibles sous certaines conditions (cf. art. 36 Cst.). L'art. 55 LPD constitue une base légale suffisante pour la communication de données personnelles à des autorités étrangères chargées de la protection des données. Le respect le plus efficace possible des règles de protection des données dans un contexte transfrontalier relève également d'un intérêt public important, qui découle en fin de compte des exigences de protection de l'art. 13, al. 2, Cst. La communication de données personnelles à des autorités étrangères chargées de la protection des données doit donc être proportionnée. Les éléments individuels des principes d'entraide administrative inscrits à l'art. 55, al. 1, LPD – principes de spécialité et de confidentialité (cf. N. 54 ss et N. 60 ss), le principe de la longue main (cf. N. 65 ss) ainsi que la possibilité de subordonner la communication de données personnelles à des conditions ou de les

anonymiser (cf. N 68 s.) – contribuent indirectement à la proportionnalité de la communication dans ce contexte. Néanmoins, le PFPDT doit vérifier, pour chaque communication de données personnelles à des a.utorités étrangères de protection des données, dans quelle mesure la communication est proportionnée dans le cas concret. Cela amène Kerboas/Lennman à faire remarquer qu'un tel **examen de proportionnalité** nécessite beaucoup de temps et de ressources dans chaque cas particulier, mais ne donne parfois que des résultats limités.

36 L'entraide administrative internationale entre le PFPDT et les autorités étrangères de protection des données relève également du **champ d'application de la LPD**. Il en résulte en premier lieu que le PFPDT ne peut communiquer des données personnelles que si, conformément à l'art. 16 LPD, l'État de l'autorité de protection des données requérante offre un niveau de protection adéquat. En ce qui concerne les parties contractantes à la Convention 108+, on peut généralement partir du principe qu'il existe un niveau de protection adéquat, sous réserve de circonstances particulières. Les motifs prévus à l'art. 36, al. 6, LPD s'opposent également à la communication de données personnelles à l'étranger par des organes fédéraux, et donc par le PFPDT. Le PFPDT refuse donc la communication dans le cadre de l'entraide administrative transfrontalière ou la limite lorsque cela est nécessaire pour des raisons d'intérêt public majeur, pour des intérêts manifestement dignes de protection de la personne concernée (let. a) ou en raison de prescriptions particulières en matière de protection des données (let. b). En ce qui concerne la possibilité de refuser ou de limiter la communication en raison d'obligations légales de garder le secret, il convient de se référer aux explications suivantes (cf. N. 64 et N. 77).

- **Les intérêts publics** qui s'opposent à la communication peuvent être la sécurité militaire, la sûreté de l'État ou les affaires policières. De tels intérêts existent également lorsque la communication est susceptible de compromettre la position dans des négociations, le processus de formation de l'opinion et de la volonté de l'organe public, l'efficacité de mesures d'enquête, de sécurité ou de surveillance ou les relations avec l'étranger. Les intérêts publics peuvent également inclure des intérêts économiques, monétaires ou de politique monétaire. Si de tels intérêts sont concernés et s'il est probable que la divulgation causerait un préjudice important, celle-ci doit être refusée.

- En ce qui concerne l'**intérêt digne de protection** de la personne concernée, il convient en premier lieu de prendre en considération la mesure dans laquelle la communication des informations porte atteinte de manière intolérable à la protection de la sphère privée.

G. Protection juridique

L'entraide administrative internationale est fournie entre le PFPDT et une autorité étrangère de protection des données. La communication d'informations et de données personnelles peut dans un premier temps être simplement qualifiée d'« [...] acte interne à l'autorité [...] » ou être attribuée à l'**acte administratif effectif**. Le fait que l'acte administratif effectif affecte la situation juridique de particuliers constitue alors un effet indirect que l'entraide administrative internationale peut avoir sur les particuliers. L'art. 55 LPD ne précise pas si les autorités sont tenues de fournir une assistance administrative pour la mise en œuvre d'une procédure administrative. 37

Une protection juridique efficace présuppose toutefois un objet de recours approprié et donc une décision. Dans la mesure où l'entraide administrative en matière d'information est un acte administratif sans décision au sens d'un **acte réel** du PFPDT, il faut donc d'abord obtenir une décision de constatation fondée sur l'art. 25*a* de la loi fédérale sur la procédure administrative (loi sur la procédure administrative, PA ; RS 172.021). Dans ces cas, la personne concernée n'aura toutefois souvent pas connaissance de l'acte d'entraide administrative, raison pour laquelle elle ne pourra de facto pas emprunter la voie prévue à l'art. 25*a* PA. Dans le contexte d'une protection juridique efficace, la question centrale est de savoir dans quels cas il existe un droit à la délivrance d'une décision. Seule la décision ouvre la possibilité de recourir à la protection juridique administrative. 38

La question de savoir si la communication d'informations et de données personnelles par le PFPDT nécessite une décision est régie par les règles générales de la PA. La LPD ne prévoit aucune dérogation légale spéciale à cet égard. La décision du PFPDT de fournir une assistance administrative doit être considérée comme une décision lorsque **des intérêts dignes de protection** de personnes privées sont concernés. L'intérêt digne de protection ne présuppose pas un intérêt juridiquement protégé. Des intérêts purement factuels, économiques ou idéaux suffisent, mais ceux-ci doivent toujours apparaître comme dignes de protection. 39

40 La notion d'intérêt digne de protection s'appuie sur la qualité de partie au sens de l'art. 6 PA, qui est lui-même lié à l'art. 48 PA. Au sens de la qualité de partie, toute personne a un intérêt à une décision qui, en cas d'adoption d'une décision, serait légitimée à la contester. La condition préalable est que la personne soit **particulièrement concernée**. Elle doit avoir un lien particulier avec l'objet qui doit être réglé dans la décision et donc être plus concernée que le grand public. Une telle implication est donnée pour Wyss lorsque des actes d'entraide administrative déterminent de manière durable et significative des droits et des obligations. Il en déduit que dans les cas où la situation juridique est modifiée de manière irréversible, une décision doit être rendue. À l'inverse, il convient de noter que la transmission de données personnelles ou d'informations ne constitue souvent « qu' » une mesure préparatoire en vue de l'adoption *ultérieure d'*une décision. L'ouverture d'une procédure administrative ne constitue pas en soi une décision. Dans le domaine de l'entraide administrative internationale, il convient toutefois de souligner que la transmission de données à l'étranger peut en soi constituer une atteinte aux intérêts dignes de protection des personnes concernées, ce que confirment les art. 16 ss LPD.

41 De manière plus générale, on peut retenir que la **communication de données personnelles** constitue dans chaque cas une atteinte au droit à l'autodétermination en matière d'information. Il y a donc toujours un intérêt suffisant. Si le PFPDT conclut que les conditions requises pour l'entraide administrative au sens de l'al. 1 sont remplies, il doit engager une procédure en cas de communication de données personnelles et statuer sur la communication des données personnelles à une autorité étrangère de protection des données dans une décision au sens des art. 5 et 34 s. PA. La qualité de partie à la procédure permet à la personne concernée d'exercer les droits qui lui sont accordés en vertu de la PA : elle a ainsi notamment le droit d'être entendue, le droit de consulter le dossier, le droit d'être représentée ou encore le droit de recevoir la décision. Enfin, la participation à la procédure administrative est également étroitement liée à la légitimation à recourir.

42 La divulgation de secrets professionnels, d'affaires ou de fabrication constitue également un cas particulier. L'al. 3 oblige le PFPDT à donner aux personnes concernées la possibilité de s'exprimer avant de communiquer à une autorité étrangère de protection des données des informations susceptibles de contenir des secrets professionnels, d'affaires ou de fabrication. Cela découle

déjà du droit d'être entendu prévu à l'art. 29 PA. L'art. 55, al. 3, LPD n'apporte donc aucune valeur ajoutée notable sur le plan procédural, mais sert à clarifier la situation.

La participation des personnes concernées à la procédure administrative doit avoir lieu à un **moment tel** qu'elles puissent exercer efficacement leurs droits en tant que parties. En d'autres termes, la protection juridique doit être assurée en temps utile. Avant de communiquer les informations ou les données personnelles à l'autorité de protection des données requérante, le PFPDT doit informer les personnes concernées de la communication prévue : une fois que les informations ou les données personnelles ont été communiquées à l'autorité de protection des données requérante, la protection juridique nationale ne peut plus s'appliquer efficacement. Le traitement ultérieur des informations ou des données personnelles est déterminé en dehors de l'ordre juridique suisse. Comme l'utilisation des informations et des données personnelles à l'étranger ne peut être empêchée, la communication à l'autorité de protection des données requérante crée une situation irréversible. Le Tribunal fédéral l'a également reconnu dans le contexte de l'assistance administrative internationale en matière fiscale : « Une fois que les données ont été transmises à l'étranger, il n'est généralement plus possible d'empêcher leur utilisation. » 43

Avec le PFPDT, une autorité fédérale statue sur la coopération avec les autorités étrangères de protection des données et sur la communication d'informations et de données personnelles à celles-ci. Si la décision de communication est rendue sous la forme d'une décision au sens de l'art. 5 PA, la **procédure de recours** est également régie par la PA. Conformément à l'art. 44 PA, les décisions peuvent faire l'objet d'un recours devant le Tribunal administratif fédéral. Les décisions relatives à l'entraide administrative internationale sont en principe exclues du recours en matière de droit public devant le Tribunal fédéral. Cela permet de décharger le Tribunal fédéral et de permettre une procédure rapide grâce à la réduction du nombre d'instances. En conséquence, le Tribunal administratif fédéral statue en dernière instance sur l'entraide administrative internationale dans le champ d'application de la LPD. Il est toutefois concevable que, pour d'autres questions relevant de la compétence du Tribunal fédéral, il faille statuer à titre préjudiciel sur la recevabilité de l'entraide administrative internationale. 44

II. CONDITIONS (AL. 1)

A. Généralités

45 L'art. 55, al. 1, LPD régit les conditions dans lesquelles le PFPDT peut échanger des informations et des données personnelles avec les autorités étrangères afin de remplir leurs tâches légales respectives dans le domaine de la protection des données. Ces conditions constituent des **éléments caractéristiques** de l'entraide administrative transfrontalière. Elles ont été élaborées dans le contexte de l'entraide judiciaire et sont utilisées dans le domaine de l'entraide administrative.

1. Autorités compétentes

46 L'art. 55, al. 1, LPD vise les autorités étrangères qui sont compétentes en matière de protection des données dans leur pays. En d'autres termes, l'échange d'informations et de données personnelles n'a lieu qu'avec **les autorités étrangères chargées de la protection des données**. La LPD ne contient pas d'exigences plus précises concernant la qualification en tant qu'autorité étrangère chargée de la protection des données. Pour comprendre cette notion, on peut, à notre avis, se référer à l'autorité de contrôle telle qu'elle est décrite à l'art. 15 de la Convention 108+. Cette disposition oblige les parties contractantes à créer une ou plusieurs autorités publiques de contrôle et de surveillance indépendantes et impartiales qui contribuent à la protection des personnes physiques lors du traitement de leurs données à caractère personnel. Ces autorités peuvent être un seul délégué à la protection des données ou un collège. Outre son indépendance, il est essentiel que l'autorité de contrôle dispose d'instruments de surveillance et de contrôle efficaces. L'autorité doit donc également disposer de compétences d'enquête.

47 Il convient en outre de distinguer entre les organes chargés du traitement des données dans les différents États – y compris les autorités de contrôle dans certains secteurs économiques ou branches – et les autorités de contrôle spécifiques dans le domaine de la protection des données. La coopération transfrontalière dans le domaine de la protection des données s'effectue principalement au niveau des **organes traitant des données**. Dans le cadre de l'accomplissement de leurs tâches légales quotidiennes, ceux-ci doivent évaluer si l'échange d'informations et de données personnelles avec un organisme étranger est autorisé. Pour les organes traitant des données, la

coopération est régie par la loi applicable en la matière. Les art. 16 et 36 LPD doivent également être respectés dans tous les cas. Le PFPDT est quant à lui chargé de la surveillance de ces organes traitant des données, pour laquelle il peut recourir à l'entraide administrative internationale prévue à l'art. 55 LPD.

2. Étendue et contenu

L'échange d'informations et de données personnelles concerne toutes les **tâches légales** du PFPDT ou de l'autorité étrangère de protection des données. L'étendue des tâches légales découle de la législation nationale et la licéité de l'échange est déterminée par la demande, qui doit exposer dans quelle mesure les informations ou les données personnelles sont nécessaires à l'accomplissement des tâches légales. Les tâches légales du PFPDT sont énumérées au chapitre 7 de la LPD. Pour répondre aux demandes d'entraide administrative étrangères, le PFPDT peut accomplir tous les actes auxquels il est habilité en vertu des dispositions de la LPD applicables à son activité. 48

Outre **des informations**, le PFPDT peut également échanger **des données personnelles** au sens de l'art. 5, let. a, LPD. Le PFPDT peut donc communiquer toutes les informations qui se rapportent à une personne physique identifiée ou identifiable. 49

3. Nature juridique

L'art. 55 LPD ne contient **aucune obligation** d'assistance administrative transfrontalière. Il autorise simplement le PFPDT à fournir une assistance administrative ou à demander une assistance administrative dans les conditions prévues à l'al. 1. Toutefois, dans les relations avec les autorités étrangères de protection des données qui sont parties à la Convention 108+, il convient de respecter l'obligation de fournir une assistance administrative prévue par la convention et les motifs de refus (cf. N. 8). 50

B. Conditions de recevabilité

Pour que le PFPDT puisse échanger des informations et des données personnelles avec les autorités étrangères de protection des données, les cinq conditions suivantes doivent être remplies **de manière cumulative**, conformément à l'art. 55, al. 1, LPD. Dans la pratique, il est difficile d'évaluer de manière définitive dans quelle mesure les différentes conditions sont remplies. Dans la pratique, il convient donc de consigner par écrit les 51

conditions requises dans le cadre de l'octroi de l'assistance administrative et de les communiquer à l'autorité étrangère de protection des données requérante.

1. Réciprocité (let. a)

52 L'art. 55, al. 1, let. a, LPD prévoit que la **réciprocité de l'entraide administrative** doit être garantie entre la Suisse et l'État étranger. La réciprocité est un élément caractéristique de l'entraide administrative. Par conséquent, une autorité de protection des données requérante ne peut demander une entraide administrative sous forme d'informations et de données personnelles que si elle est elle-même disposée à accorder une entraide administrative.

53 Une telle assistance administrative est garantie dans les relations avec les parties contractantes à la Convention 108+ ainsi qu'avec les États membres de l'UE sur la base de la directive (UE) 2016/680. Dans les relations avec d'autres autorités étrangères de protection des données, la réciprocité est garantie de manière contraignante, pour autant qu'un **traité international** prévoie l'assistance administrative avec réciprocité. Le Conseil fédéral peut conclure de tels traités internationaux de manière indépendante, en vertu de l'art. 67, let. a, LPD. En l'absence de base conventionnelle internationale, le PFPDT doit obtenir l'assurance de la réciprocité au cas par cas, et il ne peut donner suite à la demande d'assistance administrative que sur la base d'une telle assurance.

2. Principe de spécialité (let. b)

54 L'art. 55, al. 1, let. b, LPD est l'expression du principe de spécialité. Le principe de spécialité ou le principe de limitation de la finalité est un **principe traditionnel du droit international public** en matière d'entraide administrative et judiciaire internationale, qui découle du droit de l'extradition. Il est en outre inscrit à l'art. 19 de la Convention 108+. Le Tribunal fédéral reconnaît à ce principe – du moins dans le domaine du droit de l'extradition – le caractère d'une règle de droit international coutumier. En matière d'entraide administrative, ce principe est toutefois également inscrit dans de nombreuses lois fédérales.

55 Selon ce principe, les informations et les données personnelles échangées ne peuvent être utilisées par l'autorité requérante **que pour la procédure de**

protection des données qui est à la base de la demande d'entraide administrative et pour laquelle les informations ou les données personnelles ont été transmises. Une utilisation ultérieure n'est autorisée que si les lois des deux États ou un traité international prévoient une telle possibilité et si l'autorité requise qui a fourni les informations ou les données personnelles autorise cette utilisation ultérieure dans le cas concret. Pour une utilisation ultérieure et parallèle des informations et des données personnelles dans une éventuelle procédure pénale, les principes de l'entraide judiciaire internationale en matière pénale doivent être respectés.

Le principe de spécialité sert de **barrière** qui protège en premier lieu la souveraineté de l'État requis. Dans le même temps, la limitation de la finalité sert également à renforcer les droits de la personnalité des personnes concernées et vise à garantir une utilisation proportionnée des informations et des données personnelles. La limitation de la finalité interdit toute réutilisation illimitée par l'État requérant. 56

Outre sa fonction de barrière, le principe de spécialité sert également de **condition d'admissibilité** pour la communication d'informations et de données personnelles : l'autorité de protection des données requérante doit offrir des garanties suffisantes qu'elle n'utilisera les informations ou les données personnelles qu'aux fins pour lesquelles elles ont été transmises par l'autorité requise. Se fondant sur le principe de bonne foi en droit international public, le Tribunal fédéral a jusqu'à présent estimé que le respect du principe de spécialité par les États pouvait être considéré comme allant de soi. Ce n'est qu'en cas d'indices concrets d'une utilisation abusive dans l'État requérant qu'il convient de vérifier le respect de ce principe. Au vu de cette jurisprudence, le PFPDT n'a pas à obtenir de garanties lorsque l'entraide administrative repose sur un traité international qui contient le principe de spécialité. En vertu du principe de bonne foi prévu à l'art. 26 de la Convention de Vienne sur le droit des traités (RS 0.111), les deux parties contractantes sont directement tenues de respecter le principe de spécialité. En revanche, si l'entraide administrative est fondée exclusivement sur l'art. 55, al. 1, let. b, LPD, le PFPDT doit, dans le cadre de l'entraide administrative, signaler expressément à l'autorité étrangère de protection des données requérante l'obligation de (ré)utilisation liée au principe de spécialité et lui rappeler les limites dans lesquelles les informations ou les données personnelles transmises peuvent être utilisées. 57

58 Au sens d'une condition de recevabilité, la limitation de la finalité découlant du principe de spécialité exige que l'autorité de protection des données requérante indique la finalité pour laquelle les informations ou les données personnelles demandées sont nécessaires. Il résulte donc de ce principe une **obligation de justification**.

59 La contrôlabilité et l'**applicabilité** de la limitation de la finalité sont toutefois limitées. Si une autorité étrangère de protection des données enfreint le principe de spécialité, le PFPDT peut refuser les futures demandes d'entraide administrative de cette autorité au motif qu'il n'existe pas de garantie suffisante quant au respect du principe de spécialité. Indépendamment de cela, il faut partir du principe que l'application doit régulièrement être assurée par la personne concernée et par le biais de la protection des droits individuels. Cela s'applique lorsque les données personnelles de la personne concernée sont effectivement utilisées dans le cadre d'une procédure ultérieure, c'est-à-dire dans une procédure qui ne repose pas sur la demande d'entraide administrative initiale et pour laquelle les données personnelles n'ont pas été transmises. Dans un tel cas, la personne concernée devrait dénoncer la transmission illicite dans le cadre de la procédure en question. La possibilité d'exercer ce droit dépend notamment du droit procédural applicable (éventuellement étranger).

3. Principe de confidentialité (let. c)

60 L'art. 55, al. 1, let. c, LPD vise à préserver des intérêts particuliers en matière de confidentialité. Il exige ainsi que l'autorité requérante s'engage à protéger ces secrets. La **portée et le contenu** des secrets à préserver découlent des dispositions pénales pertinentes et de la jurisprudence y afférente. Pour le secret professionnel, il convient de se référer à l'art. 321 CP, pour le secret de fabrication et le secret d'affaires, aux art. 162 CP et 273 CP.

61 Sont notamment soumis au **secret professionnel** les ecclésiastiques, les avocats, les médecins, les dentistes, les pharmaciens, les sages-femmes et les psychologues.

62 La notion de secret est généralement comprise au sens large dans le contexte des **secrets d'affaires** ; il n'existe pas de définition légale. Selon la jurisprudence du Tribunal fédéral, ne sont pas considérés comme des secrets les faits manifestes ou accessibles à tous (relative méconnaissance) dont la

personne qui détient le secret a un intérêt légitime à ce qu'ils restent secrets (intérêt objectif à la confidentialité) et qu'elle souhaite garder secrets pour des raisons légitimes (intérêt subjectif à la confidentialité). Les secrets d'affaires sont des informations qui pourraient nuire au succès commercial de l'entreprise ou fausser la concurrence si elles étaient portées à la connaissance d'entreprises concurrentes. Sont donc considérés comme secrets d'affaires tous les faits techniques, organisationnels, commerciaux et financiers de la vie économique qui peuvent influencer le succès commercial du détenteur du secret.

Les **secrets de fabrication** doivent être traités de la même manière que les secrets d'affaires : ils concernent en particulier l'aspect technique de la production, c'est-à-dire les connaissances qui contiennent des instructions pour agir sur le plan technique. Il s'agit donc de connaissances utilisées dans la fabrication de produits et qui ne sont pas reconnaissables sur le produit vendu et peuvent donc être considérées comme secrètes. Il s'agit par exemple d'informations sur les procédés et les instructions de fabrication, de production ou de construction, ainsi que des résultats de recherche, des plans de production et de construction ou des sources d'approvisionnement. 63

Les **obligations légales de confidentialité** ne s'opposent pas *en soi* à la communication d'informations aux autorités étrangères chargées de la protection des données. L'art. 55, al. 1, let. c, LPD précise que ces informations peuvent être communiquées à condition que l'autorité de protection des données requérante respecte le secret professionnel ainsi que les secrets d'affaires et de fabrication (cf. N. 77 ss) ; l'art. 55 LPD autorise donc une dérogation à l'obligation légale de confidentialité. L'art. 55, al. 3, LPD oblige toutefois le PFPDT à demander l'avis des détenteurs du secret concernés avant de communiquer des informations susceptibles de contenir un secret professionnel, d'entreprise ou de fabrication (cf. N. 78). Il apparaît ainsi clairement qu'il convient dans chaque cas de mettre en balance l'intérêt à communiquer l'information et l'intérêt à la confidentialité. 64

4. Principe de la longue main (let. d)

Selon l'art. 55, al. 1, let. d, LPD, les informations et les données personnelles ne peuvent être communiquées **à des tiers**, y compris à d'autres autorités, que si l'autorité de protection des données requise a préalablement autorisé cette communication. Par tiers, on entend en premier lieu les autorités tierces 65

de l'État requérant qui ne participent pas à l'échange entre le PFPDT et l'autorité étrangère de protection des données.

66 L'**obligation d'autorisation** protège les personnes concernées contre une divulgation ultérieure des informations ou des données personnelles les concernant. Elle garantit en outre que le PFPDT conserve le contrôle des informations et des données personnelles. En cas d'intérêt particulier, la personne concernée doit être entendue avant que la communication ne soit autorisée ; les autres droits des parties doivent également être respectés. Cela vaut en particulier pour la communication de données personnelles. Pour le reste, il est renvoyé aux considérations relatives à la protection juridique (cf. N. 37 ss).

67 Le PFPDT doit obtenir une **garantie** correspondante de la part de l'autorité étrangère de protection des données. Il peut renoncer à une telle garantie si l'interdiction de la communication à des tiers est déjà efficacement garantie par une autre base légale, telle qu'un traité international.

5. Respect des conditions et des restrictions (let. e)

68 En vertu de l'art. 55, al. 1, let. e, LPD, l'autorité requérante doit respecter les conditions et restrictions imposées par l'autorité qui lui a transmis les informations et les données personnelles. Cette disposition autorise la communication d'informations et de données personnelles dans les cas où, sans la possibilité d'imposer des conditions ou des restrictions telles que l'**anonymisation**, une demande d'entraide administrative devrait être rejetée.

69 Étant donné que le PFPDT est lié par l'art. 36, al. 6, LPD dans le cadre de l'entraide administrative et que cette disposition subordonne déjà la communication de données personnelles à la possibilité de conditions et de restrictions, la let. e constitue pour l'essentiel une répétition. La disposition précise toutefois que, même dans le cadre de l'entraide administrative internationale, le PFPDT doit fonder la communication de données personnelles sur une **pondération au cas par cas** entre l'intérêt à l'entraide administrative et les intérêts contraires au sens de l'art. 36, al. 6, LPD.

III. COMMUNICATION DE DONNÉES PERSONNELLES (AL. 2)

L'art. 55, al. 2, LPD définit les informations que le PFPDT est autorisé à communiquer à l'autorité étrangère de protection des données afin de justifier sa demande d'entraide administrative ou de répondre à la demande d'une autorité étrangère de protection des données. La liste n'est **pas exhaustive**, comme l'indique le terme « en particulier » dans la phrase introductive. En d'autres termes, le PFPDT peut également fournir d'autres informations pour justifier sa demande d'entraide administrative ou pour répondre à une demande d'entraide administrative émanant d'une autorité étrangère. 70

Selon cette disposition, le PFPDT peut fournir des informations sur l'**identité** du responsable du traitement, du sous-traitant ou d'autres tiers impliqués (let. a) ainsi que sur les **catégories** de personnes concernées (let. b). La mention de catégories sert à classer les personnes dans des groupes types qui présentent certaines caractéristiques communes. Le message cite comme exemples de telles catégories notamment les « consommateurs », les « militaires » ou les « employés ». 71

Le PFPDT ne peut communiquer l'**identité des personnes concernées** que si celles-ci y ont consenti (let. c, ch. 1). Il y a divulgation de l'identité dès lors qu'une personne est identifiable. Cela peut résulter des données elles-mêmes. L'identité est toutefois déjà identifiable lorsqu'elle peut être déduite sans effort disproportionné du contexte des données ou en combinaison avec d'autres données. 72

La divulgation de l'identité nécessite le **consentement** de chaque personne concernée. Dans le cas contraire, la divulgation est interdite. Pour que le consentement soit valable, les exigences de l'art. 6, al. 6 et 7, LPD s'appliquent. Le consentement n'est donc valable que s'il est donné librement, après avoir reçu des informations adéquates, et s'il se rapporte à la communication concrète. Des informations adéquates comprennent les indications relatives à la personne responsable, à l'objectif ou au but, à la manière et à l'étendue du traitement des données, aux catégories de données traitées et à la communication des données. Le consentement n'est soumis à aucune forme particulière et n'est donc pas lié à une déclaration écrite. Toutefois, la communication de données personnelles particulièrement sensibles à des autorités étrangères chargées de la protection des données nécessite un 73

consentement explicite. Selon le message relatif à la LPD, une déclaration de volonté est expresse « [...] lorsqu'elle est faite par des mots écrits ou prononcés ou par un signe et que la volonté exprimée ressort directement des mots ou du signe utilisés. »

74 Le consentement est essentiel dans le cadre du traitement par des personnes privées, car il sert de justification à une atteinte à la personnalité. Indépendamment du consentement, le PFPDT reste toutefois le destinataire des droits fondamentaux. La communication de l'identité à des autorités étrangères chargées de la protection des données doit donc, en raison de l'atteinte à l'art. 13, al. 2, Cst. (cf. N. 34 s.), continuer à servir un intérêt public et être proportionnée pour pouvoir être justifiée. L'exigence du consentement ne constitue donc pas une justification pour le traitement des données par des organes fédéraux tels que le PFPDT, mais une **barrière supplémentaire** à la divulgation.

75 À titre exceptionnel, le PFPDT peut communiquer l'identité des personnes concernées lorsque cette communication est **indispensable à** l'accomplissement de la tâche légale du PFPDT ou de l'autorité étrangère de protection des données (let. c, ch. 2). Cette disposition dérogatoire est formulée de manière analogue à l'art. 36, al. 2, let. a et b, LPD, qui pose de telles exigences pour l'entraide administrative nationale, pour autant qu'il n'existe pas de base légale spéciale. Le caractère indispensable signifie que la tâche ne peut être accomplie sans la communication des données.

76 En outre, le PFPDT peut fournir des informations sur les données personnelles traitées ou les catégories de données personnelles traitées (let. d), sur la finalité du traitement (let. e), sur les destinataires et les catégories de destinataires (let. f) et sur les mesures techniques et organisationnelles (let. g).

IV. OBLIGATION D'INFORMER ET PRISE DE POSITION (AL. 3)

77 L'art. 55, al. 3, LPD oblige le PFPDT, dans le cadre d'une procédure d'entraide administrative, à ne communiquer à une autorité étrangère de protection des données des informations susceptibles de contenir des **secrets professionnels, d'affaires ou de fabrication** que s'il a préalablement donné aux personnes concernées la possibilité de prendre position. Les personnes concernées peuvent être aussi bien des personnes physiques que des

personnes morales. Contrairement à ce qui avait été demandé lors de la consultation, le législateur n'a pas soumis la communication de secrets d'affaires et de fabrication à l'exigence du consentement de la personne concernée.

Cette disposition a pour but de préserver les droits des personnes concernées qui détiennent des secrets professionnels, commerciaux ou de fabrication. À cette fin, l'al. 3 prévoit une **obligation d'informer et un droit d'être entendu**. Avant de communiquer à une autorité étrangère de protection des données des informations susceptibles de contenir un secret professionnel, d'affaires ou de fabrication, le PFPDT doit informer les personnes concernées qui détiennent ces secrets de la communication éventuelle. Le PFPDT est ensuite tenu de recueillir l'avis des personnes concernées. Cela leur donne la possibilité d'exposer leur point de vue au PFPDT dans une prise de position et de justifier pourquoi les informations relatives à des secrets professionnels, d'affaires ou de fabrication ne doivent pas être communiquées à l'autorité étrangère de protection des données. 78

En informant préalablement les personnes concernées et en leur donnant la possibilité de prendre position, le PFPDT contribue à la prise en compte de leurs intérêts et à la protection de leurs secrets. La prise de position doit être prise en compte dans la décision du PFPDT, mais elle n'a **aucun effet contraignant quant au fond** : l'al. 3 n'oblige pas le PFPDT à se conformer au contenu des prises de position des personnes concernées. Il a toutefois l'obligation de prendre connaissance des avis et de leur accorder une grande importance dans sa prise de décision. Plus les secrets professionnels, d'affaires ou de fabrication du détenteur de secrets sont concernés, plus il convient d'accorder d'importance aux avis des personnes concernées. 79

Selon Gerschwiler, les personnes concernées doivent être informées dès lors qu'il existe une **certaine probabilité** que des secrets professionnels, d'affaires ou de fabrication soient divulgués. Il convient d'approuver cette position. La protection des secrets professionnels, d'affaires et de fabrication ne peut être efficacement garantie que si le PFPDT n'informe pas les personnes concernées uniquement lorsqu'il est certain que des secrets protégés par le droit pénal sont concernés. Afin de pouvoir prendre efficacement en compte les intérêts des détenteurs de secrets et de les associer en temps utile à la prise de décision en leur donnant la possibilité de 80

prendre position, il convient d'appliquer un critère généreux. Cela peut également contribuer à éviter des recours ultérieurs.

81 À titre exceptionnel, le PFPDT n'est pas tenu de demander l'avis des personnes concernées. C'est le cas lorsqu'il n'est pas possible de recueillir leur avis ou que cela impliquerait des efforts disproportionnés. Cette exception a manifestement été introduite pour des raisons pratiques et vise à empêcher que la communication des informations aux autorités étrangères de protection des données ne soit compromise lorsque l'obtention d'un avis est impossible ou ne peut se faire qu'au prix d'efforts disproportionnés. Étant donné que le PFPDT porte atteinte aux secrets professionnels, commerciaux ou de fabrication des personnes concernées, protégés par le droit pénal, il ne faut pas présumer trop rapidement qu'il est **impossible ou déraisonnable** de recueillir leur avis. La procédure admissible devra toutefois être déterminée en fin de compte par la jurisprudence.

BIBLIOGRAPHIE

Bachmann Gregor, Anspruch auf Verfahren und Entscheid, Bern 2019.

Baeriswyl Bruno, Die Einwilligung hilft (nicht) weiter, digma 2020, S. 62–66.

Baeriswyl Bruno, Kommentierung zu Art. 31, in: Bruno Baeriswyl/Kurt Pärli (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz (DSG), 1. Aufl., Bern 2015.

Baeriswyl Bruno, Kommentierung zu Art. 55 DSG: in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023.

Baeriswyl Bruno, Kommentierung zu Art. 6 DSG: in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023.

Bai Alain, Der Rechtsschutz gemäss Art. 6 EMRK in Verfahren der internationalen Amtshilfe im Bereich der direkten Steuern, Zürich 2018.

Bellanger François, L'entraide administrative en Suisse, in: Bellanger François/Tanquerel Thierry (Hrsg.), L'entraide administrative, Zürich/Basel 2005, S. 9–28.

Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011.

Benhamou Yaniv/Jacot-Guillarmod Emilie, GDPR on the Swiss Territory, Jusletter IT vom 24. Mai 2018.

Biaggini Giovanni, BV Kommentar, 2. Aufl., Zürich 2017.

Blöchlinger Karin, Amtsgeheimnis und Behördenkooperation, Zum Spannungsfeld von Geheimnisschutz und Verwaltungstätigkeit, Zürich 2015.

Bopp Christian, Das Schweizerische Bankgeschäft, 8. Aufl., Zürich 2021.

Breitenmoser Stephan, Internationale Amtshilfe in Finanzmarktsachen in der Rechtsprechung des Bundesverwaltungsgerichts – aktuelle Fragen und Tendenzen, in: Breitenmoser Stephan/ Ehrenzeller Bernhard (Hrsg.), Internationale Amts- und Rechtshilfe in Steuer- und Finanzmarktsachen, Zürich 2017, S. 185–199.

Breitenmoser Stephan/Bai Alain, Internationale Amts- und Rechtshilfe mit Bezügen zum Ausländerrecht, in: Uebersax Peter/Rudin Beat/Hugi Yar Thomas/Geiser Thomas/Vetterli Luzia (Hrsg.), Ausländerrecht, 3. Aufl., Basel 2022, S. 1921–2015.

Breitenmoser Stephan/Weyeneth Robert, Amts- und Rechtshilfe ist nicht gleich Amts- und Rechtshilfe, in: Fankhauser Roland/Widmer Lüchinger Corinne/Klingler Rafael/Seiler Benedikt (Hrsg.), Das Zivilrecht und seine Durchsetzung, Festschrift für Professor Thomas Sutter-Somm, Zürich 2016, S. 1063–1084.

Diggelmann Oliver, Kommentierung zu Art. 13 BV, in: Waldmann Bernhard/ Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar, Bundesverfassung, Basel 2015.

Dix Alexander, Kommentierung zu Art. 61 DSGVO, in: Kühlig Jürgen/Buchner Benedikt (Hrsg.), DS-GVO/BDSG, Datenschutz-Grundversorgung, Bundesdatenschutzgesetz, Kommentar, 3. Aufl., München 2020.

Donatsch Andreas/Heimgartner Stefan/Meyer Frank/Simonek Madeleine, Internationale Rechtshilfe, 2. Aufl., Zürich 2015.

du Pasquier Shelby R., Internationale Amtshilfe: Informationsaustausch und verfahrensrechtliche Aspekte, AJP 2006, S. 74–82.

Egli Patricia, Kommentierung zu Art. 44 BV, in: Ehrenzeller Bernhard et al. (Hrsg.), St. Galler Kommentar, Bundesverfassung, 4. Aufl., Zürich 2023.

Ferrari-Visca Reto, Strafrechtliche Datenschutzbestimmungen, in: Dal Molin Luca/Wesiak-Schmidt Kirsten (Hrsg.), Datenschutz im Unternehmen, Praxishandbuch mit Beispielen und Checklisten, Zürich/St. Gallen 2023, S. 365–427.

Frei Nula, Kommentierung zu Art. 67 DSG, in: Steiner Thomas/Morand Anne-Sophie/Hürlimann Daniel (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz (Version: 07.09.2023), https://onlinekommentar.ch/de/kommentare/dsg67.

Gächter Thomas/Egli Philipp, Kommentierung zu Art. 43 VwVG, in: Auer Christoph/Müller Markus/Schindler Benjamin (Hrsg.), Kommentar, Bundesgesetz über das Verwaltungsverfahren (VwVG), 2. Aufl., Zürich 2019.

Gerschwiler Stefan, Kommentierung zu Art. 55 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar, DSG, Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023.

Häberli Thomas, Kommentierung zu Art. 83 BGG, in: Niggli Marcel Alexander/Uebersax Peter/Wiprächtiger Hans/Kneubühler Lorenz (Hrsg.), Basler Kommentar, Bundesgerichtsgesetz, 3. Aufl., Basel 2018.

Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich 2020.

Harrendorf Stefan/König Stefan/Voigt Lea, Kommentierung zu Art. 6 EMRK, in: Meyer-Ladewig Jens/Nettesheim Martin/von Raumer Stefan (Hrsg.), Handkommentar, Europäische Menschenrechtskonvention, 5. Aufl., Baden-Baden 2023.

Husi-Stämpfli Sandra/Rudin Beat, Datenschutz, in: Tschudi Hans Martin/Schindler Benjamin/Ruch Alexander/Jakob Eric/Friesecke Manuel (Hrsg.), Die Grenzüberschreitende Zusammenarbeit der Schweiz, Zürich/St. Gallen 2014, S. 623–648.

Jaag Tobias/Häggi Furrer Reto, Kommentierung zu Art. 43 VwVG, in: Waldmann Bernhard/Weissenberger Philippe (Hrsg.), Praxiskommentar, Verwaltungsverfahrensgesetz, 2. Aufl., Zürich 2016.

Kerboas Cécile/Lennman Catherine, Kommentierung zu Art. 55 DSG, in: Meier Philippe/Métille Sylvain (Hrsg.), Commentaire Romand, Loi fédérale sur la protection des données, Basel 2023.

Kiener Regina/Rütsche Bernhard/Kuhn Mathias, Öffentliches Verfahrensrecht, 3. Aufl., Zürich 2021.

Kölz Alfred/Häner Isabelle/Bertschi Martin/Bundi Livio, Verwaltungsverfahren und Verwaltungsrechtspflege des Bundes, 4. Aufl., Zürich/Genf 2025.

Mazidi Simon, Kommentierung zu Art. 59 DSG, in: Blechta Gabor-Paul/Vasella David (Hrsg.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz, 4. Aufl., Basel 2023.

Mund Claudia, Kommentierung zu Art. 36 DSG: in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023.

Opel Andrea, Amtshilfe ohne Information der Betroffenen – eine rechtsstaatlich bedenkliche Neuerung, ASA 83 (2014), S. 265–295 (zit. als Opel, Amtshilfe).

Opel Andrea, Neuausrichtung der schweizerischen Abkommenspolitik in Steuersachen: Amtshilfe nach dem OECD-Standard, Bern 2015 (zit. als Opel, Neuausrichtung).

Oswald Diana, Verfahrensrechtliche Aspekte der internationalen Amtshilfe in Steuersachen, Zürich 2015.

Pasquier Aurélien, Die Sanktionen in der DSGVO, in: Epiney Astrid/Rovelli Sophia (Hrsg.), Datenschutzgrundverordnung (DSGVO): Tragweite und erste Erfahrungen/Le Règlement général sur la protection des données (RPDG): portée et premières expériences, Zürich 2020, S. 99–138.

Poltier Etienne, L'entraide administrative interne, in: Poltier Etienne/Favre Anne-Christine/Martenet Vincent (Hrsg.), L'entraide administrative, Évolution ou révolution?, Zürich 2019, S. 61–102.

Popp Peter, Grundzüge der internationalen Rechtshilfe in Strafsachen, Basel 2001.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter 16. November 2020.

Roth Florian/Mazidi Simon, Kommentierung zu Art. 54 DSG, in: Steiner Thomas/Morand Anne-Sophie/Hürlimann Daniel (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz (Version: 30.01.2024), https://onlinekommentar.ch/de/kommentare/dsg54.

Rudin Beat, Kommentierung zu Art. 5 DSG: in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023.

Schweizer Rainer J., Anforderungen der EGMR-Rechtsprechung an die internationale Amts- und Rechtshilfe, in: Lorandi Franco/Staehelin Daniel (Hrsg.), Innovatives Recht, Festschrift für Ivo Schwander, Zürich 2011, S. 985–1010 (zit. als Schweizer, FS Schwander).

Schweizer Rainer J., Kommentierung zu Art. 44 BV, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J./Vallender Klaus A. (Hrsg.), St. Galler Kommentar, Bundesverfassung, 3. Aufl., Zürich 2014.

Schweizer Rainer J., Von einer Amts- und Rechtshilfe auf Ersuchen zum internationalen Informationsverbund: Grundsätzliche Aspekte, in: Breitenmoser Stephan/Ehrenzeller Bernhard (Hrsg.), Internationale Amts- und Rechtshilfe in Steuer- und Finanzmarktsachen, Zürich 2017, S. 227–293 (zit. als Schweizer, Informationsverbund).

Seferovic Goran, Kommentierung zu Art. 21 UWG, in: Heizmann Reto/Loacker Leander D. (Hrsg.), Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Kommentar,2. Aufl., Zürich/St. Gallen 2025 (zit. als Seferovic, in: Heizmann/Loacker).

Seiler Hansjörg, Internationale Amtshilfe aus Schweizer Sicht, Liechtensteinische Juristenzeitung 32 (2011), S. 42–50.

Thurnherr Daniela, Verfahrensgrundrechte und Verwaltungshandeln, Zürich/St. Gallen 2013.

Vasella David, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, Jusletter 16. November 2015.

Vest Hans, Kommentierung zu Art. 32 BV, in: Ehrenzeller Bernhard et al. (Hrsg.), St. Galler Kommentar, Bundesverfassung, 4. Aufl., Zürich 2023.

Waldmann Bernhard, Anspruch auf den Erlass einer Verfügung, in: Häner Isabelle/Waldmann Bernhard (Hrsg.), 8. Forum für Verwaltungsrecht – Brennpunkt «Verfügung», Bern 2022, S. 55–85.

Waldmann Bernhard/Kraemer Raphael, Kommentierung zu Art. 44 BV, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar, Bundesverfassung, Basel 2015.

Weber-Dürler Beatrice/Kunz-Notter Pandora, Kommentierung zu Art. 25 VwVG, in: Auer Christoph/Müller Markus/Schindler Benjamin (Hrsg.), VwVG – Bundesgesetz über das Verwaltungsverfahren, Kommentar, 2. Aufl., Zürich 2019 (zit. als Weber-Dürler/Kunz-Notter, in: Auer/Müller/Schindler).

Weissenberger Philippe, Grenzüberschreitende Amtshilfe auf dem Prüfstand – Wege zu mehr Rechtssicherheit, Rechtsschutz und Effizienz, ASA 77 (2009), S. 825–835.

Widmer Thomas, Les amendes «administratives» prévues par l'art. 83 du RGPD peuvent-elles être reconnues et exécutées en Suisse?, sic! 2023, S. 387–390.

Wyss Martin Philipp, Gesetzgebungsbedarf bei der internationalen Amtshilfe?, in: Ehrenzeller Bernhard/Breitenmoser Stephan (Hrsg.), Aktuelle Fragen der internationalen Amts- und Rechshilfe, St. Gallen 2009, S. 217–248.

MATÉRIAUX

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988 II 413 ff. (zit. als Botschaft DSG 1988).

Botschaft zur Auferlegung der Kosten für die Behandlung zweier Amtshilfegesuche des Internal Revenue Service der Vereinigten Staaten von Amerika auf die UBS AG, BBl 2010 3211 (zit. als Botschaft Kostenauferlegung).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941 ff. (zit. als Botschaft DSG 2017)

Botschaft zur Genehmigung des Protokolls vom 10.10.2018 zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, BBl 2020 565 ff. (zit. Botschaft Konvention 108+).

Botschaft zur Totalrevision der Bundesrechtspflege, BBl 2001 4202 ff. (zit. als Botschaft Bundesrechtspflege 2001).

Bundesamt für Justiz, Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016, https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf.download.pdf/vn-ber-d.pdf, besucht am 1.8.2023 (zit. als Erl. Bericht VE).

Bundesamt für Justiz, Rechtsfragen im Zusammenhang mit der Zusammenarbeit mit ausländischen Behörden (Amtshilfe, Rechtshilfe, Souveränitätsschutz), Bericht vom 14.3.2011, https://www.bj.admin.ch/dam/bj/de/data/sicherheit/gesetzgebung/archiv/zssg/ber-auslandszusammenarbeit-d.pdf.download.pdf/ber-auslandszusammenarbeit-d.pdf, besucht am 1.10.2023 (zit. als BJ, Bericht Zusammenarbeit).

Bundesamt für Justiz, Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens vom 10.8.2017, https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/ve-ber-d.pdf.download.pdf/ve-ber-d.pdf, besucht am 1.8.2023 (zit. als Ergebnisse Vernehmlassungsverfahren DSG).

Bundesamt für Justiz, Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, Stellungnahme der Organisationen A–H, https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/organisationen-a-h.pdf.download.pdf/organisationen-a-h.pdf, besucht am 1.8.2023 (zit. als Vernehmlassungsverfahren DSG, Stellungnahme der Organisationen A–H).

Council of Europe, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a, besucht am 20.9.2023 (zit. als CoE, Explanatory Report).

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, 30. Tätigkeitsbericht 2022/23, https://edb.reader.epaper.guru/de-CH/viewer/616971da-d98a-4d01-9554-87a20c0277e9/fd949f38-fa10-4c60-a59a-0354346b8612, besucht am 9.10.2023 (zit. als EDÖB, 30. Tätigkeitsbericht 2022/23).

OECD, Review of the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy, 22.9.2023, https://www.oecd-ilibrary.org/docserver/67774f69-en.pdf?expires=1696874300&id=id&accname=guest&checksum=20FD51C34B496C02E3550F9EE3868428, besucht am 9.10.2023 (zit. als OECD 2023).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 58 LDP

Un commentaire de Myriam Christ

PROPOSITION DE CITATION

Myriam Christ, Kommentierung zu Art. 58 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Christ, N. XXX zu Art. 58 DSG.

Art. 58 Autres tâches

[1] Le PFPDT a notamment les autres tâches suivantes:

a. informer, former et conseiller les organes fédéraux et les personnes privées dans le domaine de la protection des données;

b. assister les organes cantonaux et collaborer avec les autorités chargées de la protection des données en Suisse et à l'étranger;

c. sensibiliser le public, en particulier les personnes vulnérables, à la protection des données personnelles;

d. fournir sur demande à la personne concernée des informations sur l'exercice de ses droits;

e. se prononcer sur les projets d'actes législatifs fédéraux et de mesures fédérales impliquant des traitements de données;

f. assumer les tâches qui lui sont conférées par la loi du 17 décembre 2004 sur la transparence[22] ou par d'autres lois fédérales;

g. élaborer des outils valant recommandations de bonne pratique à l'attention des responsables du traitement, des sous-traitants et des personnes concernées; ce faisant, il tient compte des particularités des différents secteurs, ainsi que du besoin de protection des personnes vulnérables.

[2] Il peut conseiller les organes fédéraux, même s'ils ne sont pas soumis à sa surveillance en vertu des art. 2 et 4. Les organes fédéraux peuvent lui donner accès à leurs dossiers.

[3] Il est autorisé à remettre aux autorités étrangères chargées de la protection des données une déclaration indiquant que, dans le domaine de la protection des données, la Suisse autorise la notification directe sur son territoire si la réciprocité lui est accordée.

TABLE DES MATIÈRES

En bref ... 758
I. Généralités ... 758
A. But de la norme et contexte ... 758
B. Historique ... 759
C. Indications de droit comparé ... 759
II. Al. 1 : Tâches particulières du PFPDT ... 760
A. Let. a : Mandat d'information ... 760
B. Let. b : Soutien aux autorités cantonales et internationales ... 762
C. Let. c : Mission de sensibilisation ... 763
D. Let. d : Mandat de conseil ... 765
E. Let. e : consultation du PFPDT dans le cadre de la procédure législative de la Confédération. ... 766
F. Let. f : tâches prévues par la LTrans. ... 767
G. Let. g : Recommandations de bonnes pratiques ... 767
III. Al. 2 : Mandat de conseil élargi ... 768
IV. Al. 3 : Entraide judiciaire internationale ... 769
Bibliographie ... 769
Matériaux ... 770

EN BREF

La liste des tâches fixée à l'art. 58 LPD complète les tâches du PFPDT déjà prévues à l'art. 57 LPD. Cette disposition prévoit par exemple que le PFPDT sensibilise la population à la protection des données, donne son avis sur les projets d'actes législatifs de la Confédération ou publie des recommandations de bonnes pratiques. La liste des tâches de l'art. 58 LPD n'est toutefois pas exhaustive. D'autres tâches non spécifiquement définies peuvent donc être assumées par le PFPDT, pour autant qu'elles soient en accord avec les objectifs fondamentaux de la LPD.

I. GÉNÉRALITÉS

A. But de la norme et contexte

1 Selon le libellé du préambule ("Le PFPDT assume en outre notamment les tâches suivantes"), l'art. 58 LPD doit être compris comme un complément ou une disposition subsidiaire à l'art. 57 LPD. L'art. 58 LPD concrétise l'étendue de l'activité de conseil et d'information du PFPDT selon l'art. 57 LPD, que le PFPDT définit en grande partie lui-même en raison de son indépendance ancrée dans la loi.

2 La liste des tâches du PFPDT n'est pas exhaustive ("en particulier"), même sous le régime du droit révisé. Le nouveau droit laisse donc une certaine marge de manœuvre pour des tâches supplémentaires, pour autant qu'elles ne soient pas contraires au but de la LPD. Dans ce contexte, il convient également de souligner que d'autres tâches du PFPDT sont définies à d'autres endroits de la LPD, par exemple à l'art. 11 LPD (avis sur les codes de conduite), à l'art. 12 al. 4 LPD (notification des listes d'activités de traitement), à l'art. 16 al. 2 LPD (communication de données à l'étranger), à l'art. 23 LPD (consultation du PFPDT dans le cadre d'évaluations d'impact sur la protection des données) ou à l'art. 24 LPD (notification des violations de la sécurité des données). D'autres tâches du PFPDT sont définies dans différentes lois spéciales, par exemple à l'art. 84b LAMal (garantie de la protection des données par les assureurs) ou à l'art. 63 al. 3 en relation avec la loi sur la protection des données. art. 64 LPD (examen par le PFPDT pour déterminer

si le SRC a traité les données personnelles du requérant conformément à la loi).

Pour de plus amples explications sur le but et le contexte de la norme, nous renvoyons aux explications générales y relatives concernant l'art. 57 LPD. 3

B. Historique

Dans le cadre de la révision, l'art. 31 aDSG a été adapté au droit de l'UE et aux directives du Conseil de l'Europe. Pour cette raison, la liste des tâches du PFPDT a été légèrement adaptée ou complétée. 4

L'art. 31 al. 1 let. d aLPD (protection adéquate des législations de protection des données à l'étranger), l'art. 31 al. 1 let. e aLPD (examen des garanties pour les transferts de données vers des Etats non équivalents) et l'art. 31 al. 1 let. f aLPD (procédure de certification) n'ont pas été repris dans l'art. 58 LPD révisé. Désormais, ce n'est plus le PFPDT, mais le Conseil fédéral ou l'OFJ qui détermine si la législation d'un Etat concerné assure une protection adéquate (art. 16 al. 1 LPD). La liste des Etats, territoires, secteurs spécifiques dans un Etat et organisations internationales disposant d'une protection des données adéquate selon le Conseil fédéral figure désormais à l'annexe 1 de l'OLPD. L'examen des garanties pour un transfert de données vers un Etat non équivalent est désormais réglé en détail à l'art. 16 al. 2 LPD et est en principe repris par le PFPDT, même sous le nouveau droit. La certification est désormais réglée à l'art. 13 LPD. Sous le droit actuel, le PFPDT ne peut plus contrôler lui-même les procédures de certification (art. 31 al. 1 let. f aDSG). Une procédure de surveillance au sens des art. 49 ss LPD reste possible. LPD demeure réservée dans ce contexte. 5

Pour de plus amples explications sur la genèse des activités de conseil et d'information des autorités de surveillance en matière de protection des données, nous renvoyons aux explications relatives à l'art. 57 LPD. 6

C. Indications de droit comparé

En droit européen, les tâches des autorités respectives de protection des données sont définies à l'article 57 du RGPD, sans préjudice d'autres tâches exposées à certains endroits du RGPD. 7

8 L'article 58 du RGPD définit les pouvoirs concrets dont disposent les autorités de contrôle pour atteindre les objectifs fixés à l'article 57 du RGPD.

9 En ce qui concerne le degré de détail, les articles 57 et 58 du RGPD vont nettement plus loin que les "réglementations sœurs" des articles 57 et 58 de la LPD. Ce souci du détail dans le droit européen de la protection des données vise à améliorer la sécurité juridique et la protection des droits fondamentaux, alors que la disposition précédente (article 28 de la directive 95/46/CE) n'offrait qu'un cadre sommaire qui, sous l'ancien droit, avait été rempli de manière très différente par les dispositions nationales. Hormis les différences formelles (niveau de détail et structure), on ne peut pas déceler de différences fondamentales sur le fond entre les dispositions européennes et les dispositions suisses. Cette constatation n'est pas surprenante : l'ancienne liste de tâches de l'art. 31 aDSG a été complétée dans le but explicite de mettre en œuvre les prescriptions du droit européen selon l'art. 46 al. 1 let. d et e de la directive (UE) 2016/680 et les exigences de l'art. 12bis ch. 2 let. e P-LPD.

II. AL. 1 : TÂCHES PARTICULIÈRES DU PFPDT

A. Let. a : Mandat d'information

10 L'art. 58 al. 1 let. a LPD a été nouvellement introduit dans la LPD dans le cadre de la révision. Cette nouvelle disposition vise à préciser le mandat d'information du PFPDT défini à l'art. 57 LPD.

11 Cette nouvelle disposition prévoit expressément que le PFPDT exerce son mandat de conseil et d'information non seulement à l'égard des organes publics, mais également à l'égard des particuliers. Cette précision linguistique, qui correspond à la pratique du PFPDT sous l'ancien droit, est à saluer.

12 Au vu tant du texte de la loi que du message, le PFPDT dispose d'une large marge de manœuvre quant à la manière dont il souhaite mettre en œuvre ce mandat d'information dans la pratique. Il est en principe libre de choisir les décideurs administratifs, politiques, scientifiques et économiques qu'il informera, formera ou conseillera. Toutefois, la marge d'appréciation du PFPDT n'est pas sans limites : L'indépendance du PFPDT doit toujours être respectée, même lors de la mise en œuvre du mandat d'information au sens de l'art. 58 al. 1 let. a LPD. Dans la pratique, il peut arriver que le PFPDT lui-même ou des membres de sa direction entretiennent des contacts personnels

trop étroits avec certains décideurs et que ces contacts ou échanges donnent à des tiers l'impression que le PFPDT est partial ou qu'il influence le PFPDT dans une éventuelle procédure de surveillance en aval.

Dans le cadre de son mandat d'information, le PFPDT participe par exemple à la journée annuelle du droit de la protection des données de l'Université de Fribourg, publie des guides, des lettres-types et des FAQ concernant des traitements de données effectués par des organes fédéraux ou des particuliers, conseille des particuliers aussi bien par téléphone que par écrit ou échange régulièrement des informations avec l'Association pour la protection des données en entreprise (VUD). Il peut également organiser des séances d'information ou des formations continues pour les responsables du secteur public. Sous le mot-clé "former", une collaboration avec les différentes facultés de droit serait également envisageable. Actuellement, le droit de la protection des données n'est un cours obligatoire dans aucune université suisse. En l'état actuel, les futurs juristes ne sont pas du tout ou pas suffisamment préparés aux défis que pose la pratique juridique dans ce domaine transversal qu'est la protection des données. 13

Désormais, le PFPDT peut percevoir des émoluments pour les conseils donnés aux particuliers en matière de protection des données conformément à l'art. 58 al. 1 LPD, en vertu de l'art. 59 al. 1 let. e LPD en relation avec l'art. l'art. 44 OLPD, des émoluments sont perçus. Ces émoluments sont calculés en fonction du temps consacré, un tarif horaire de 150 à 250 CHF étant appliqué. 14

Dans l'optique, entre autres, d'une mise en œuvre efficace et à l'échelle nationale de ce mandat d'information normé par la loi, il est également décisif, sous le nouveau droit, que le PFPDT et son suppléant ne proviennent pas de la même région linguistique. En principe, le PFPDT et son suppléant devraient donc continuer à être responsables de la mise en œuvre du mandat d'information dans leur région d'origine respective (p. ex. répondre aux demandes d'interviews). 15

Plus le PFPDT exerce son mandat d'information par divers canaux, plus il est susceptible d'informer un large public sur les défis actuels en matière de protection des données. Toutefois, la mise en œuvre effective du mandat d'information dépend des ressources en personnel disponibles, qui restent modestes. 16

B. Let. b : Soutien aux autorités cantonales et internationales

17 L'art. 58 al. 1 LPD let. b est issu de l'art. 31 al. 1 let. a et let. c aDSG. Selon le libellé explicite de la loi, le soutien aux autorités cantonales et internationales ne constitue pas un cas particulier de l'activité de conseil du PFPDT. Le PFPDT ne peut "que" soutenir les autorités cantonales et non pas les "conseiller". En raison de la répartition des compétences entre la Confédération et les cantons, il n'appartient pas au PFPDT, dans la mesure où les services cantonaux de protection des données sont compétents, de conseiller les organes cantonaux. Sous l'ancien droit, la formulation de la loi ("organes des cantons") excluait que le PFPDT assiste également les communes. Désormais, en raison d'une légère adaptation de la formulation de la loi ("autorités suisses"), il est envisageable que le PFPDT assiste également des organes communaux. En raison de la répartition des compétences dans le domaine de la protection des données, les organes communaux devraient toutefois continuer à s'adresser en pratique au service cantonal de protection des données compétent en cas de questions ou d'incertitudes.

18 Sous l'ancien droit, il n'était pas clair, en raison de la formulation de la loi, si la disposition en question ne s'appliquait qu'aux organes publics ou si elle englobait également les services de protection des données d'entreprises privées. Au vu du libellé actuel de l'art. 58 al. 1 let. b LPD, il est clair que le champ d'application de cette disposition se limite aux organes publics.

19 Il découle de ce qui précède que les consultations du PFPDT doivent se limiter aux domaines pour lesquels les cantons ne sont pas compétents (consultations de personnes privées et d'organes fédéraux, cf. art. 58 al. 1 let. a LPD) ainsi qu'aux clarifications concernant la délimitation des compétences entre la Confédération et les cantons. Une véritable collaboration dans des cas individuels concrets n'a pas lieu en raison de la répartition des compétences entre la Confédération et les cantons. En ce sens, le libellé choisi ("collabore avec les autorités suisses") est trompeur.

20 L'assistance fournie par le PFPDT au sens de l'art. 58 al. 1 let. b LPD n'est toujours soumise à aucune forme et reste gratuite sous le nouveau droit.

21 Au vu des problématiques de plus en plus transnationales, le soutien des autorités étrangères devient de plus en plus important. Au regard de l'art. 58 al. 1 let. b LPD, le PFPDT n'échange pas seulement avec des représentants des autorités cantonales, mais siège également dans diverses organisations

internationales et soutient dans ce cadre les autorités étrangères ou internationales dans la mise en œuvre d'une protection des données efficace à l'échelle mondiale.

En raison de son indépendance fixée par la loi, le PFPDT doit toujours pouvoir décider lui-même si et dans quelle mesure il souhaite soutenir une autre autorité. Un mandat de soutien contraignant ne serait pas compatible avec l'indépendance du PFPDT. 22

En ce qui concerne les limites de l'assistance offerte par le PFPDT, il convient de relever que l'art. 58 al. 1 let. b LPD ne constitue ni une base pour une compétence fédérale en matière de protection des données, ni une base pour un échange d'informations avec d'autres autorités (nationales ou internationales). Cette disposition devrait uniquement permettre un échange professionnel entre autorités et ainsi permettre aux autres organes publics de profiter des connaissances juridiques et techniques du PFPDT. 23

Depuis la création de "privatim", les échanges avec les autorités cantonales sont organisés par des représentants de cette association ou par certains groupes de travail. Dans la pratique, il s'est avéré à plusieurs reprises que les échanges entre la Confédération et les représentants des cantons sont enrichissants dans les domaines où leurs compétences respectives se recoupent, notamment lors de la pandémie du Covid-19, qui a soulevé diverses questions de protection des données dans le domaine de la santé non seulement au niveau cantonal, mais aussi au niveau national (et international). Récemment, le PFPDT et "privatim" ont révisé ensemble leur guide "Elections et votations" dans la perspective des élections fédérales de 2023 : Les élections et les votations se déroulent à tous les niveaux fédéraux et sont confrontées à des défis similaires à tous les niveaux fédéraux. 24

C. Let. c : Mission de sensibilisation

L'art. 58 al. 1 let. c LPD précise le mandat de sensibilisation du PFPDT défini à l'art. 57 LPD. 25

La sensibilisation des personnes vulnérables a été nouvellement introduite dans la LPD en s'inspirant du droit européen (art. 57 al. 1 let. b RGPD). La notion de "personnes vulnérables" n'est toutefois définie ni à l'art. 58 LPD ni à l'art. 5 LPD (définitions). Dans le message, les mineurs et les personnes âgées sont mentionnés comme personnes vulnérables. En raison du choix des 26

termes ("notamment"), cette énumération n'est pas exhaustive. Les malades et les réfugiés, par exemple, devraient également être considérés comme des personnes particulièrement dignes de protection au sens de l'art. 58 al. 1 let. c LPD, surtout si l'on considère que dans ces cas de figure, des données personnelles sensibles sont souvent traitées au sens de l'art. 5 let. c ch. 1, 2 ou 5 LPD. Le PFPDT intervient par exemple chaque année au sujet du traitement de données personnelles dans le domaine de la santé.

27 Sous l'ancien droit, le PFPDT s'est déjà efforcé de sensibiliser les jeunes à la protection des données. Il a par exemple conçu sept leçons pour les élèves des niveaux secondaires I et II, chacune consacrée à un thème particulier pertinent pour les jeunes dans leur vie quotidienne. Il a également publié sur son site web des conseils pour les nouveaux parents. Le service interactif de sensibilisation à la protection des données et à la transparence dans les organisations "Think Data", soutenu par le PFPDT, s'adresse aussi explicitement, entre autres, aux étudiantes et aux étudiants. La mission de sensibilisation des enfants et des jeunes connaît toutefois aussi ses limites. Selon l'art. 62 al. 1 Cst., l'éducation est l'affaire des cantons. Il appartient donc en premier lieu aux directrices et directeurs cantonaux de l'éducation de s'occuper de la sensibilisation à la protection des données pendant la scolarité obligatoire.

28 En ce qui concerne le mandat de sensibilisation des personnes âgées, il n'existe actuellement aucune collaboration spécifique avec une organisation active dans ce domaine ou un projet s'adressant spécialement à ce groupe social. Une collaboration avec "pro senectute" ou d'autres associations ou groupements d'intérêts serait envisageable ou souhaitable sur la base de l'art. 58 al. 1 let. c LPD.

29 L'attribution de prix et de distinctions sur le modèle, par exemple, du Rodotà Award du Conseil de l'Europe ou des Big Brother Awards du Chaos Computer Club Suisse serait une possibilité de sensibiliser la population civile d'une manière un peu différente.

30 Lors de la mise en œuvre du mandat de sensibilisation du PFPDT, il faut toutefois toujours garder à l'esprit qu'il s'agit - comme dans le cadre de la lutte contre le changement climatique - de sensibiliser le grand public à un danger dont les conséquences ne se feront sentir ou ne seront perceptibles qu'à un

stade ultérieur. Le travail de sensibilisation s'en trouve considérablement compliqué.

D. Let. d : Mandat de conseil

Le mandat de conseil du PFPDT a été expressément introduit dans la LPD dans le cadre de la révision. La loi reflète ainsi un changement observé dans la pratique : contrairement à ce que le législateur de 1988 avait prévu, ce n'est pas la surveillance, mais le conseil aux personnes privées qui constitue l'essentiel de l'activité du PFPDT : 31

L'application individuelle des droits par le biais des tribunaux civils (art. 32 al. 2 LPD), prévue par le législateur, joue un rôle secondaire, voire (presque) inexistant, dans la pratique. Face à une procédure longue et coûteuse à l'issue incertaine, il est extrêmement rare que les personnes concernées engagent une procédure devant le tribunal compétent. Ceci est d'autant plus vrai que de plus en plus de traitements de données sont effectués par des personnes privées ayant leur siège à l'étranger et qu'ils entraînent une atteinte à la personnalité en Suisse. Une procédure prometteuse devant un tribunal civil suisse devient ainsi (presque) impossible ou plus difficile. Par conséquent, les questions de principe relatives à la protection des données ne sont guère abordées dans la jurisprudence, et les rares décisions de justice n'ont qu'une portée limitée au-delà du cas d'espèce. Le PFPDT joue donc un rôle important dans l'application du droit grâce à son mandat de conseil. 32

Le PFPDT est libre quant à la forme. Il exerce son mandat de conseil aussi bien oralement (hotline) que par écrit (formulaire de contact, modèles de lettres ou de plaintes, guides, FAQ, communiqués de presse, Twitter). 33

Contrairement aux conseils donnés aux "personnes privées en matière de protection des données" selon l'art. 58 al. 1 let. a LPD, les "renseignements sur la manière dont une personne privée peut exercer ses droits" selon l'art. 58 al. 1 let. d LPD en liaison avec l'art. l'art. 59 al. 1 let. e a contrario LPD est gratuit. Il va de soi que la délimitation entre le champ d'application de la let. a et celui de la let. d LPD risque d'être difficile dans la pratique. Dans l'intérêt de l'égalité de droit, il faut espérer que le PFPDT fera généreusement usage de l'exception prévue à l'art. 59 al. 3 LPD (renonciation à la perception d'émoluments) dans ce contexte. 34

35 Dans le cadre de ses consultations, le PFPDT apprend de première main dans quels domaines ou dans quelles entreprises il existe éventuellement des problèmes en matière de protection des données. Une mise en œuvre aussi large que possible du mandat de conseil contribue ainsi notamment à ce que le PFPDT puisse remplir efficacement son mandat de surveillance selon les art. 49 ss LPDS. LPD de manière efficace.

E. Let. e : consultation du PFPDT dans le cadre de la procédure législative de la Confédération.

36 La consultation du PFPDT dans le cadre de la procédure législative fédérale est un cas particulier du mandat de conseil du PFPDT.

37 Selon la nouvelle teneur de la loi, le préposé doit être consulté sur tous les projets d'actes législatifs et de mesures de la Confédération qui concernent un traitement de données (et pas seulement sur les projets qui touchent de manière importante à la protection des données). Cette précision linguistique reflète la pratique sous l'ancien droit et doit être saluée dans l'optique de la sécurité juridique.

38 L'art. 38 al. 2 OLPD précise encore cette obligation pour tous les organes fédéraux : Les organes fédéraux soumettent au PFPDT tous les projets législatifs qui concernent le traitement de données personnelles, la protection des données et l'accès aux documents officiels.

39 Le délai interne (non officiel) pour prendre position dans le cadre des consultations des offices est de trois semaines. Dans la pratique, tous les offices ne respectent toutefois pas cet accord officieux. Dans certains cas, le délai très court pour prendre position peut entraîner une baisse de la qualité de l'avis du PFPDT. Il faut espérer que ce délai sera à nouveau plus souvent respecté après la fin de la pandémie de Corona. Un retour au "courant normal" permettrait au PFPDT de préparer soigneusement ses prises de position et, s'il le juge nécessaire, de rechercher le dialogue avec l'office fédéral compétent et de trouver une solution acceptable pour tous les services impliqués.

40 Si le PFPDT a été écarté de la procédure législative et qu'il estime que cette information présente un intérêt public, il peut s'adresser directement au public en vertu de l'art. 57 al. 2 LPD (en relation avec l'art. 39 let. i OLPD).

La notion de "mesures" est une notion floue. Ce flou linguistique permet au PFPDT de siéger dans différents organes ou groupes de travail. En vertu de l'art. 58 al. 1 let. e LPD, le PFPDT peut donc être impliqué dès la première phase d'un nouveau projet relevant de la protection des données. Par exemple, le PFPDT a été consulté très tôt dans le cadre de la stratégie d'informatique en nuage de l'administration fédérale. Le SECO a également fait appel aux conseils du PFPDT lors de la révision des directives relatives à l'art. 26 OLT 3, qui ont été publiées en février 2023. Il convient toutefois de préciser que le fait de consulter le PFPDT au début d'un nouveau projet n'exclut pas que le PFPDT, dans le cadre de son activité de surveillance au sens des art. 49 ss LPD, puisse intervenir dans le cadre d'un nouveau projet. LPD, le projet en question sera examiné a posteriori. En d'autres termes, la consultation du PFPDT ne doit pas être confondue avec une sorte de "procédure de certification". 41

F. Let. f : tâches prévues par la LTrans.

La mention des tâches du PFPDT selon la LTrans a un caractère purement déclaratoire. Les tâches du PFPDT en rapport avec le principe de transparence découlent directement de l'art. 18 LTrans (direction de la procédure de médiation, relations publiques, consultation dans le cadre de la procédure législative) et de l'art. 19 LTrans (évaluation). 42

La coordination entre la LPD et la LTrans est régie par les art. 7, al. 2, et 9 LTrans ou par l'art. 36, al. 3, LPD. 43

La question de savoir si la protection des données ou le principe de transparence sont servis lorsque la même autorité doit, d'une part, s'engager pour une protection des données efficace et, d'autre part, accorder le plus grand accès possible aux documents officiels est controversée. La solution suisse est également en vigueur dans certains autres pays, comme l'Allemagne (au niveau fédéral) ou la Grande-Bretagne. La France, en revanche, a confié chacune de ces deux tâches à deux autorités différentes. Au niveau européen, le compromis à ce sujet est réglé par l'article 86 du DSGVO. 44

G. Let. g : Recommandations de bonnes pratiques

L'art. 58 al. 1 let. g LPD a été nouvellement introduit dans la LPD dans le cadre de la révision. Le PFPDT s'acquittait toutefois déjà intensivement de cette 45

tâche dans le cadre de son activité de conseil sous l'ancien droit, en publiant de nombreux guides, modèles de lettres et FAQ sur son site Internet.

46 La publication des recommandations de bonnes pratiques est, tout comme la consultation du PFPDT dans le cadre de la procédure législative au niveau fédéral (art. 58 al. 1 let. e LPD), un cas particulier de l'activité de conseil du PFPDT. En ce qui concerne les recommandations de bonnes pratiques, il faut également souligner que la mise en œuvre des recommandations n'exclut pas toute procédure de surveillance. En d'autres termes, les recommandations ne sont pas juridiquement contraignantes. Le PFPDT ne peut pas légiférer sur la base de l'art. 58 al. 1 let. g LPD. Un éventuel tribunal saisi décidera, indépendamment des éventuelles recommandations du PFPDT, s'il y a ou non violation de la LPD dans un cas particulier. Le fait qu'une personne privée ait suivi les recommandations du PFPDT peut toutefois jouer un rôle important dans l'examen de la faute dans le cadre d'actions en réparation.

47 En ce qui concerne la notion de personnes vulnérables, on peut se référer aux explications précédentes relatives à l'art. 58 al. 1 let. c LPD.

III. AL. 2 : MANDAT DE CONSEIL ÉLARGI

48 Du point de vue du contenu, l'art. 58 al. 2 LPD correspond à l'art. 31 al. 2 aDSG.

49 Certains traitements de données sont exclus du champ d'application de la LPD en vertu de l'art. 2 al. 2, 3 et 4 LPD et de l'art. 4 al. 2 LPD. L'art. 58 al. 2 LPD permet au PFPDT, s'il le souhaite, de prendre position sur des questions qui sont exclues du champ d'application de la LPD conformément au texte de loi. La précision linguistique apportée dans la deuxième phrase clarifie le fait que les organes fédéraux éventuellement concernés peuvent autoriser le PFPDT à consulter les dossiers. En d'autres termes, le secret de fonction est levé dans ces cas.

50 L'art. 58 al. 2 LPD est une disposition dite "potestative". Contrairement aux tâches définies à l'al. 1, il n'existe aucun droit pour les mandats de conseil mentionnés à l'al. 2.

51 La liste fixée à l'art. 58 al. 1 LPD n'est pas exhaustive. Il est donc admissible que le PFPDT conseille également sur des traitements de données qui n'entrent pas dans le champ d'application de la LPD (cf. art. 2 al. 2 let. a LPD).

Cette possibilité est l'expression du fait que l'art. 13 Cst. a une portée générale et ne s'applique pas uniquement aux domaines dans lesquels la LPD est applicable.

En raison des ressources toujours limitées du PFPDT, l'art. 58 al. 2 LPD sera probablement rarement appliqué, tout comme la disposition qui l'a précédé. 52

Par souci d'exhaustivité, il convient de préciser que dans les domaines où la LPD n'est pas applicable, toute activité de surveillance du PFPDT est exclue, par exemple dans une procédure civile en cours. 53

IV. AL. 3 : ENTRAIDE JUDICIAIRE INTERNATIONALE

L'art. 58 al. 3 LPD a été ajouté à la LPD dans le cadre de la révision. Cette disposition a pour but de simplifier la transmission de documents officiels aux responsables privés de la protection des données qui ont leur siège à l'étranger, mais qui doivent désigner une représentation en Suisse conformément à l'art. 14 LPD. 54

BIBLIOGRAPHIE

Baeriswyl Bruno, Datenschutzgesetzgebung in der Schweiz – Standortbestimmung und Ausblick, in: Kieser Ueli/Pärli Kurt (Hrsg.), Datenschutz im Arbeits-, Versicherungs- und Sozialbereich: Aktuelle Herausforderungen, St. Gallen 2012, S. 10 ff. (zit. Baeriswyl, Standortbestimmung).

Baeriswyl Bruno, Kommentierung zu Art. 31 aDSG, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 1. Aufl., Bern 2015 (zit. SHK-Baeriswyl, Art. 31 aDSG).

Belser Eva Maria, § 5 Die Kompetenzverteilung zwischen Bund und Kantonen, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard (Hrsg.), Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, S. 4 ff. (zit. Belser).

Cottier Bertil, Transparence et protection des données, Une relation amour-haine?, in: Waldmann Bernhard/Bergamin Florian (Hrsg.), 10 Jahre InfoG Freiburg, Bern 2021, S. 159 ff. (zit. Cottier).

Huber René, Kommentierung zu Art. 31 aDSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. BSK-Huber, Art. 31 aDSG).

Jöhri Yvonne, §8 Aufgabe und Bedeutung der öffentlichen Datenschutzbeauftragten, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht: Beraten in Privatwirtschaft und öffentlicher Verwaltung, Handbücher für die Anwaltspraxis, Basel 2015, S. 245 ff. (zit. Jöhri).

Meier Philippe, Protection des données: fondements, principes généraux et droit privé, Berne 2011 (zit. Meier).

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. Rosenthal/Jöhri).

Specht Louisa/Bienemann Linda, Kommentierung zu Art. 86 DSGVO, in: Sydow Gernot (Hrsg.), Nomos Handkommentar, Europäische Datenschutzgrundverordnung, 2. Aufl., Baden-Baden 2018 (zit. NHK-Specht/Bienemann, Art. 86 DSGVO).

Waldmann Bernhard/Oeschger Marcus, §15 Aufsicht, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011 (zit. Waldmann/Oeschger).

Ziebarth Wolfgang, Kommentierung zu Art. 57 DSGVO, in: Sydow Gernot (Hrsg.), Nomos Handkommentar, Europäische Datenschutzgrundverordnung, 2. Aufl., Baden-Baden 2018 (zit. NHK-Ziebarth, Art. 57 DSGVO).

Ziebarth Wolfgang, Kommentierung zu Art. 58 DSGVO, in: Sydow Gernot (Hrsg.), Nomos Handkommentar, Europäische Datenschutzgrundverordnung, 2. Aufl., Baden-Baden 2018 (zit. NHK-Ziebarth, Art. 58 DSGVO).

MATÉRIAUX

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988 (zit. BBl 1988 II S. 413 ff.).

Zusammenstellung der Ergebnisse des Vernehmlassungsverfahrens zum Bundesgesetz über die Öffentlichkeit der Verwaltung (Öffentlichkeitsgesetz, BGÖ) vom März 2001 (zit. Zusammenstellung Vernehmlassungsverfahren).

Gutachten 051124 des Bundesamtes für Justiz, VPB 70.54, vom 24.11.2005 (zit. Gutachten des BJ, VPB 70.54).

Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9.12.2011 (zit. BBl 2012 S. 335 ff.).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017 (zit. BBl 2017 S. 6941 ff.).

28. Tätigkeitsbericht des EDÖB 2020/2021 vom 31.3.2021 (zit. EDÖB, 28. Tätigkeitsbericht 2020/2021).

29. Tätigkeitsbericht des EDÖB 2021/2022 vom 31.3.2022 (zit. EDÖB, 29. Tätigkeitsbericht 2021/2022).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 57 LPD

Un commentaire de Myriam Christ

PROPOSITION DE CITATION

Myriam Christ, Kommentierung zu Art. 57 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Christ, N. XXX zu Art. 57 DSG.

Art. 57 Information

[1] Le PFPDT remet annuellement un rapport sur son activité à l'Assemblée fédérale. Il transmet simultanément ce rapport au Conseil fédéral. Le rapport est publié.

[2] S'il en va de l'intérêt général, le PFPDT informe le public de ses constatations et de ses décisions.

TABLE DES MATIÈRES

En bref 775
I. Généralités 775
A. But de la norme et contexte 775
B. Historique 777
C. Remarques de droit comparé 778
II. Al. 1 : Publication annuelle du rapport d'activité. 779
A. Publication annuelle 779
B. Rapport d'activité 780
III. Al. 2 : Publication de constatations et de décisions d'intérêt général. 782
A. Constatation 782
B. Décision 783
C. Intérêt général 783
D. Publication 784
Bibliographie 787
Matériaux 788

EN BREF

La disposition relative aux relations publiques du PFPDT fait partie des dispositions les plus importantes, mais moins connues, de la loi sur la protection des données. Les expériences internationales ont montré dès les années 1980 qu'une mise en œuvre réussie des prescriptions légales en matière de protection des données nécessite un dialogue entre l'autorité de surveillance et les autres autorités fédérales ou la population civile (p. ex. lorsqu'il s'agit de mettre en évidence une nécessité de légiférer ou d'exercer une pression sur certains responsables qui ne respectent pas les prescriptions légales).

L'art. 57 al. 1 LPD oblige le PFPDT à informer une fois par an l'Assemblée fédérale - organe de nomination du PFPDT selon l'art. 43 al. 1 LPD - de ses activités. Le Conseil fédéral est informé par écrit des activités du PFPDT. Le deuxième alinéa doit permettre au PFPDT d'exercer son mandat d'information indépendamment des autorités fédérales surveillées. La disposition est formulée de manière très ouverte. Le PFPDT dispose donc de nombreuses possibilités pour exercer son mandat légal d'information.

I. GÉNÉRALITÉS

A. But de la norme et contexte

L'art. 57 LPD ne fait pas partie des dispositions les plus connues de la LPD. 1
Pourtant, cette disposition légale relative au travail de relations publiques du PFPDT contribue de manière décisive à la mise en œuvre pratique des prescriptions en matière de protection des données. En effet, la sensibilisation au droit de la protection des données, tant dans le secteur privé que dans le secteur public, est surtout renforcée par le travail de relations publiques du PFPDT (et des commissaires cantonaux et communaux à la protection des données). Une sensibilisation réussie du public à la protection des données passe par un dialogue entre l'autorité de surveillance et le public. Les réflexions ou les mesures relevant du droit de la protection des données ne doivent donc pas rester purement internes aux services traitant des données, que ce soit dans le domaine privé ou public, mais être présentées à la population de manière très consciente et proactive.

2 La sensibilisation du public visée par le travail de relations publiques du PFPDT poursuit plusieurs objectifs concrets. D'une part, elle contribue à renforcer l'efficacité de l'activité de surveillance du PFPDT (art. 49 à 53 LPD) - dans le cadre de son activité de surveillance, le PFPDT peut sanctionner les traitements de données illicites. Sur la base de l'art. 57 LPD, il peut publier ses résultats et exercer ainsi une pression sur le responsable de la protection des données fautif et encourager d'autres responsables de la protection des données, non directement concernés par l'enquête, à adapter leur pratique. D'autre part, le travail de relations publiques du PFPDT peut le décharger de manière décisive dans son activité de conseil (art. 58 LPD). La publication d'outils faciles à comprendre, tels que des guides, des modèles de lettres ou des FAQ, contribue de manière décisive à réduire le temps consacré au conseil personnel et à prévenir les violations potentielles de la protection des données.

3 En outre, le PFPDT peut, sur la base de son travail de relations publiques, rendre compte de son activité à l'organe de nomination (Assemblée fédérale selon l'art. 43 al. 1 LPD) et donner ainsi à l'Assemblée fédérale un aperçu de sa gestion.

4 Le travail de relations publiques au sens de l'art. 57 LPD offre au PFPDT la possibilité de publier des informations sur des développements problématiques et de mettre en évidence ce qu'il considère comme un besoin d'agir au niveau législatif.

5 En l'occurrence, il convient de constater que l'application individuelle des droits par le biais des tribunaux civils (art. 32 al. 2 LPD), prévue par le législateur, joue un rôle secondaire, voire (presque) inexistant, dans la pratique. Face à une procédure longue et coûteuse à l'issue incertaine, il est extrêmement rare que les personnes concernées engagent une procédure devant le tribunal compétent. Ceci est d'autant plus vrai que de plus en plus de traitements de données sont effectués par des personnes privées à l'étranger. Une procédure prometteuse devant un tribunal civil suisse devient ainsi (presque) impossible. Par conséquent, les questions de principe de la protection des données sont rarement abordées dans la jurisprudence et les rares décisions de justice n'ont qu'une portée limitée au-delà du cas d'espèce. Le PFPDT joue donc un rôle important dans l'application du droit grâce à son travail de relations publiques.

B. Historique

Ad al. 1 :

Une disposition très similaire à l'al. 1 actuel figurait déjà à l'art. 30 aDSG. S'appuyant sur les expériences internationales qui avaient déjà montré dans les années 1980 que la sensibilisation au droit de la protection des données était renforcée notamment par le travail de relations publiques des autorités de protection des données, cette disposition avait été introduite dans le droit suisse en 1988 et était entrée en vigueur en 1992. 6

L'art. 30a LPD n'a pas donné lieu à des débats au Parlement - l'article correspondait au projet du Conseil fédéral de 1988. Il en va de même pour l'art. 57 LPD. Dans le cadre de la révision, la disposition a uniquement été précisée dans la mesure où le PFPDT doit désormais établir un rapport annuel (et non plus périodique). Cette précision correspond à la pratique sous l'ancien droit. 7

Le PFPDT fait rapport à l'Assemblée fédérale et donne ainsi à l'organe électoral une vue d'ensemble de l'exercice de sa fonction. Comme sous l'ancien droit, le Conseil fédéral ne reçoit que le rapport d'activité écrit. 8

En outre, l'expression "et en cas de besoin" a été supprimée. Désormais, le PFPDT rendra compte une fois par an. Ni l'évaluation de la procédure de consultation ni le message ne font référence à cette suppression. Dans la pratique, la possibilité d'informer le public également en cas de besoin (c'est-à-dire à tout moment et pas seulement une fois par an) n'a pas joué un grand rôle. En outre, il convient de souligner que le PFPDT peut, si nécessaire, informer le public de ses activités en vertu de l'art. 57 al. 2 LPD. 9

Ad al. 2 :

L'art. 57 al. 2 LPD a été raccourci dans le cadre de la révision par rapport à l'al. 2 de l'ancienne LPD. Dans le sens d'un renforcement de l'indépendance du PFPDT, déjà souhaité en décembre 2011, le PFPDT peut désormais décider lui-même de ce dont il informe le public. La publication de données personnelles soumises au secret de fonction ne dépend plus de l'accord de l'autorité concernée et il n'est plus prévu de distinguer expressément les données personnelles des données matérielles dans le cadre du mandat d'information du PFPDT. 10

11 Le deuxième alinéa précise en outre que le PFPDT "informe" et non plus simplement "peut informer" sur les constatations d'intérêt général. Cette précision linguistique est à saluer, mais ne change pas grand-chose dans la pratique. La disposition "peut" de l'ancien droit établissait déjà un mandat d'information contraignant.

C. Remarques de droit comparé

Ad al. 1 :

12 L'établissement régulier d'un rapport d'activité était déjà prévu à l'art. 28 al. 5 de la directive 95/46/CE et est régi depuis le 25 mai 2018 par l'art. 59 du DSGVO. Du point de vue du contenu, cette disposition se distingue de l'art. 57 al. 1 LPD dans la mesure où la règle correspondante du droit européen définit un contenu possible du rapport d'activité (liste des types de violations signalées et des types de mesures prises conformément à l'art. 58 al. 2 RGPD).

13 L'art. 15 al. 7 STE 108 stipule que chaque autorité de contrôle européenne prépare régulièrement un rapport d'activité et le publie ensuite. Selon le rapport explicatif, un rapport d'activité doit être publié une fois par an. Ce rapport doit notamment contenir des informations sur les mesures prises pour faire respecter la législation nationale en matière de protection des données. A l'exception du fait que la LPD révisée ne comporte pas de prescriptions relatives au contenu, le législateur suisse a repris aussi bien les prescriptions du Conseil de l'Europe que celles de l'UE. Il va toutefois de soi que les mesures prises pour faire respecter les dispositions de protection des données sont mentionnées dans le rapport d'activité du PFPDT, même en l'absence de dispositions légales correspondantes.

Ad al. 2 :

14 L'art. 15 al. 2 let. e STE 108 fixe le cadre des tâches de sensibilisation des autorités de surveillance. Selon le rapport explicatif, les autorités de surveillance doivent rendre visibles de manière proactive les mesures qu'elles prennent, leurs tâches et leurs compétences. Elles peuvent à cet effet publier des rapports d'activité périodiques (cf. art. 15 al. 7 STE 108), des avis ou des recommandations générales. Ils peuvent en outre sensibiliser le public par d'autres canaux de communication qu'ils choisissent librement. Selon le rapport explicatif, le travail de relations publiques consiste également à informer les personnes et les responsables de leurs droits et obligations

respectifs dans un langage approprié, c'est-à-dire facilement compréhensible (surtout lorsque le traitement de données concerne des enfants ou d'autres personnes particulièrement vulnérables).

II. AL. 1 : PUBLICATION ANNUELLE DU RAPPORT D'ACTIVITÉ.

A. Publication annuelle

Dans le cadre de la révision, l'art. 30 aDSG a été légèrement précisé : la publication doit avoir lieu "chaque année". Cette précision avait été souhaitée lors de la procédure de consultation, mais elle ne change pas grand-chose dans la pratique. La loi ne contient toujours pas de directives sur le moment de la publication. Sous l'ancien droit, l'habitude avait été prise que le rapport couvre la période allant du 1er avril au 31 mars de l'année suivante et qu'il soit publié fin juin. Une conférence de presse est organisée à l'occasion de la publication. Le PFPDT présente personnellement le rapport, souvent accompagné d'un autre collaborateur de la direction, et répond aux questions des journalistes. Rien n'indique que cette pratique ne sera pas maintenue sous le nouveau droit. 15

Le rapport n'est pas soumis au Conseil fédéral ou à l'Assemblée fédérale pour une éventuelle adaptation, ni avant ni après sa publication. En d'autres termes, le rapport est publié de la même manière qu'il est soumis à l'Assemblée fédérale et au Conseil fédéral (voir les directives à ce sujet à l'art. 37 OLPD). Le PFPDT exerce entre autres la surveillance des traitements de données effectués par les organes fédéraux. On peut donc imaginer que, selon les résultats de l'enquête, des organes fédéraux soumis à un contrôle prudentiel pourraient exiger certaines adaptations du rapport d'activités. Dans ce contexte, la publication du rapport d'activités inchangé est à saluer et contribue à renforcer l'indépendance du PFPDT. 16

Il n'est pas prévu de présenter le rapport d'activités devant la commission chargée de préparer l'élection du PFPDT ou devant les Chambres, même si la doctrine en fait parfois la demande. 17

B. Rapport d'activité

18 Le rapport d'activité est la pièce maîtresse du travail de relations publiques du PFPDT (cf. art. 57 al. 2 et art. 58 LPD pour d'autres possibilités de sensibiliser le public).

19 Contrairement au droit européen - c'est-à-dire l'art. 59 RGPD et l'art. 15 al. 7 STE 108 - en Suisse, ni la LPD ni l'OLPD ne fixent de directives quant au contenu. Le PFPDT décide donc en principe librement du contenu du rapport d'activité. Conformément à l'art. 58 al. 1 let. f LPD, le préposé assume également les tâches qui lui sont confiées par la loi du 17 décembre 2004 sur la transparence (LTrans, RS 152.3). Selon l'art. 19 LTrans, le Préposé fédéral à la transparence est tenu de présenter régulièrement un rapport au Conseil fédéral et de le publier. Depuis l'entrée en vigueur de la LTrans le 1er juillet 2006, le PFPDT publie un rapport d'activités qui retrace à la fois ses activités de préposé à la protection des données et ses tâches de préposé à la transparence.

20 Année après année, le rapport d'activité suit une structure similaire, mais la pondération des différents thèmes peut varier : Défis actuels, Protection des données (numérisation et droits fondamentaux ; justice, police, sécurité ; fiscalité et finances ; commerce et économie ; santé ; travail ; assurances ; transports ; international), Principe de transparence (généralités ; demandes d'accès ; procédures de médiation ; procédures législatives), Le PFPDT (tâches et ressources ; communication ; statistiques ; organisation du PFPDT). Le PFPDT met en outre l'accent sur plusieurs thèmes dans chaque rapport d'activités. Par exemple, dans le rapport d'activités 2020/2021, il a consacré son premier thème à la LPD révisée et son deuxième thème au Privacy Shield et aux défis qui y sont liés.

21 Comme toutes les autorités fédérales, le PFPDT doit, dans l'exercice de ses tâches légales, respecter les dispositions légales en vigueur, notamment celles relatives à la protection des secrets de fabrication et d'affaires. Il est en outre soumis au secret de fonction selon l'art. 22 de la loi sur le personnel de la Confédération (LPers, RS 172.220.1). Par conséquent, il doit garantir le traitement confidentiel des données personnelles auxquelles il a accès dans l'exercice de ses tâches de surveillance, notamment lorsqu'il publie son rapport d'activité.

En raison de la brièveté des articles du rapport d'activité (sous l'ancien droit, environ une colonne par enquête prudentielle), il est difficile d'imaginer que des secrets de fabrication ou d'affaires soient divulgués dans le rapport d'activité, contrairement à ce qui se passe lors de la publication de décisions. 22

Dans la pratique, le PFPDT rend anonymes les noms des personnes privées contre lesquelles une procédure de droit de surveillance a été ouverte, mais n'est pas encore terminée. Dès que la procédure est terminée, le nom de la personne morale concernée est mentionné dans le rapport d'activité qui suit. La mention du nom des entreprises fautives n'est pas toujours agréable pour les personnes concernées, mais elle ne relève pas du secret de fabrication ou du secret d'affaires. En outre, la mention des noms des responsables fautifs est couverte par le but normatif de l'art. 57 al. 1 LPD, car le travail de relations publiques du PFPDT vise notamment à exercer une pression sur le responsable fautif et à encourager d'autres responsables de la protection des données qui ne sont pas directement concernés par l'enquête à adapter leur pratique. 23

Il en va autrement des secrets de fonction, qui peuvent également être révélés sur une ligne. Toutefois, dans ces cas, l'intérêt public à informer le public sur les traitements de données illégaux effectués par les autorités fédérales - également au vu de la responsabilité historique du PFPDT après le scandale des fiches - devrait prévaloir (cf. explications ci-dessous concernant l'art. 57 al. 2 LPD). 24

La loi ne donne pas non plus de directives concernant la forme du rapport d'activités. Le design et le tirage sont donc déterminés de manière autonome par le PFPDT. Le rapport d'activités n'est expressément pas publié dans le format interne de l'administration fédérale. L'indépendance du PFPDT s'exprime ainsi également sur le plan formel. 25

En raison de l'objectif du rapport, le rapport d'activité doit être un document accessible au public. Le PFPDT publie le rapport sous forme de e-paper gratuit sur son site web, le rapport imprimé peut être commandé pour CHF 17.00 auprès de l'Office fédéral des constructions et de la logistique. 26

Depuis 2017/2018, le rapport est également publié en italien et en anglais. Entre 1993 et 2017, le rapport n'était publié qu'en allemand et en français. L'absence de traduction italienne constituait une violation manifeste de l'art. 10 de la loi fédérale sur les langues nationales et la compréhension entre les 27

communautés linguistiques (RS 441.1). Même si cette loi fédérale n'impose pas la publication en anglais, il faut saluer le fait que le rapport d'activité soit également publié en anglais depuis quelques années. Cette nouvelle traduction facilite le conseil personnel du PFPDT, car de plus en plus de personnes anglophones demandent au PFPDT ses conseils juridiques. Un renvoi à la version anglaise du rapport d'activités contribue à rendre ces consultations en langue étrangère plus efficaces.

28 Les destinataires du rapport d'activités sont l'Assemblée fédérale en tant qu'organe d'élection du PFPDT, les conseillers fédéraux en tant que chefs des différents départements, qui effectuent tous d'innombrables traitements de données, ainsi que le grand public (journalistes, conseillers juridiques, techniciens et population civile en général). En d'autres termes, l'art. 57 al. 1 LPD s'applique à toutes les activités du PFPDT. Ces destinataires très hétérogènes constituent un défi à ne pas sous-estimer lors de la rédaction du rapport d'activités.

29 Dans ce contexte, il convient de souligner, pour être complet, que les défis en matière de protection des données qui se posent dans le secteur privé et dans le secteur public sont souvent de nature similaire. C'est pourquoi il peut être instructif de lire les rapports d'activité des commissaires cantonaux à la protection des données, qui sont tenus de publier leurs rapports d'activité en vertu du droit cantonal.

III. AL. 2 : PUBLICATION DE CONSTATATIONS ET DE DÉCISIONS D'INTÉRÊT GÉNÉRAL.

A. Constatation

30 La "constatation" n'est pas une notion juridiquement clairement définie, elle décrit de manière exhaustive le mandat d'information juridiquement contraignant du PFPDT.

31 Les faits d'intérêt général relevant de la protection des données peuvent être portés à la connaissance du PFPDT par les médias, par le biais de la hotline ou du formulaire de contact, ou encore lors d'échanges avec d'autres autorités fédérales ou cantonales. La manière dont le PFPDT souhaite réagir à une information constatée est laissée à son appréciation, notamment en ce qui concerne le moment et le canal d'information.

La notion juridiquement floue de "constatation" offre l'avantage de réagir à une (éventuelle) infraction à la LPD de manière plus flexible et plus rapide que par le biais d'une décision. De plus, cette notion floue offre la possibilité d'informer le public d'un fait pertinent en matière de protection des données même si les conditions pour l'ouverture d'une enquête selon l'article 49 LPD ne sont pas remplies. 32

L'avenir nous dira si et à quelle fréquence les constatations seront publiées à l'avenir. Comme pour toutes les notions juridiquement floues, l'interprétation de cette notion dépend du PFPDT concerné. 33

B. Décision

Le PFPDT peut désormais rendre des décisions (cf. art. 49 à 51 LPD). Dans le cadre de la consultation, certains participants issus de l'économie ont souhaité que le PFPDT ne publie pas ses décisions, mais uniquement les faits sur lesquels une enquête a été ouverte. Ces participants étaient d'avis que c'était la seule manière de garantir les droits de la personnalité des personnes concernées. Certains participants ont par contre estimé que toutes les décisions du PFPDT devaient être publiées. La règle fixée dans la loi représente donc un compromis et permet au PFPDT de mettre en balance, dans un cas particulier, d'éventuels secrets d'affaires ou de fonction avec l'intérêt général à l'élucidation d'un fait illicite. L'intérêt général devrait en principe être interprété de manière large au vu des objectifs du travail de relations publiques du PFPDT. 34

C. Intérêt général

Ni la LPD révisée, ni l'OLPD révisée, ni le message de 2017 ne définissent l'"intérêt général". Cette notion n'était pas non plus définie dans le précédent message relatif à l'ancienne LPD. Seul un exemple était alors cité par le Conseil fédéral : la publication d'une recommandation relative à un système d'information d'importance nationale était dans l'intérêt général. La doctrine mentionne d'autres exemples plus actuels : le traitement de données en question représente une situation de menace particulière pour les droits fondamentaux et les droits de la personnalité des personnes concernées, il concerne la mise en œuvre générale de la LPD, il a un caractère préjudiciel ou il fait l'objet d'un large débat public. En outre, selon Rosenthal/Jöhri, la publication d'irrégularités constatées peut être d'intérêt public (sans autre 35

précision). En raison du marché numérique actuel, la publication d'une violation de la LPD par un leader du marché devrait également être d'intérêt public. En tout état de cause, la notion doit être interprétée de manière large, même sous le régime du droit révisé. Dans le cas contraire, le PFPDT pourrait ne pas être en mesure de mener à bien son travail de relations publiques.

36 En règle générale, les informations d'intérêt général revêtent un certain caractère d'urgence et s'écartent des rapports habituels. En l'absence d'urgence, ces informations peuvent être publiées dans le rapport d'activité suivant.

37 La question de savoir quelles informations sont d'intérêt général et devraient donc être publiées dépend entre autres de la priorisation des affaires en cours sur la base des ressources en personnel disponibles. Même s'il est vrai que l'Assemblée fédérale a créé des postes supplémentaires avec l'entrée en vigueur de la nouvelle LPD, le PFPDT reste en sous-effectif chronique. Il est donc possible qu'à l'avenir également, des constatations qui seraient dans l'intérêt général soient publiées tardivement, voire pas du tout.

D. Publication

38 Le moment de la publication peut être choisi librement, comme c'était déjà le cas sous l'ancien droit. La question du moment de la publication n'a pas toujours la même importance. Mais si la publication d'une constatation est utilisée comme moyen de pression, une publication stratégique du point de vue du temps est décisive.

39 La LPD ne prévoit aucune exigence de forme pour le travail de relations publiques du PFPDT. Le canal de communication peut donc être choisi librement, même sous le nouveau droit. Par le passé, le PFPDT a publié des lettres types, des contrats types, des guides, des fiches d'information et des FAQ sur son site Internet. Il rédige également des expertises internes à l'administration. En outre, le PFPDT donne des conférences sur des thèmes d'actualité, publie des articles écrits dans des revues spécialisées et accorde des interviews dans les médias. Le service de communication gère un compte Twitter (@lePréposé) et rédige régulièrement des communiqués de presse. Plusieurs collaborateurs ont collaboré à l'élaboration d'un matériel pédagogique destiné aux jeunes. Des campagnes plus larges seraient également envisageables. Quel que soit le canal de communication choisi, le

PFPDT doit toujours suivre les principes d'une politique de communication professionnelle en vue de sensibiliser efficacement le public.

Les constatations publiées n'ont pas la portée juridique d'une décision ou d'une loi. Elles ne sont pas juridiquement contraignantes. En cas de litige, le tribunal saisi statue en toute indépendance, même si le responsable concerné s'est adressé au préalable au PFPDT dans sa fonction de conseiller ou s'est appuyé sur une constatation publiée. Le fait que la personne privée ait suivi le conseil du PFPDT peut toutefois jouer un rôle important dans l'examen de la faute dans le cadre d'actions en réparation. 40

La publication des constatations connaît toutefois aussi des limites, fixées à l'art. 36 al. 6 LPD (intérêts publics essentiels, intérêt manifestement digne de protection de la personne concernée, obligations légales de garder le secret ou prescriptions particulières en matière de protection des données). Comme toutes les autorités fédérales, le PFPDT doit respecter les dispositions légales en vigueur, notamment celles qui protègent les secrets de fabrication et d'affaires et celles qui protègent le domaine secret et le domaine privé (diffamation [art. 173 CP], calomnie [art. 174 CP], injure [art. 177 CP]) ainsi que l'interdiction de la contrainte (art. 181 CP). En outre, il est soumis au secret de fonction selon l'art. 22 LPers. Par conséquent, le PFPDT doit garantir le traitement confidentiel des données personnelles auxquelles il a accès dans l'exercice de ses tâches de surveillance. Rien n'indique que le PFPDT change sa pratique qui consiste à contacter les responsables concernés avant une publication prévue et à leur demander s'il faut éventuellement caviarder des secrets d'affaires ou de fonction avant la publication. Il ne faut toutefois pas confondre cette prise de contact avec l'obtention d'un consentement. 41

En outre, le principe de l'anonymisation des données personnelles s'applique. Pour cette raison, les données personnelles qui doivent être publiées sont en principe rendues anonymes avant la publication prévue. Les noms des cadres de l'administration qui agissent dans l'exercice de leur mandat administratif ou les noms des responsables privés ne bénéficient pas d'une protection particulière dans ce contexte. 42

Le principe de l'anonymisation connaît une exception importante. Si le PFPDT estime que la publication de la constatation ou de la décision non expurgée est dans l'intérêt public, il peut désormais renoncer lui-même à l'anonymisation (sous l'ancien droit, le PFPDT ne pouvait publier des données 43

personnelles soumises au secret de fonction qu'avec l'accord de l'autorité concernée). Cette évolution est à saluer, car elle renforce clairement l'indépendance du PFPDT. Avec la sensibilisation croissante du public aux questions de protection des données, cette révision de la loi n'est pas surprenante. En résumé, il faut donc partir du principe que le principe de l'anonymisation sera interprété de manière plutôt restrictive et que toutes les publications ne seront pas rendues anonymes par principe.

44 En ce qui concerne l'anonymisation, il convient en outre de noter qu'une anonymisation effective des données personnelles devient de plus en plus difficile au vu des progrès technologiques. En outre, l'anonymisation peut ne pas être efficace, notamment si la publication de la constatation doit être utilisée comme moyen de pression.

45 Les dispositions pénales, telles que la diffamation, la calomnie, l'injure, la contrainte ou l'abus d'autorité, sont bien entendu réservées. Le PFPDT ne bénéficie pas d'une immunité pénale et doit respecter ces dispositions pénales dans le cadre de ses activités de relations publiques.

46 Dans ce contexte, il convient de rappeler pour finir que la LPD ne s'applique qu'aux communications ou aux publications de données personnelles (cf. art. 1 LPD ou art. 36 LPD). Il est toutefois envisageable que le PFPDT, dans le cadre de son activité de surveillance, tombe sur des données matérielles au sens de l'art. 5 let. a a contrario. La communication de données matérielles n'est pas soumise à la LPD, mais ces données peuvent être protégées par le secret de fonction et leur communication peut donc être soumise aux dispositions de la LPers (p. ex. stratégies, plans ou mesures dans le domaine de la cybersécurité). Dans ces cas, les explications relatives à la communication de données personnelles (art. 36 ss LPD) s'appliquent par analogie. La LPD ne contient pas de disposition sur la levée du secret de fonction concernant les données matérielles. Il faut donc partir du principe que le PFPDT peut également se libérer lui-même du secret de fonction dans de tels cas de figure. On peut se demander si cela correspond effectivement à la volonté du législateur, surtout au vu de la situation politique tendue en Europe.

BIBLIOGRAPHIE

Baeriswyl Bruno, Datenschutzgesetzgebung in der Schweiz – Standortbestimmung und Ausblick, in: Kieser Ueli/Pärli Kurt (Hrsg.), Datenschutz im Arbeits-, Versicherungs- und Sozialbereich: Aktuelle Herausforderungen, St. Gallen 2012, S. 10 ff. (zit. Baeriswyl, Standortbestimmung).

Baeriswyl Bruno, Kommentierung zu Art. 30 aDSG, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 1. Aufl., Bern 2015 (zit. SHK-Baeriswyl, Art. 30 aDSG).

Baeriswyl Bruno, Kommentierung zu Art. 57 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023 (zit. SHK-Baeriswyl, Art. 57 DSG).

Huber René, Kommentierung zu Art. 30 aDSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. BSK-Huber, Art. 30 aDSG).

Jöhri Yvonne, §8 Aufgabe und Bedeutung der öffentlichen Datenschutzbeauftragten, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht: Beraten in Privatwirtschaft und öffentlicher Verwaltung, Handbücher für die Anwaltspraxis, Basel 2015, S. 245 ff. (zit. Jöhri).

Meier Philippe, Protection des données: fondements, principes généraux et droit privé, Berne 2011 (zit. Meier, Protection).

Meier Philippe, Le défi de Big Data dans les relations entre privés: avec quelques réflexions de lege ferenda, in: Epiney Astrid (Hrsg.), Big Data und Datenschutzrecht, Zürich 2016, S. 47 ff. (zit. Meier, Big Data).

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. Rosenthal/Jöhri).

Waldmann Bernhard/Oeschger Marcus, §15 Aufsicht, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011 (zit. Waldmann/Oeschger).

Walter Jean-Philippe, L'indépendance des autorités de protection des données, in: Epiney Astrid/Hänni Julia/Brülisauer Flavia (Hrsg.), Die Unabhängigkeit der Aufsichtsbehörden und weitere aktuelle Fragen des Datenschutzrechts/L'indépendance des autorités de surveillance et autres questions actuelles en droit de la protection des données, Zurich/Bâle/Genève 2012, S. 71 ff. (zit. Walter).

Ziebarth Wolfgang, Kommentierung zu Art. 59 DSGVO, in: Sydow Gernot (Hrsg.), Nomos Handkommentar, Europäische Datenschutzgrundverordnung, 2. Aufl., Baden-Baden 2018 (zit. NHK-Ziebarth, Art. 59 DSGVO).

MATÉRIAUX

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988 (zit. BBl 1988 II S. 413 ff.).

14. Tätigkeitsbericht des EDÖB 2006/2007 vom 31.3.2007 (zit. EDÖB, 14. Tätigkeitsbericht 2006/2007).

Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9.12.2011 (zit. BBl 2012 S. 335 ff.).

Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens vom 10.8.2017 (zit. Zusammenfassung Vernehmlassungsverfahren).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.72017 (zit. BBl 2017 S. 6941 ff.).

Rapport explicatif relatif à la Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel du 18.5.2018 (zit. Rapport explicatif Convention 108+).

28. Tätigkeitsbericht des EDÖB 2020/2021 vom 31.3.2021 (zit. EDÖB, 28. Tätigkeitsbericht 2020/2021).

29. Tätigkeitsbericht des EDÖB 2021/2022 vom 31.3.2022 (zit. EDÖB, 29. Tätigkeitsbericht 2021/2022).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 60 LPD

Un commentaire de Jonas D. Gassmann

PROPOSITION DE CITATION
Jonas D. Gassmann, Kommentierung zu Art. 60 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Gassmann, N. XXX zu Art. 60 DSG.

Chapitre 8 Dispositions pénales

Art. 60 Violation des obligations d'informer, de renseigner et de collaborer

[1] Sont, sur plainte, punies d'une amende de 250 000 francs au plus les personnes privées qui:

a. contreviennent aux obligations prévues aux art. 19, 21 et 25 à 27 en fournissant intentionnellement des renseignements inexacts ou incomplets;b.omettent intentionnellement:

d'informer la personne concernée conformément aux art. 19, al. 1, et 21, al. 1,
de lui fournir les informations prévues à l'art. 19, al. 2.

[2] Sont punies d'une amende de 250 000 francs au plus les personnes privées qui, dans le cadre d'une enquête, en violation de l'art. 49, al. 3, fournissent intentionnellement au PFPDT des renseignements inexacts ou refusent intentionnellement de collaborer.

TABLE DES MATIÈRES

En bref ... 792
I. Généralités ... 792
II. Eléments objectifs de l'infraction ... 793
A. Cercle des auteurs ... 793
B. Comportement punissable ... 794
1. Fourniture de renseignements faux ou incomplets (art. 60 al. 1 let. a) ... 794
2. Omission d'informations (art. 60 al. 1 let. b) ... 796
3. Fourniture de faux renseignements ou refus de coopérer dans le cadre d'une enquête du PFPDT (art. 60 al. 2). ... 796
III. Eléments subjectifs de l'infraction ... 797
IV. Illicéité et culpabilité ... 798
Bibliographie ... 798
Matériaux ... 799

EN BREF

La disposition de l'art. 60 sanctionne (i) la violation intentionnelle de l'obligation de renseigner, (ii) la violation intentionnelle de l'obligation d'informer et (iii) le manque de coopération intentionnel avec le PFPDT dans le cadre d'une enquête. En cas de réalisation de l'une de ces infractions, une amende de 250 000 francs au maximum est encourue.

I. GÉNÉRALITÉS

1 L'art. 60 reprend des éléments de réglementation déjà contenus dans l'art. 34 aDSG. L'art. 34 al. 2 let. a aLPD n'est pas repris, car les obligations de déclaration correspondantes ne figurent plus dans la LPD révisée. Désormais et en plus, la norme pénale s'étend également à l'obligation d'informer en cas de décision individuelle automatisée selon l'art. 21. Contrairement à l'art. 34 aDSG en relation avec l'art. En vertu de l'art. 60 en relation avec l'art. 14 aDSG, le devoir d'information ne s'applique plus seulement aux données sensibles et aux profils de la personnalité, mais désormais à toutes les données personnelles. l'art. 19, à toutes les données personnelles. Cette disposition est donc encore plus étendue. Dans l'avant-projet, un article très complet avait été créé à cet effet. Il prévoyait une sanction en cas de violation intentionnelle de l'obligation d'informer, de renseigner et de collaborer, ainsi qu'une infraction par négligence. Lors de la procédure de consultation, la punissabilité de la violation par négligence a été partiellement critiquée. En conséquence, l'article 54 P-LPD renonce à l'élément constitutif de négligence.

2 La norme pénale de l'art. 60 al. 1 est un délit poursuivi sur plainte et celle de l'art. 60 al. 2 un délit poursuivi d'office.

3 La disposition de l'art. 60 vise, d'une part, à protéger les personnes susceptibles d'être concernées d'une mise en danger de leur personnalité et, d'autre part, à protéger la fonction de surveillance du PFPDT (et donc son fonctionnement) dans le domaine privé. Il s'agit d'un délit de mise en danger abstraite ; l'infraction est consommée par la fourniture d'un renseignement faux ou incomplet, par la non-communication d'informations/données contraire aux obligations ou par le refus de coopérer avec le PFPDT. Il n'est pas nécessaire qu'il y ait eu une atteinte à la personnalité ou que la procédure d'enquête du PFPDT ait été compromise.

L'art. 60 al. 2 se distingue de la disposition de l'art. 63 par le fait que, contrairement à l'art. 63, l'art. 60 al. 2 ne requiert pas de décision au sens formel. 4

La disposition pénale est toujours conçue comme une contravention, mais le plafond de l'amende prévue à cet effet a été nettement relevé. L'art. 50 de l'AP-LPD prévoyait encore une amende pouvant aller jusqu'à 500 000 francs. Le Conseil fédéral avait justifié ce montant par "le manque de contrôle des personnes concernées sur leurs données, le manque de transparence du traitement des données et les acteurs économiques toujours plus puissants". La comparaison avec d'autres dispositions pénales du droit pénal accessoire (comme l'art. 49 LB) et l'importance d'amendes élevées pour décider si la législation suisse offre encore un "niveau de protection suffisant" par rapport à l'UE avaient également été évoquées. Cette limite supérieure des amendes prévue dans l'avant-projet a suscité des critiques lors de la consultation. Certains ont estimé que les amendes étaient trop basses, d'autres qu'elles étaient trop élevées. En outre, le fait que les sanctions ne s'adressent qu'à des personnes privées a été critiqué. En réaction, le plafond des amendes a été fixé à 250 000 francs à l'art. 54 P-LPD, ce qui correspond à 25 fois l'amende actuelle. L'amende effective est fixée en tenant compte de la situation économique de l'auteur (art. 106 al. 3 CP en relation avec l'art. 47 CP). L'art. 54 P-LPD a été repris en tant qu'art. 60 avec quelques modifications rédactionnelles. 5

II. ELÉMENTS OBJECTIFS DE L'INFRACTION

A. Cercle des auteurs

L'art. 60 est un délit spécial, car seules les personnes tenues de fournir des informations ou des renseignements (art. 60 al. 1) ou les personnes invitées par le PFPDT à fournir des renseignements ou à collaborer d'une autre manière dans le cadre d'une enquête (art. 60 al. 2) entrent en ligne de compte comme auteurs. Celui qui ne peut pas être l'auteur de l'infraction dans le cadre de l'art. 60 et qui, par conséquent, ne réagit pas à une demande de renseignements ou donne de faux renseignements, n'est pas punissable. Si les conditions sont réunies, la punissabilité en tant qu'instigateur reste possible. 6

L'orientation de la disposition pénale s'oppose au RGPD, dans lequel l'entreprise concernée est tenue pour responsable. En Suisse, la responsabilité 7

incombe aux personnes physiques qui agissent effectivement pour l'entreprise et qui sont coupables de l'infraction. Cela est justifié par le refus d'imputer la faute d'autrui dans la punissabilité des entreprises par l'article 102 du Code pénal. En outre, il n'existerait pas encore de garanties suffisantes en matière de procédure pénale dans le droit de procédure administrative, ce qui entraînerait une insécurité juridique. Pour pallier l'absence de punissabilité des entreprises, le Conseil fédéral prévoit de renforcer la responsabilité pénale des organes dirigeants en appliquant l'art. 6 DPA en plus de l'art. 29 CP.

8 Peuvent être poursuivis les dirigeants, mais aussi d'autres personnes responsables d'opérations pertinentes. Parallèlement, les personnes tenues ne sont pas seulement responsables des informations erronées qu'elles ont elles-mêmes fournies, mais aussi, par exemple, du cas où un collaborateur donne de fausses informations conformément à ses instructions.

B. Comportement punissable

9 L'art. 60 prévoit trois actes différents. Sont sanctionnées la violation de l'obligation de renseigner (art. 60 al. 1 let. a ; ci-dessous, n. 10 ss), la violation de l'obligation d'informer (art. 60 al. 1 let. b ; ci-dessous, n. 17 ss) ainsi que la coopération insuffisante avec le PFPDT dans le cadre d'une enquête (art. 60 al. 2 ; ci-dessous, n. 19 ss).

1. Fourniture de renseignements faux ou incomplets (art. 60 al. 1 let. a)

10 L'art. 60 al. 1 let. a punit le fait de fournir un renseignement faux ou incomplet et se réfère ainsi à la violation des art. 19, 21 et 25-27.

11 L'élément objectif de l'infraction est l'existence d'une obligation de fournir des informations et l'absence de motif qui supprime ou limite cette obligation (art. 19, 21 et 25-27). On peut faire une distinction entre l'obligation d'informer selon les articles 19 et 21 et l'obligation de fournir des informations selon les articles 25 à 27.

12 Dans le cadre de l'obligation de renseigner (art. 25), seul est punissable celui qui donne un renseignement faux ou incomplet, mais pas celui qui, par exemple, fait valoir un faux motif de refus selon l'art. 26. Un renseignement est faux lorsqu'il ne correspond pas à la situation réelle (par exemple lorsque d'autres données que celles qui sont effectivement traitées sont fournies à la

personne qui demande des renseignements ou lorsqu'il est affirmé contrairement à la vérité qu'aucune donnée la concernant n'est traitée). En outre, un renseignement est également faux lorsqu'il induit en erreur, c'est-à-dire qu'il donne une fausse image de la situation réelle. Un renseignement est incomplet lorsque toutes les indications mentionnées à l'article 25 ne sont pas fournies (par exemple lorsque la durée de conservation des données personnelles n'est pas communiquée alors qu'elle pourrait l'être). Un renseignement peut également être cumulativement faux et incomplet.

N'est toutefois pas punissable celui qui révèle, par des caviardages ou d'une autre manière, que le renseignement est incomplet, car il ne donne pas l'impression d'être complet. La raison en est qu'en cas de refus de divulgation, il est possible d'agir sans problème par le biais de l'article 32, le tribunal civil pouvant alors ordonner la fourniture des renseignements sous peine de sanction pénale conformément à l'article 292 du Code pénal. L'art. 60 al. 1 let. a ne s'applique pas non plus au cas où des renseignements sont certes fournis, mais en violation de l'interdiction et moyennant la facturation d'un émolument. Dans un tel cas, l'art. 146 CP (escroquerie) est toutefois parfois applicable si l'on donne la fausse impression qu'il s'agit de l'émolument normalement dû. 13

L'article 60 al. 1 let. a, ne s'applique pas non plus lorsque (par exemple parce que l'existence d'une situation obligeant à fournir des renseignements est contestée) aucun renseignement n'est fourni ou que les renseignements ne sont fournis qu'avec retard. Toutefois, en cas de refus de fournir des informations, la punissabilité selon l'art. 60 al. 1 let. b entre en ligne de compte. 14

Dans le cadre de l'obligation d'informer (art. 19 et 21), la fourniture d'informations fausses ou incomplètes est également punissable. 15

A l'art. 21, le devoir d'informer ne se réfère plus seulement, comme à l'art. 14 aDSG, à la collecte de données personnelles sensibles et de profils de la personnalité, mais désormais à la collecte de toutes les données personnelles. Le contenu de l'obligation d'informer est donc devenu plus complet et le risque de punissabilité est élargi. 16

2. Omission d'informations (art. 60 al. 1 let. b)

17 L'art. 60 al. 1 let. b couvre les cas dans lesquels une personne privée omet (i) d'informer la personne concernée que des données personnelles la concernant ont été collectées (art. 19, al. 1) ou qu'une décision individuelle automatisée a été prise (art. 21 al. 1) ou (ii) de fournir à la personne concernée les informations dont elle a besoin pour faire valoir ses droits en vertu de la LPD (art. 19 al. 2). L'élément constitutif objectif de l'art. 61 let. b serait par exemple rempli si une entreprise omettait d'indiquer dans une déclaration de protection des données conforme au droit quelles données personnelles elle traite.

18 Est également punissable celui qui donne une raison pour l'absence d'information. La punissabilité est donc plus large qu'à l'art. 60 al. 1 let. a.

3. Fourniture de faux renseignements ou refus de coopérer dans le cadre d'une enquête du PFPDT (art. 60 al. 2).

19 La norme pénale de l'art. 60 al. 2 reprend le contenu réglementaire de l'art. 34 al. 2 let. b aDSG, qui déclarait punissable la fourniture de faux renseignements ou le refus de collaborer dans le cadre d'une enquête du PFPDT. Elle se réfère à l'obligation de collaborer prévue à l'art. 49 al. 3, selon lequel les personnes privées sont tenues de fournir au PFPDT tous les renseignements et documents nécessaires à l'enquête. La variante d'infraction "fourniture de faux renseignements" est conçue comme un délit d'activité et la variante d'infraction "refus de collaborer" comme un véritable délit d'omission.

20 L'élément constitutif objectif de l'infraction présuppose une enquête formelle du PFPDT au sens de l'art. 49, ouverte en raison d'une éventuelle violation des prescriptions sur la protection des données. Un éventuel faux renseignement ou un refus de collaborer dans le cadre d'investigations menées par le PFPDT en dehors d'une enquête formelle ne sont pas couverts par l'art. 60 al. 2. Il faut en outre que (i) le PFPDT ait invité sans équivoque l'auteur de l'infraction à fournir des renseignements ou à collaborer d'une autre manière dans le cadre de l'enquête ouverte, (ii) le PFPDT ait été habilité à le faire, (iii) l'auteur de l'infraction ait fourni de faux renseignements ou refusé de collaborer et (iv) l'auteur de l'infraction n'ait pas été autorisé à fournir de faux renseignements ou à refuser de collaborer (par exemple en vertu du droit de refuser de fournir des renseignements mentionné à l'art. 49

al. 3). Les faux renseignements ne sont pas punissables si le PFPDT n'a pas demandé de renseignements.

Le tribunal pénal ne doit pas se contenter d'examiner l'acte ou l'omission de la personne accusée, mais doit également vérifier si la demande de renseignements ou de collaboration du PFPDT était licite. 21

La demande du PFPDT ne doit pas (à la différence de l'art. 63 et de l'art. 292 CP) être faite en faisant référence à la punissabilité, mais il doit être clair pour la personne invitée que sa collaboration n'est pas volontaire. Dans les cas où le PFPDT demande la collaboration d'une personne potentiellement punissable, il faut exiger qu'il attire explicitement l'attention de cette personne sur le droit de refuser de fournir des renseignements. 22

III. ELÉMENTS SUBJECTIFS DE L'INFRACTION

D'un point de vue subjectif, l'intention est requise. Le dol éventuel, c'est-à-dire le fait de considérer comme possible et de s'accommoder de la réalisation de l'infraction, est déjà suffisant. Au moment de la commission de l'infraction, l'auteur doit avoir reconnu les circonstances de fait sur la base desquelles les éléments objectifs de l'infraction doivent être considérés comme établis, et il doit avoir compris, au moins en profane, les appréciations juridiques qui s'en sont suivies (évaluation parallèle dans la sphère profane). 23

Dans la pratique, il ne devrait pas être rare que la personne qui agit soit consciente de la possibilité qu'une information soit incomplète et qu'elle s'en accommode, car elle préfère fournir une telle information plutôt que pas d'information du tout. Si une déclaration d'exhaustivité est remise à la personne concernée, l'intention est généralement présumée si l'information n'est pas complète. La personne tenue de fournir des informations agit par négligence et n'est donc pas punissable si elle a cru que les données fournies et non vérifiées étaient complètes. La délimitation par rapport à l'existence d'un dol éventuel doit être effectuée au cas par cas sur la base d'indices. 24

Si l'auteur se trompe sur les faits pertinents pour les éléments constitutifs de l'infraction, il y a erreur sur les faits au sens de l'art. 13 CP. Dans ce cas, le tribunal juge l'infraction en fonction de l'idée que l'auteur se fait des faits. Cela est particulièrement pertinent lorsque ce dernier fournit un renseignement incomplet parce qu'il pense que celui-ci a été fourni de manière complète. Une erreur sur les faits peut également exister concernant 25

des éléments normatifs de l'infraction, comme la question de savoir s'il existe une obligation de renseignement, d'information ou de communication. L'opinion d'une tierce personne moyenne est alors déterminante.

IV. ILLICÉITÉ ET CULPABILITÉ

26 En ce qui concerne l'illicéité, les règles générales du CP s'appliquent conformément à l'art. 333 al. 1 CP. Un comportement conforme à l'infraction peut être exceptionnellement autorisé en raison de motifs justificatifs légaux ou supra-légaux.

27 Les règles générales s'appliquent également en ce qui concerne la culpabilité, conformément à l'art. 333 al. 1 CP. En vertu de l'art. 21 CP, la punissabilité peut être empêchée par une erreur sur l'interdiction. Cela ne se produit toutefois que si la personne entrant en ligne de compte comme auteur ne pouvait pas savoir qu'elle agissait de manière illicite. Dans ce cas, elle pense ne pas avoir commis d'acte illicite. Si l'erreur de droit avait pu être évitée, la peine ne sera que réduite.

BIBLIOGRAPHIE

Niggli Marcel Alexander/Maeder Stefan, Kommentierung zu Art. 34 aDSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Basler Kommentar, Datenschutzgesetz / Öffentlichkeitsgesetz, 3. Aufl., Basel 2014.

Niggli Marcel Alexander/Maeder Stefan, Kommentierung zu Art. 21 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafrecht (StGB/JStGB), 4. Aufl., Basel 2018.

Rosenthal David, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, https://jusletter.weblaw.ch/juslissues/2020/1045/das-neue-datenschutz_0e89d89706.html, besucht am 8.8.2023.

Rosenthal David/Gubler Seraina, Die Strafbestimmungen des neuen DSG, SZW 1/2021, S. 52 ff.; Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Wohlers Wolfgang, Kommentierung zu Art. 66 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski, Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 S. 6941 ff. (zit. Botschaft 2017), abrufbar unter https://www.admin.ch/opc/de/federal-gazette/2017/6941.pdf, besucht am 8.8.2023.

Erläuternder Bericht des Bundesamts für Justiz BJ zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016, abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf.download.pdf/vn-ber-d.pdf (zit. Erläuternder Bericht VE-DSG), besucht am 8.8.2023.

Zusammenfassung des Bundesamts für Justiz BJ der Ergebnisse des Vernehmlassungsverfahrens vom 10.8.2017 betreffend Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016 (zit. Zusammenfassung Vernehmlassung VE-DSG), abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/ve-ber-d.pdf.download.pdf/ve-ber-d.pdf, besucht am 8.8.2023

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 61 LPD

Un commentaire de Jonas D. Gassmann

PROPOSITION DE CITATION

Jonas D. Gassmann, Kommentierung zu Art. 61 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Gassmann, N. XXX zu Art. 61 DSG.

Art. 61 Violation des devoirs de diligence

Sont, sur plainte, punies d'une amende de 250 000 francs au plus les personnes privées qui, intentionnellement:

a. communiquent des données personnelles à l'étranger en violation de l'art. 16, al. 1 et 2, et sans que les conditions de l'art. 17 soient remplies;

b. confient le traitement de données personnelles à un sous-traitant sans que les conditions de l'art. 9, al. 1 et 2, soient remplies;

c. ne respectent pas les exigences minimales en matière de sécurité des données édictées par le Conseil fédéral selon l'art. 8, al. 3.

TABLE DES MATIÈRES

En bref ... 803
I. Généralités ... 803
II. Faits objectifs ... 804
A. Violation des prescriptions lors de l'exportation de données (art. 61 let. a) ... 804
1. généralités ... 804
2. Pas de responsabilité pénale de l'importateur ... 806
B. Violation des prescriptions lors de la remise du traitement des données à un sous-traitant (art. 61 let. b) ... 806
1. généralités ... 806
2. Pas de punissabilité du sous-traitant (ou des personnes agissant pour son compte) ... 807
C. Violation des exigences minimales en matière de sécurité des données (art. 61 let. c) ... 807
1. Généralités ... 807
2. Violation des principes de l'art. 1 OLPD ... 807
3. Violation des objectifs de l'article 2 du RGPD ... 808
4. Violation de la disposition relative aux mesures techniques et organisationnelles (art. 3 OLPD) ... 809
5. Omission de la journalisation selon l'art. 4 OLPD ... 809
6. Omission de l'établissement d'un règlement de traitement conformément à l'article 5 f. DSV ... 810
7. Prise en compte des coûts lors de la détermination de la sécurité adéquate des données et des mesures appropriées ... 810
III. Eléments subjectifs de l'infraction ... 811
IV. Illégalité et culpabilité ... 812
Bibliographie ... 812
Matériaux ... 812

EN BREF

La disposition de l'article 61 sanctionne (i) la violation intentionnelle des prescriptions lors de l'exportation de données, (ii) la violation intentionnelle des prescriptions lors du transfert du traitement des données à un sous-traitant et (iii) le non-respect intentionnel des exigences minimales en matière de sécurité des données. En cas de réalisation de l'une de ces infractions, une amende de 250 000 francs au maximum est encourue. En ce qui concerne la variante de l'infraction consistant à ne pas respecter intentionnellement les exigences minimales en matière de sécurité des données (art. 61 let. c), il existe des doutes fondés quant à sa justiciabilité.

I. GÉNÉRALITÉS

La disposition de l'art. 61 est nouvelle. Le Conseil fédéral a justifié l'introduction de cette disposition dans le message par le fait que la loi sur la protection des données totalement révisée prévoit de "nouvelles obligations élémentaires" qui "ne sont pas couvertes par les dispositions pénales en vigueur". Il s'agit d'un délit de mise en danger abstraite ; le délit est consommé dès la réalisation de l'acte, la punissabilité ne présuppose donc pas la prise de connaissance des données personnelles concernées par des tiers non autorisés. 1

La norme pénale de l'art. 61 est un délit poursuivi sur plainte. 2

Le but de l'art. 61 est de donner du poids aux obligations des responsables du traitement et des sous-traitants ancrées dans la loi (art. 16 al. 1 et 2 en relation avec l'art. 17 ; art. 9 al. 1 et 2 ; art. 8 al. 3) en rendant leur violation punissable. Selon le message, la sanction pénale doit en fin de compte contribuer à ce que la personnalité des personnes concernées soit protégée efficacement. L'art. 61 let. a doit également être lu en relation avec l'objectif de la révision de la LPD, tel que le Conseil fédéral l'avait mentionné dans son rapport sur l'évaluation de la LPD du 9 décembre 2011 : la révision devait s'adresser à l'augmentation des traitements de données, à la dimension de plus en plus internationale des traitements de données et à la difficulté croissante de pouvoir continuer à contrôler des données une fois qu'elles ont été communiquées. 3

4 L'infraction visée à l'article 61 est un délit spécial : l'auteur de l'infraction ne peut être que celui qui est chargé d'assurer le respect des obligations visées à l'article 61, à savoir, dans le cas des personnes morales visées à l'article 29 du code pénal, leurs dirigeants. De par sa nature, la disposition de l'art. 61 s'adresse donc en premier lieu aux personnes habilitées à donner des instructions, puisque ce sont elles qui doivent garantir le respect des obligations en question. Celui qui n'empêche pas les infractions commises par des collaborateurs subordonnés ou qui n'en supprime pas les effets entre également en ligne de compte comme auteur (art. 6 al. 2 et 3 DPA en relation avec l'art. 64 al. 1 LPD).

5 En ce qui concerne l'infraction visée à l'art. 61 let. c, elle a été critiquée à plusieurs reprises au cours de la procédure législative comme étant trop vague. La demande de suppression n'a toutefois pas été acceptée en fin de compte. Meyle/Morand/Vasella remettent à juste titre en question la justiciabilité des "exigences minimales en matière de sécurité des données" régies par le RGPD (cf. ci-dessous, n. 17 ss).

II. FAITS OBJECTIFS

6 L'art. 61 LPD mentionne trois faits dont la réalisation est considérée comme une violation du devoir de diligence. Une infraction commise par des personnes privées est passible d'une amende pouvant atteindre 250 000 francs. En particulier, la violation des trois éléments constitutifs suivants est poursuivie pénalement sur plainte : La violation des prescriptions lors de l'exportation de données (art. 61 let. a, n. 7 ss ci-dessous), la violation des prescriptions lors du transfert du traitement des données à un sous-traitant (art. 61 let. b, n. 12 ss ci-dessous) et le non-respect des exigences minimales en matière de sécurité des données (art. 61 let. c, n. 15 ss ci-dessous).

A. Violation des prescriptions lors de l'exportation de données (art. 61 let. a)

1. généralités

7 Sous l'ancien droit, celui qui ne respectait pas les prescriptions légales dans le cadre d'une communication de données à des Etats ne disposant pas d'une protection légale adéquate des données n'était pas punissable. En vertu de

l'art. 34, al. 2, let. aDSG, n'était punissable que celui qui, tout en se souciant d'une protection sous forme de contrat, omettait intentionnellement de déclarer ce contrat au PFPDT conformément à l'art. 6, al. 3, aDSG ou donnait intentionnellement de fausses indications.

Selon l'art. 61 let. a, est désormais punissable celui qui exporte intentionnellement des données vers un Etat ne disposant pas d'une protection des données adéquate et qui ne peut ni présenter une garantie suffisante de protection des données ni s'appuyer sur une exception selon l'art. 17. Si le Conseil fédéral n'a pas pris de "décision d'adéquation" sur la base de l'art. 16 al. 1, les données personnelles ne peuvent être communiquées à l'État concerné qu'aux conditions mentionnées à l'art. 16 al. 2, la conclusion de clauses contractuelles standard ("clauses standard de protection des données", let. d) étant la plus pertinente en pratique. 8

Dans le domaine d'application du DSGVO, la Commission européenne a abrogé les anciennes clauses contractuelles standard avec effet au 27 septembre 2021 par la décision d'exécution (UE) 2021/914 du 4 juin 2021 et les a remplacées par de nouvelles clauses contractuelles standard. Le 27 août 2021, le PFPDT a reconnu ces nouvelles clauses contractuelles standard, sous réserve qu'elles soient adaptées et/ou complétées si nécessaire dans des cas d'application concrets. Quiconque communique des données dans un Etat qui ne dispose pas d'une protection légale adéquate des données ne peut toutefois pas se contenter de conclure des clauses contractuelles standard reconnues. Au contraire, le libellé de l'art. 16 al. 2 let. d exige que ces clauses contractuelles standard garantissent effectivement une protection des données "appropriée". Les nouvelles clauses contractuelles types prévoient que les parties (i) s'assurent en outre qu'elles peuvent respecter les clauses contractuelles types indépendamment du droit national de l'importateur et (ii) documentent leur évaluation à cet égard. Il faut donc procéder à une évaluation de l'impact du transfert (TIA) et les données ne peuvent être transférées que si cette TIA est satisfaisante. 9

L'article 10 al. 1 du RGPD précise ou relativise le fait que l'exportateur de données doit prendre des "mesures appropriées" en cas de communication de données au moyen de clauses contractuelles types afin de s'assurer que l'importateur de données respecte les clauses en question. Il s'ensuit que (dans l'esprit de l'approche fondée sur les risques) il est permis d'accepter un risque résiduel que le droit local de l'importateur fasse échec au respect des clauses 10

contractuelles types par l'importateur, tant que des mesures ont été prises pour réduire ce risque de manière appropriée. Voir à ce sujet le commentaire sur les articles 16 et 17.

2. Pas de responsabilité pénale de l'importateur

11 Celui qui (en tant qu'exportateur) communique des données personnelles à l'étranger en sachant que le destinataire (importateur) des données n'assure pas une protection des données appropriée malgré le contrat, s'expose au risque de punissabilité selon l'art. 61 let. a. En revanche, l'importateur qui reçoit des données personnelles ou qui les utilise en violation du contrat ou de la protection des données n'est pas soumis à un risque de punissabilité - seule la communication de données personnelles est constitutive d'une infraction au sens de l'art. 61 let. a.

B. Violation des prescriptions lors de la remise du traitement des données à un sous-traitant (art. 61 let. b)

1. généralités

12 Selon l'art. 61 let. b, est punissable quiconque remet intentionnellement le traitement de données à un sous-traitant sans que les conditions de l'art. 9 al. 1 et 2 soient remplies. Selon l'art. 9 al. 1, le traitement de données personnelles peut être confié par contrat ou par la loi à un sous-traitant si (a) les données sont traitées comme le responsable du traitement serait en droit de le faire lui-même et si (b) aucune obligation légale ou contractuelle de garder le secret n'interdit la délégation. Selon l'article 9 al. 2, le responsable du traitement doit notamment s'assurer "que le sous-traitant est en mesure d'assurer la sécurité des données". L'état de fait objectif de l'art. 61 let. b serait par exemple rempli si une entreprise, en tant que responsable, faisait appel à un sous-traitant (p. ex. un fournisseur de services cloud) sans avoir conclu avec lui un contrat de traitement des données de commande juridiquement suffisant.

13 L'art. 7 RGPD précise ces conditions du traitement sur commande : le responsable doit autoriser au préalable le recours à des sous-traitants de manière générale ou concrète (art. 7 al. 1 RGPD). En cas d'autorisation générale, le responsable doit être informé de tout changement envisagé concernant le recours à d'autres tiers ou leur remplacement, le responsable

pouvant s'y opposer (art. 7 al. 2 RGPD). Voir sur l'ensemble le commentaire relatif à l'article 9.

2. Pas de punissabilité du sous-traitant (ou des personnes agissant pour son compte).

La violation de l'art. 9 al. 3, c'est-à-dire l'obligation pour le sous-traitant de faire approuver au préalable par le responsable du traitement de nouveaux sous-traitants, n'est pas punissable. Même en cas de violation de l'art. 9 al. 1 ou 2, le texte de l'art. 61 let. b exclut toute punissabilité du sous-traitant (ou des personnes agissant en son nom) : seul le responsable (ou les personnes agissant en son nom) peut être sanctionné. Il en va de même lorsque le responsable du traitement confie à son tour le traitement des données à un sous-traitant : les normes pénales doivent être interprétées de manière restrictive. 14

C. Violation des exigences minimales en matière de sécurité des données (art. 61 let. c)

1. Généralités

Selon l'art. 61 let. c, est punissable celui qui, intentionnellement, ne respecte pas les exigences minimales en matière de sécurité des données édictées par le Conseil fédéral en vertu de l'art. 8 al. 3. Il est fait référence ici à la première section ("Sécurité des données", art. 1 ss) du premier chapitre de l'OLPD. 15

La disposition de l'art. 61 let. c est un délit de mise en danger abstraite conçu comme une norme en blanc (cf. déjà ci-dessus, n. 1) ; il n'est pas nécessaire qu'il y ait eu une "violation de données". Inversement, chaque "data breach" n'entraîne pas non plus une punissabilité - s'il y a bien eu "data breach", mais que les "exigences minimales en matière de sécurité des données" ont été respectées, il n'y a pas de punissabilité. 16

2. Violation des principes de l'art. 1 OLPD

La disposition de l'art. 1 RGPD contient des principes que le responsable du traitement et le sous-traitant doivent respecter lorsqu'ils déterminent le niveau de protection adéquat et les mesures appropriées à cet effet. Il s'agit de lignes directrices générales et non d'exigences (minimales) concrètes en 17

matière de sécurité des données. Selon l'avis exact de Meyle/Morand/Vasella, cette disposition très générale concernant la procédure du responsable lors de la détermination des mesures de sécurité n'est pas justiciable - on ne voit pas quelles "exigences minimales" en matière de sécurité des données au sens de l'art. 8 al. 3 devraient découler de l'art. 1 OLPD.

18 Si le responsable ne respecte pas les principes de l'art. 1 OLPD, par exemple s'il ne détermine pas le besoin de protection des données personnelles selon les critères prévus à l'al. 1, s'il ne tient pas compte de critères pertinents lors de l'évaluation des risques comme prévu à l'al. 2 ou s'il ne vérifie pas ses mesures "pendant toute la durée du traitement" comme prévu à l'al. 5, cela n'indique pas encore une violation des "exigences minimales" en matière de sécurité des données : d'une part, l'art. 1 RGPD ne définit justement pas de telles exigences, mais contient uniquement des lignes directrices sur la manière de les atteindre, et d'autre part, un responsable peut également mettre en œuvre des mesures efficaces pour garantir une sécurité adéquate des données sans procéder strictement selon l'art. 1 RGPD.

3. Violation des objectifs de l'article 2 du RGPD

19 La disposition de l'art. 2 RGPD définit des objectifs de protection de la sécurité des données que le responsable du traitement et le sous-traitant doivent atteindre au moyen de mesures techniques et organisationnelles : Confidentialité (let. a), Disponibilité (let. b), Intégrité (let. c) et Traçabilité (let. d).

20 Ces objectifs de protection sont identiques à ceux de l'art. 6 al. 2 de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (loi sur la sécurité de l'information). A l'instar des principes énoncés à l'art. 1 OLPD, les objectifs visés à l'art. 2 OLPD sont formulés de manière très générale (ce qui ressort déjà du seul titre "Objectifs") et il n'est pas possible d'en déduire des "exigences minimales" en matière de sécurité des données au sens de l'art. 8 al. 3. Il n'en ressort pas quelles mesures techniques et organisationnelles concrètes devraient être mises en œuvre. Meyle/Morand/Vasella remettent à juste titre en question la justiciabilité de cette disposition.

4. Violation de la disposition relative aux mesures techniques et organisationnelles (art. 3 OLPD)

La disposition de l'article 3 OLPD contient des prescriptions relatives aux mesures techniques et organisationnelles et concrétise ainsi la sécurité des données. Elle ne contient toutefois pas (non plus) d'"exigences minimales" en matière de sécurité des données au sens de l'article 8 al. 3 ; l'art. 3 OLPD ne fait que concrétiser les objectifs de protection contenus dans l'article 2 OLPD. 21

En cas d'interprétation large, l'art. On pourrait y lire des "exigences minimales" dans la mesure où, selon cette disposition, les objectifs de protection au sens de l'article 2 du RGPD "doivent être garantis". Une telle interprétation signifierait toutefois que toute violation d'un objectif de protection serait la preuve de l'absence d'une mesure appropriée. Cela serait à son tour incompatible avec l'approche basée sur les risques reconnue dans le domaine de la sécurité des données. Le terme "garantir" doit donc être interprété comme "s'efforcer de". 22

L'article 3 du RGPD doit être lu conjointement avec les articles 1 et 2 du RGPD comme une concrétisation de la notion de sécurité des données, sans qu'il soit possible d'en déduire des "exigences minimales" en matière de sécurité des données. En outre, le responsable du traitement et le sous-traitant ne doivent pas nécessairement tenir compte de tous les objectifs de protection visés à l'article 3 du RGPD pour leurs mesures techniques et organisationnelles. La justiciabilité de cette disposition est également remise en question à juste titre par Meyle/Morand/Vasella. 23

5. Omission de la journalisation selon l'art. 4 OLPD

La disposition de l'art. 4 OLPD reprend l'actuel art. 10 OLPD. La journalisation doit permettre de garantir la finalité. 24

En règle générale, la journalisation ne constitue pas une "exigence minimale en matière de sécurité des données", comme le mentionne l'art. 61 let. c (même si l'art. 4 OLPD est mentionné dans la première section "Sécurité des données" de l'OLPD) et l'omission de la journalisation ne peut donc pas non plus être punissable. Une punissabilité serait exceptionnellement envisageable si une autorité de poursuite pénale pouvait prouver dans un cas particulier que la journalisation, en tant que mesure de traçabilité, devait indirectement 25

servir à la sécurité des données et que la personne accusée en était consciente, du moins dans les grandes lignes.

6. Omission de l'établissement d'un règlement de traitement conformément à l'article 5 f. DSV

26 Les dispositions de l'art. 5 f. OLPD reprennent les anciens art. 11 OLPD et art. 21 OLPD. Dans le rapport explicatif OLPD, le Conseil fédéral constate lui-même que l'établissement d'un règlement de traitement porte sur l'obligation de rendre compte - et donc pas sur la sécurité des données. Le fait que l'obligation d'établir un tel règlement n'existe qu'en cas de risque accru n'y change rien.

27 Une "exigence minimale en matière de sécurité des données", telle que mentionnée à l'art. 61 let. c, est l'établissement d'un "règlement de traitement" (même si l'art. 5 f. DSV sont mentionnés dans la première section "Sécurité des données" du DSV) n'en font pas partie et l'omission de cet établissement ne peut pas non plus être punissable dans cette mesure.

7. Prise en compte des coûts lors de la détermination de la sécurité adéquate des données et des mesures appropriées

28 Selon l'art. 1 al. 1 RGPD, pour garantir une sécurité adéquate des données, le responsable du traitement et le sous-traitant doivent déterminer le besoin de protection des données personnelles et définir "les mesures techniques et organisationnelles appropriées au regard du risque". L'art. 1 al. 2 OLPD décrit les critères d'évaluation du besoin de protection des données personnelles et l'art. 1 al. 3 OLPD décrit les critères d'évaluation du risque pour la personnalité ou les droits fondamentaux de la personne concernée. Plus le besoin de protection des données personnelles est élevé et/ou plus le risque mentionné est important, plus les exigences relatives aux mesures sont strictes. Selon l'art. 1 al. 4 OLPD, les "coûts de mise en œuvre" doivent également être pris en compte lors de la définition des mesures techniques et organisationnelles.

29 Selon le Conseil fédéral, les coûts de mise en œuvre doivent être compris au sens large et englober non seulement les ressources financières nécessaires, mais aussi les ressources en personnel et en temps. Les coûts doivent déjà être pris en compte lorsqu'il s'agit de déterminer quelles mesures sont

"appropriées" ou non. Meyle/Morand/Vasella font remarquer à juste titre que l'avis défendu par le Conseil fédéral, selon lequel les responsables du traitement et les sous-traitants "ne peuvent pas se dispenser de l'obligation d'assurer une sécurité appropriée des données au motif que cela entraîne des coûts excessifs", viderait de son sens la disposition de l'art. 1 al. 4 OLPD : "seule" une sécurité "appropriée" est exigée et les coûts doivent être pris en compte comme critère dans la détermination du caractère approprié.

Les "exigences minimales en matière de sécurité des données" ne sont donc pas violées (et il n'est pas punissable) si le responsable du traitement ou le sous-traitant tient compte, entre autres, des coûts lors de la détermination du caractère adéquat de la sécurité des données et des mesures appropriées. 30

III. ELÉMENTS SUBJECTIFS DE L'INFRACTION

D'un point de vue subjectif, l'infraction de l'article 61 requiert l'intention, le dol éventuel étant suffisant. L'auteur agit par dol éventuel notamment lorsqu'il ne sait pas avec certitude que son comportement enfreint les prescriptions relatives à l'exportation des données (art. 16, al. 1 et 2 ; art. 17) ou à la remise du traitement des données à un sous-traitant (art. 9, al. 1 et 2) ou qu'il ne respecte pas les exigences minimales en matière de sécurité des données (art. 8 al. 3 en relation avec les art. 1 ss OLPD), mais qu'il s'en accommode ou accepte de commettre éventuellement une infraction. 31

Il y a dol éventuel dans le cas de l'infraction visée à l'art. 61 let. b lorsque l'auteur, en confiant le traitement des données à un sous-traitant, accepte au moins que le sous-traitant (i) traite les données de manière contraire à la loi ou (ii) ne garantisse pas la sécurité des données. Les circonstances dans lesquelles le sous-traitant en question a été "examiné" et finalement choisi sont déterminantes pour répondre à la question de savoir si l'on est en présence d'une telle acceptation. Les dispositions de l'art. 9 sont formulées de manière très ouverte et floue (notamment en comparaison avec la réglementation parallèle de l'art. 28 RGPD), ce qui devrait rendre difficile dans la pratique pour les autorités pénales de prouver un comportement punissable dans un cas particulier (sans compter qu'il existe de toute façon des doutes fondés quant à la justiciabilité de la variante de l'infraction consistant à ne pas respecter intentionnellement les exigences minimales en matière de sécurité des données, voir ci-dessus N. 17 ss). En revanche, on pourrait admettre un simple acte de négligence (non punissable) si l'auteur, 32

sur la base d'un conseil juridique externe (qui ne devait faire aucun doute), partait du principe qu'un contrat de traitement des données de commande donné était juridiquement suffisant, mais que celui-ci s'avérait insuffisant.

IV. ILLÉGALITÉ ET CULPABILITÉ

Cf. OK-Gassmann sur l'art. 60, n. 26 s.

BIBLIOGRAPHIE

EDÖB, Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge vom 27. August 2021, https://www.edoeb.admin.ch/dam/edoeb/de/Dokumente/datenschutz/Paper%20SCC_DE.pdf.download.pdf/Paper%20SCC_DE.pdf, besucht am 8.8.2023.

Meyle Hannes/Morand Anne-Sophie/Vasella David, DSV: keine Mindestanforderungen an die Datensicherheit, keine entsprechende Strafbarkeit, weitere Anmerkungen, https://datenrecht.ch/dsv-keine-mindestanforderungen-an-die-datensicherheit-keine-entsprechende-strafbarkeit-weitere-anmerkungen/, besucht am 8.8.2023.

Popp Peter/Berkemeier Anne, Kommentierung zu Art. 1 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafrecht (StGB/JStGB), 4. Aufl., Basel 2018.

Rosenthal David, Neue EU Standardvertragsklauseln für Datentransfers in unsichere Drittländer, https://www.rosenthal.ch/downloads/VISCHER-faq-scc.pdf, besucht am 8.8.2023.

Rosenthal David/Gubler Seraina, Die Strafbestimmungen des neuen DSG, SZW 1/2021, S. 52 ff.; Wohlers Wolfgang, Kommentierung zu Art. 61 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski, Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom

15.9.2017, BBl 2017 S. 6941 ff. (zit. Botschaft 2017), abrufbar unter https://www.admin.ch/opc/de/federal-gazette/2017/6941.pdf, besucht am 8.8.2023.

Erläuternder Bericht des Bundesamts für Justiz BJ zur Verordnung über den Datenschutz vom 31.8.2022, abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vdsg/erlaeuterungen-vo.pdf.download.pdf/erlaeuterungen-vo-d.pdf (zit. Erläuternder Bericht DSV), besucht am 8.8.2023.

Kommentar des Bundesamts für Justiz BJ zur Vollzugsverordnung zum Bundesgesetz über den Datenschutz vom 1.1.2008 (zit. Kommentar BJ zur VDSG), abrufbar unter https://www.edoeb.admin.ch/dam/edoeb/de/Dokumente/deredoeb/kommentar_des_bundesamtsfuerjustizzurvollzugsverordnungvom14juni.pdf.download.pdf/kommentar_des_bundesamtsfuerjustizzurvollzugsverordnungvom14juni.pdf, besucht am 8.8.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 62 LPD

Un commentaire de Jonas D. Gassmann

PROPOSITION DE CITATION

Jonas D. Gassmann, Kommentierung zu Art. 62 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Gassmann, N. XXX zu Art. 62 DSG.

Art. 62 Violation du devoir de discrétion

[1] Est, sur plainte, puni d'une amende de 250 000 francs au plus quiconque révèle intentionnellement des données personnelles secrètes portées à sa connaissance dans l'exercice d'une profession qui requiert la connaissance de telles données.

[2] Est passible de la même peine quiconque révèle intentionnellement des données personnelles secrètes portées à sa connaissance dans le cadre des activités qu'il exerce pour le compte d'une personne soumise à l'obligation de garder le secret ou lors de sa formation chez elle.

[3] La révélation de données personnelles secrètes demeure punissable alors même que l'exercice de la profession ou la formation ont pris fin.

TABLE DES MATIÈRES

En bref 817
I. Généralités 817
II. Violation du secret professionnel 818
A. Cercle des auteurs 818
B. Eléments objectifs de l'infraction 819
C. Eléments subjectifs de l'infraction 821
III. Illégalité et culpabilité 822
IV. Délimitation et concurrence 822
Bibliographie 822
Matériaux 823

EN BREF

La disposition de l'article 62 a pour objet ce que l'on appelle le "petit secret professionnel". Elle punit la révélation intentionnelle de données personnelles secrètes apprises dans l'exercice de la profession. Par rapport à l'ancien droit, les éléments constitutifs de l'infraction de "violation du secret professionnel" sont considérablement élargis. En cas de réalisation de cette infraction, une amende de 250 000 francs au maximum est encourue.

I. GÉNÉRALITÉS

La disposition de l'art. 62 se fonde sur l'art. 35 aDSG, mais élargit considérablement les éléments constitutifs de la "violation du devoir de discrétion professionnelle". Il ne s'agit plus seulement de la révélation de "données personnelles secrètes et sensibles ou de profils de la personnalité", mais plus généralement de "données personnelles secrètes". Le Conseil fédéral a justifié cette extension de la protection du secret à tous les types de données personnelles par le développement des technologies de l'information et de la communication et l'extension massive de la collecte de données qui en découle. L'art. 62 vise à protéger la sphère secrète des personnes qui confient leurs données personnelles à des tiers. 1

La norme pénale de l'art. 62 est un délit poursuivi sur plainte. 2

Selon le Conseil fédéral, l'art. 62 vise à combler les lacunes "qui résultent du cercle restreint des auteurs des art. 320 et 321 CP (délits spéciaux)". L'obligation de garder le secret doit également s'appliquer aux personnes qui ne tombent pas sous le coup de l'art. 320 ou 321 CP. Le législateur a préféré cette solution à une extension des dispositions de droit pénal (général), car il n'a pas jugé opportun d'étendre également le droit de refuser de témoigner, que les lois de procédure prévoient généralement pour les professions mentionnées à l'art. 321 CP. D'un point de vue terminologique, le "petit secret professionnel" s'inspire toutefois du "grand" secret professionnel de l'art. 321 CP (qui s'applique notamment aux médecins, aux avocats, aux ecclésiastiques, etc.) et du secret bancaire de l'art. 47 LB. 3

4 Lors de l'élaboration du projet, le Conseil fédéral avait déjà renoncé à mentionner la communication de données traitées à des fins commerciales. Cette position a été maintenue par les chambres parlementaires.

5 L'avant-projet prévoyait encore une peine privative de liberté de trois ans au plus ou une peine pécuniaire en cas de violation du devoir de discrétion professionnelle (art. 52 AP-LPD). Selon le rapport explicatif AP-LPD, ce durcissement était prévu parce qu'une amende ne correspondrait plus à la gravité des atteintes possibles, notamment au regard de l'art. 321 CP. Lors de la consultation, plusieurs participants ont toutefois estimé que la sanction pénale était trop élevée, raison pour laquelle une amende de 250 000 francs a été introduite. Le montant maximal de l'amende de 250 000 francs a finalement été maintenu, car la majorité a estimé que ce montant était proportionné et suffisamment dissuasif.

6 Dans l'ensemble, il est étonnant que la disposition de l'article 62, inhabituellement sévère au vu de son large champ d'application et du cadre des amendes, notamment en comparaison internationale, n'ait guère été discutée (sur le fond) lors des débats parlementaires.

II. VIOLATION DU SECRET PROFESSIONNEL

A. Cercle des auteurs

7 L'art. 62 LPD n'englobe pas toutes les personnes qui révèlent les données personnelles secrètes d'autrui. Selon le texte, sont concernées les personnes qui exercent une profession nécessitant la connaissance de données personnelles secrètes. L'art. 62 LPD est donc conçu comme un délit spécial. Contrairement à l'art. 321 CP, il n'est pas nécessaire d'appartenir à une profession particulière. Depuis l'introduction de l'art. 62, les employés n'ont donc plus besoin de posséder une qualité particulière comme celle d'avocat, de médecin, d'employé de banque ou de fonctionnaire pour être soumis à une obligation de garder le secret (qui va au-delà des secrets d'affaires et de fabrication au sens de l'art. 321a al. 4 CO) : il suffit qu'ils aient pris connaissance de "données personnelles secrètes" dans l'exercice de leur profession. En vertu de l'art. 2 al. 1, les membres des autorités fédérales sont également concernés par la disposition pénale de l'art. 62.

Selon l'art. 62 al. 3, ce n'est pas seulement l'exercice actuel de la profession qui est visé, la protection du secret se poursuit également lorsque les personnes tenues d'exercer la profession ont abandonné celle-ci ou ont terminé leur formation correspondante. Cela correspond à la réglementation de l'art. 35 al. 3 aDSG. On peut supposer que cela signifie (par analogie avec l'art. 321 CP) que l'obligation de garder le secret professionnel subsiste jusqu'au décès du détenteur du secret, indépendamment de la poursuite de la relation d'affaires. 8

Selon l'art. 62 al. 2, les auxiliaires (collaborateurs ; personnes traitant des données sur mandat) et les personnes en formation (y compris les stagiaires) sont également soumis à la punissabilité. Cette extension correspond à la réglementation de l'art. 35 al. 2 aDSG. Les tiers qui agissent à la place du détenteur primaire du secret sont, selon la conception défendue ici, soumis à l'obligation de garder le secret en tant qu'auxiliaires. 9

N'est pas punissable selon l'art. 62 celui qui révèle des données personnelles secrètes que le détenteur du secret ou un auxiliaire lui a révélées en violation de l'art. 62. 10

L'art. 62 LPD ne prévoit pas de punissabilité directe de l'entreprise. Pour y remédier, la responsabilité pénale des organes dirigeants a été renforcée par l'application de l'art. 6 DPA en plus de l'art. 29 CP. 11

B. Eléments objectifs de l'infraction

Selon l'art. 62 al. 1, est punissable "[celui qui] révèle intentionnellement des données personnelles secrètes dont il a eu connaissance dans l'exercice de sa profession, qui requiert la connaissance de telles données". L'élément objectif de l'infraction exige tout d'abord qu'il s'agisse de données personnelles "secrètes". Les données personnelles sont toutes les informations qui se rapportent à une personne physique identifiée ou identifiable (art. 5 let. a). L'art. 62 ne définit pas lui-même quelles données personnelles sont considérées comme "secrètes", mais le message renvoie à la notion matérielle de secret du droit pénal. Il y a secret protégé par le droit pénal lorsque (i) le fait n'est pas généralement connu ou accessible, (ii) le détenteur du secret a un intérêt digne de protection à ce qu'il soit connu de manière limitée et (iii) il a également la volonté de le faire. 12

13 En outre, l'auteur doit avoir pris connaissance des données personnelles dans l'exercice de sa profession. Sont concernées, d'une part, les données que le client/maître du secret a confiées au détenteur du secret et, d'autre part, celles que le détenteur du secret a lui-même recueillies dans l'exercice de sa profession.

14 La notion de "révélation" de données personnelles secrètes correspond à celle des articles 320 et 321 du Code pénal : Il y a révélation lorsque le détenteur du secret porte des données personnelles secrètes à la connaissance d'un tiers qui n'y est pas autorisé ou permet à ce tiers d'en prendre connaissance, peu importe la manière dont cela se passe (p. ex. transmission directe de données personnelles secrètes ou conservation insuffisante des dossiers de manière à permettre au tiers d'en prendre connaissance). Si les données ont été effectivement anonymisées, pseudonymisées ou cryptées avant d'être transmises, de sorte que le tiers ne peut pas en prendre connaissance, il n'y a pas de révélation constitutive d'infraction.

En revanche, la transmission de données personnelles secrètes à un collaborateur interne ou à un prestataire de services externe est également considérée comme une divulgation. Les situations dans lesquelles des tiers révèlent des données personnelles à un employé en lui demandant de les garder strictement secrètes peuvent s'avérer problématiques. On peut penser ici à un employé du service du personnel d'une entreprise qui est informé par un autre employé d'un dysfonctionnement au sein de l'entreprise, ce dernier exigeant que son identité reste secrète. D'une part, l'employé du service du personnel peut se rendre punissable s'il révèle (malgré tout) son identité en interne, d'autre part, l'entreprise devra prendre en compte les connaissances de certains employés. Dans la pratique, il faut ici des règles claires sur la manière de traiter de telles communications et sur ce qui doit être communiqué, à qui, quand et comment.

15 Ni le libellé de l'art. 62 ni le message ne permettent de déterminer qui est le maître du secret protégé par cette disposition. Selon le message, la disposition de l'art. 62 se rattache toutefois expressément au secret professionnel de l'art. 321 CP, raison pour laquelle il se justifie de comprendre l'art. 62 comme un "secret professionnel" et non comme une norme relevant uniquement du droit de la protection des données : Le maître du secret est celui qui a confié son secret à la personne professionnelle pour l'exercice de sa profession. C'est donc la confiance du maître du secret dans la confidentialité de la

communication à la personne exerçant une activité professionnelle qui est protégée, et seule la rupture de cette confiance (c'est-à-dire pas toute violation de la protection des données) est punissable. L'article 62 protège la confiance d'un professionnel dans le fait qu'il gardera en tant que tel le secret qui lui a été confié dans le cadre de l'exercice de sa profession - indépendamment de l'existence d'une relation contractuelle directe avec la personne à qui le secret a été confié. Selon le point de vue défendu ici, seule une révélation de données personnelles qui intervient en réponse à une attente légitime du maître du secret quant au traitement confidentiel de ces données peut être constitutive d'une infraction. Une entreprise peut orienter les attentes du client/maître du secret en mentionnant dans sa déclaration de protection des données les catégories de tiers auxquelles elle transmet des données personnelles. Pour autant que la mention dans la déclaration de confidentialité soit "suffisamment claire", le détenteur du secret ne pourra plus faire valoir d'"attentes légitimes" quant au traitement confidentiel des données personnelles concernées.

Même si l'article 62 est compris dans ce sens plus étroit, cette disposition est encore très large et indéterminée : La question de savoir quand on peut partir du principe que la confidentialité est protégée par le droit pénal n'est pas clarifiée (et ne l'était pas non plus sous l'art. 35 aDSG). Il est tout de même clair que tout fait révélé à une personne exerçant une activité professionnelle et qui n'est pas de notoriété publique ne mérite pas cette protection. Avec Rosenthal/Gubler (p. 61), il faut exiger (compte tenu des exigences posées à une norme pénale par le principe de précision de l'art. 1 CP) que (i) le maître du secret ait suscité une attente légitime que sa volonté de garder le secret soit respectée et que (ii) le secret ait été révélé au détenteur du secret ou à son organisation dans ce cadre. Il faut donc qu'il y ait au moins un accord tacite de confidentialité. 16

C. Eléments subjectifs de l'infraction

D'un point de vue subjectif, l'intention de l'auteur est requise, c'est-à-dire que l'auteur doit avoir connaissance de l'obligation de garder le secret, du caractère secret des données personnelles et de la révélation. Il suffit que l'auteur considère comme possible que des tiers puissent avoir connaissance des données personnelles, mais qu'il agisse malgré tout parce qu'il s'en accommode (dol éventuel). Dans la pratique, il n'est pas rare que la 17

punissabilité échoue parce qu'il n'est pas possible de prouver la connaissance du devoir de discrétion et du caractère secret des données personnelles, notamment en l'absence d'indications selon lesquelles l'entreprise concernée a transmis les connaissances correspondantes à ses employés.

III. ILLÉGALITÉ ET CULPABILITÉ

18 Cf. OK-Gassmann ad art. 60, n. 26 s. La révélation peut notamment être justifiée par le consentement du maître du secret, les principes développés par la jurisprudence et la dogmatique à l'art. 321 ch. 2 CP s'appliquant par analogie. Des dispositions légales autorisant la révélation (art. 14 CP) ou même l'imposant entrent également en ligne de compte. On pense ici par exemple à l'obligation de collaborer dans le cadre de la procédure.

IV. DÉLIMITATION ET CONCURRENCE

20 Outre l'art. 320 CP (violation du secret de fonction) et l'art. 321 CP (violation du secret professionnel), l'art. 62 protège également le maître du secret contre la divulgation illicite de données secrètes à des tiers. L'art. 62 comble toutefois la lacune créée par la limitation de la qualité d'auteur et se trouve par conséquent en faux concours idéal avec les deux dispositions du code pénal. Par analogie avec l'art. 35 aDSG, la violation du secret des données est absorbée par les art. 320 et 321 CP (consommation).

21 Si les éléments constitutifs de l'infraction de l'art. 47 LB sont également remplis, ce dernier prime en tant que norme spéciale.

L'auteur remercie chaleureusement MLaw Antonia Straden pour sa collaboration au commentaire de cet article.

BIBLIOGRAPHIE

Niggli Marcel Alexander/Maeder Stefan, Kommentierung zu Art. 35 aDSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Basler Kommentar, Datenschutzgesetz / Öffentlichkeitsgesetz, 3. Aufl., Basel 2014.

Oberholzer Niklaus, Kommentierung zu Art. 321 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafrecht (StGB/JStGB), 4. Aufl., Basel 2018.

Poledna Thomas/Berger Brigitte, Öffentliches Gesundheitsrecht, Bern 2002.

Rosenthal David, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020; Rosenthal David/Gubler, Seraina, Die Strafbestimmungen des neuen DSG, SZW 1/2021, S. 52 ff.; Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Wohlers Wolfgang, Kommentierung zu Art. 62 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski, Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Daten-schutz und die Änderung weiterer Erlasse zum Datenschutz vom 23.3.1988, BBl 1988 II S. 413 ff. (zit. Botschaft 1988), abrufbar unter https://www.admin.ch/opc/de/federal-gazette/1988/II/413.pdf, besucht am 8.8.2023.

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 S. 6941 ff. (zit. Botschaft 2017), abrufbar unter https://www.admin.ch/opc/de/federal-gazette/2017/6941.pdf, besucht am 8.8.2023.

Erläuternder Bericht des Bundesamts für Justiz BJ zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016, abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf.download.pdf/vn-ber-d.pdf (zit. Erläuternder Bericht VE-DSG), besucht am 8.8.2023.

Zusammenfassung des Bundesamts für Justiz BJ der Ergebnisse des Vernehmlassungsverfahrens vom 10.8.2017 betreffend Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016 (zit. Zusammenfassung Vernehmlassung VE-DSG), abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/ve-ber-d.pdf.download.pdf/ve-ber-d.pdf, besucht am 8.8.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 63 LPD

Un commentaire de Jonas D. Gassmann

PROPOSITION DE CITATION

Jonas D. Gassmann, Kommentierung zu Art. 63 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Gassmann, N. XXX zu Art. 63 DSG.

Art. 63 Insoumission à une décision

Sont punies d'une amende de 250 000 francs au plus les personnes privées qui, intentionnellement, ne se conforment pas à une décision du PFPDT ou d'une autorité de recours, à elles signifiée sous la menace de la peine prévue au présent article.

TABLE DES MATIÈRES

En bref 827
I. Généralités 827
II. Non-respect d'une décision du PFPDT ou d'une décision d'une instance de recours 828
A. Faits objectifs 828
1. Décision du PFPDT ou décision d'une instance de recours 828
2. Non-respect de l'obligation 829
B. Eléments subjectifs de l'infraction 830
III. Illégalité et culpabilité 830
Bibliographie 830
Matériaux 830

EN BREF

La disposition de l'art. 63 punit le fait de ne pas se conformer intentionnellement à une décision du PFPDT ou à une décision d'une instance de recours. La punissabilité suppose que la décision soit assortie d'une menace de sanction correspondante et qu'il ressorte suffisamment concrètement de la décision pour le destinataire ce qu'il doit faire ou ne pas faire. Si cette condition est remplie, une amende de 250 000 francs au maximum est encourue.

I. GÉNÉRALITÉS

L'art. 63 est une norme de désobéissance conçue en blanc. Des dispositions pénales comparables se rencontrent souvent dans le droit pénal accessoire, même si la peine encourue est à chaque fois nettement plus faible. En tant que lex specialis, la disposition de l'art. 63 prime sur la disposition de l'art. 292 CP (désobéissance à une décision de l'autorité) contenue dans le droit pénal fondamental. 1

La disposition de l'art. 63 n'a été ajoutée à la loi qu'après la consultation. De l'avis du législateur, le recours à l'art. 292 CP n'aurait pas été suffisant en raison de la sanction trop faible qu'il prévoyait. Lors de la consultation, plusieurs critiques ont été émises quant au fait que les nouvelles dispositions pénales étaient formulées de manière trop ouverte. L'art. 63 permet désormais au PFPDT d'ordonner le respect des obligations prévues par la LPD et de les assortir d'une menace de peine. L'obligation peut ainsi être concrétisée dans la décision de manière à ce qu'il soit suffisamment clair pour le destinataire ce qu'il doit faire ou ne pas faire. 2

La norme pénale de l'art. 63 est un délit poursuivi d'office. 3

Le but de la disposition de l'art. 63 est, d'une part, de compenser les dispositions pénales supprimées par rapport à l'AP-LPD (concernant les communications au PFPDT) et, d'autre part, de prendre en compte "les questions relatives au principe nulla poena sine lege, telles qu'elles ont souvent été soulevées lors de la consultation". 4

Selon le Conseil fédéral, la solution créée par l'art. 63 "permet de continuer à concevoir les dispositions correspondantes de la LPD électronique sous une 5

forme suffisamment générale, sans entrer en même temps en conflit avec les exigences de droit pénal en matière de précision d'une réglementation légale". En outre, selon le Conseil fédéral, elle facilite le travail des autorités de poursuite pénale compétentes, ce qui permettrait de tenir compte des doutes partiellement exprimés lors de la consultation.

6 Cette disposition vise l'exécution des décisions du PFPDT au sens de l'art. 51, que celui-ci rend après une enquête et l'exécution des décisions des instances de recours. En revanche, la menace d'amende de l'art. 60 al. 2 concerne la fourniture intentionnelle de faux renseignements et le refus intentionnel de coopérer dans le cadre d'une enquête du PFPDT.

7 L'infraction visée à l'art. 63 est un délit spécial : seules les personnes destinataires d'une décision du PFPDT ou d'une décision d'une instance de recours peuvent être considérées comme des auteurs. D'autres personnes entrent tout au plus en ligne de compte en tant qu'instigateurs. Si la décision du PFPDT ou la décision d'une instance de recours s'adresse à une entreprise, la punissabilité s'applique à une personne dirigeante en vertu de l'art. 29 CP : L'obligation qui incombe à l'entreprise et qui fonde l'infraction est imputée à la personne physique. Celui qui n'empêche pas les infractions commises par des collaborateurs subordonnés ou qui n'en supprime pas les effets entre également en ligne de compte comme auteur (art. 6 al. 2 et 3 DPA en relation avec l'art. 64 al. 1 LPD).

II. NON-RESPECT D'UNE DÉCISION DU PFPDT OU D'UNE DÉCISION D'UNE INSTANCE DE RECOURS

A. Faits objectifs

1. Décision du PFPDT ou décision d'une instance de recours

8 Une sanction au sens de l'art. 63 présuppose qu'une personne déterminée se voit prescrire, dans une décision valablement rendue et notifiée, un comportement suffisamment concret en cas de non-respect de la décision ou de la décision, sous la menace d'une sanction au sens de cette disposition. Il n'existe aucune obligation pour le PFPDT ou les instances de recours d'assortir leurs décisions de la menace de sanction prévue à l'art. 63. Afin de

rendre plus probable le respect des décisions, le PFPDT et les instances de recours devraient toutefois faire régulièrement usage de cette possibilité.

Une décision du PFPDT est un acte de souveraineté adressé par le PFPDT à une personne déterminée sur la base de l'art. 51, par lequel une relation juridique concrète de droit administratif est réglée de manière contraignante et exécutoire en créant ou en constatant un droit. Comme pour l'art. 292 CP, il est exigé que la décision contienne une instruction concrète de comportement (faire, tolérer ou s'abstenir) ; une simple décision de constatation ne satisfait pas à cette exigence. Une décision générale n'est pas non plus un objet approprié. Une instruction de comportement concrète comprend par exemple l'ordre d'adapter ou de cesser un certain traitement de données personnelles ou de s'abstenir de communiquer des données personnelles à l'étranger (voir sur l'ensemble OK-Fanger/Oehri sur l'art. 51 LPD). La décision doit "exister juridiquement" (elle ne doit donc pas être entachée d'un vice grave qui la rendrait nulle), être valablement communiquée au destinataire et avoir formellement force de chose jugée. 9

Une décision d'une instance de recours signifie un jugement d'un tribunal qui statue sur un recours contre une décision du PFPDT, c'est-à-dire un jugement du Tribunal administratif fédéral (art. 33 let. d LTAF) ou du Tribunal fédéral (art. 86 al. 1 let. a LTF). 10

Conformément à l'art. 1 CP, une sanction n'entre en ligne de compte que si la norme pénale applicable satisfait au principe de précision. Etant donné que l'art. 63 lui-même ne décrit pas l'acte, mais renvoie à la décision du PFPDT ou à la décision d'une instance de recours, la décision ou l'ordonnance pénale doit également satisfaire aux exigences du principe de précision de la base légale. Le principe de légalité exige que l'obligation imposée dans la décision soit "décrite de manière suffisamment claire" (cf. déjà ci-dessus, n. 9) ; en d'autres termes, il doit être clair pour le destinataire de la décision quel comportement concret est exigé de lui. 11

2. Non-respect de l'obligation

En tant qu'acte, l'infraction de l'art. 63 exige que le destinataire de la décision ne donne pas suite à la décision. Le contenu de la décision ou de l'ordonnance détermine ce qu'il faut entendre par "ne pas donner suite". Si le PFPDT décide par exemple d'interdire la communication de données 12

personnelles à l'étranger, la communication correspondante constitue une "non-exécution" ; si l'auteur communique plusieurs fois des données personnelles à l'étranger malgré l'interdiction, il remplit plusieurs fois les éléments constitutifs de l'infraction visée à l'art. 63.

B. Eléments subjectifs de l'infraction

13 D'un point de vue subjectif, l'élément constitutif de l'infraction de l'art. 63 exige l'intention, le dol éventuel étant suffisant. L'auteur agit avec un dol éventuel lorsqu'il ne sait pas avec certitude que son comportement contrevient à la décision ou à l'ordonnance, mais qu'il s'accommode ou accepte de commettre éventuellement une infraction.

III. ILLÉGALITÉ ET CULPABILITÉ

Cf. OK-Gassmann, art. 60 LPD, n. 26 s.

BIBLIOGRAPHIE

Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich 2020.

Riedo Christof/Boner Barbara, Kommentierung zu Art. 292 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafrecht (StGB/JStGB), 4. Aufl., Basel 2018.

Rosenthal David/Gubler, Seraina, Die Strafbestimmungen des neuen DSG, SZW 1/2021, S. 52 ff.; Wohlers Wolfgang, Kommentierung zu Art. 63 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski, Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 S. 6941 ff. (zit. Botschaft 2017), abrufbar unter https://www.admin.ch/opc/de/federal-gazette/2017/6941.pdf, besucht am 8.8.2023.

Erläuternder Bericht des Bundesamts für Justiz BJ zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die

Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016, abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf.download.pdf/vn-ber-d.pdf (zit. Erläuternder Bericht VE-DSG), besucht am 8.8.2023.

Vernehmlassung der Kantone betreffend Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016 (zit. Vernehmlassung VE-DSG Kantone), abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/kantone.pdf.download.pdf/kantone.pdf, besucht am 8.8.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 64 LPD

Un commentaire de Jonas D. Gassmann

PROPOSITION DE CITATION

Jonas D. Gassmann, Kommentierung zu Art. 64 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Gassmann, N. XXX zu Art. 64 DSG.

Art. 64 Infractions commises dans une entreprise

[1] Les art. 6 et 7 de la loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA) sont applicables aux infractions commises dans une entreprise.

[2] Lorsque l'amende entrant en ligne de compte ne dépasse pas 50 000 francs et que l'enquête rendrait nécessaires à l'égard des personnes punissables selon l'art. 6 DPA des mesures d'instruction hors de proportion avec la peine encourue, l'autorité peut renoncer à poursuivre ces personnes et condamner l'entreprise (art. 7 DPA) au paiement de l'amende à leur place.

TABLE DES MATIÈRES

En bref 835
I. Généralités 835
II. Infractions commises dans des entreprises commerciales 836
A. Applicabilité des art. 6 et 7 DPA (al. 1) 836
B. Condamnation de l'entreprise à une amende (al. 2) 837
1. généralités 837
2. Infraction dans l'exploitation commerciale 838
3. Amende de 50 000 francs au maximum 838
4. Les mesures d'enquête visant à identifier les personnes punissables seraient disproportionnées. 839
5. Transfert de l'amende 840
Bibliographie 840
Matériaux 841

EN BREF

La responsabilité du chef d'entreprise est introduite dans la LPD par le biais d'un renvoi à deux dispositions isolées de la loi fédérale sur le droit pénal administratif (DPA). L'art. 64 permet, dans certaines circonstances, de répercuter sur l'entreprise une amende infligée à la personne physique responsable en cas d'infraction commise dans le cadre de l'exploitation d'une entreprise, si cette amende s'élève à 50 000 francs au maximum.

I. GÉNÉRALITÉS

Comme il incombe aux cantons de poursuivre et de juger les infractions au sens du chapitre 8 (art. 65 al. 1), la loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA) n'est en principe pas applicable (art. 1 DPA e contrario). Or, l'art. 64 al. 1 renvoie expressément aux art. 6 et 7 DPA en ce qui concerne les infractions commises dans les entreprises. 1

Le renvoi à l'art. 6 DPA (détermination de la personne responsable d'une infraction commise dans une entreprise) et à l'art. 7 DPA (responsabilité subsidiaire de l'entreprise) introduit la responsabilité du chef d'entreprise dans la LPD. Cela doit permettre "une attribution appropriée de la responsabilité pénale dans les entreprises", c'est-à-dire à son niveau de direction (personnes dirigeantes ayant le pouvoir de décider et de donner des instructions). 2

Le montant maximal de l'amende selon l'al. 2 (qui modifie la disposition de l'art. 7 DPA), jusqu'auquel l'entreprise (au lieu de la personne physique) doit pouvoir être condamnée au paiement de l'amende, était encore fixé à 100 000 francs dans l'art. 53 AP-LPD. Des déclarations controversées lors de la procédure de consultation ont conduit à ce que le montant maximal de l'amende soit finalement fixé à 50 000 francs. Le montant maximal de l'amende, substantiellement plus élevé que celui de l'art. 7 DPA, s'explique par le fait que le cadre des amendes en cas d'infraction à la LPD (amendes jusqu'à 250 000 francs) dépasse largement le montant prévu à l'art. 7 DPA (5 000 francs) et que le montant maximal de l'amende a dû être augmenté pour qu'il y ait encore une place dans la pratique pour l'application de la disposition de l'art. 64, al. 2. 3

II. INFRACTIONS COMMISES DANS DES ENTREPRISES COMMERCIALES

A. Applicabilité des art. 6 et 7 DPA (al. 1)

4 L'art. 64 al. 1 renvoie, pour les "infractions commises dans une entreprise", aux art. 6 et 7 DPA, et donc à deux articles isolés au sein du DPA. Le calcul de l'amende ne se base donc pas sur l'art. 8 DPA, mais sur l'art. 106 al. 3 CP. Etant donné que, selon son art. 1, la DPA ne s'applique en principe pas aux infractions à la LPD passibles de sanctions pénales, ce renvoi explicite est nécessaire si l'on veut également introduire une sorte de "responsabilité du chef d'entreprise" dans la LPD (cf. aussi ci-dessus, n. 1 ss).

5 Par "entreprise commerciale", on entend toute activité entrepreneuriale dans laquelle on participe activement à la vie économique en utilisant du capital et du travail. Il s'agit donc d'infractions commises dans l'exercice d'activités économiques au sein d'une entreprise. L'art. 6 al. 1 DPA ne couvre pas les actes commis à la seule occasion de l'exercice d'activités commerciales.

6 L'art. 6 al. 1 DPA établit le principe dit de l'auteur : est auteur celui qui a commis l'infraction. Est par exemple punissable l'employé qui, sans y avoir été invité par un supérieur hiérarchique et sans y avoir été autorisé, utilise pour l'exercice de son activité un outil d'un fournisseur de services en ligne dans le cadre duquel des données personnelles sont traitées, mais qui ne s'est pas soucié de conclure un contrat de traitement des données de commande juridiquement suffisant (punissabilité selon l'art. 61 al. 1 let. b). Un autre exemple serait la divulgation non autorisée de données personnelles secrètes par un collaborateur à un tiers dans l'exercice de sa profession (punissabilité selon l'art. 62).

7 La condition préalable à la responsabilité de l'employeur (responsabilité de l'employeur au sens de l'art. 6 al. 2 DPA) est, d'un point de vue objectif, l'existence d'une obligation de garantie, celle-ci ne pouvant pas être déduite de l'art. 6 al. 2 DPA, mais découlant "de la responsabilité pour l'entreprise en tant que source de danger et/ou de la responsabilité pour le comportement des subordonnés". On peut penser ici par exemple à un responsable de la conformité qui est contractuellement responsable de la garantie du respect des exigences légales en matière de protection des données dans l'entreprise ou au responsable du personnel qui est contractuellement responsable du

traitement des données du personnel. Une délégation de responsabilité est autorisée par la loi, la personne qui délègue restant responsable de la sélection, de l'instruction et de la surveillance de la personne concernée. Une autre condition préalable est l'existence d'un pouvoir d'action de la part de l'employeur : pour que la responsabilité de l'employeur s'applique, l'employeur doit avoir eu la possibilité d'empêcher l'acte ou d'en supprimer les effets. D'un point de vue subjectif, l'art. 6 al. 2 DPA exige l'intention ou la négligence. Dans le cas d'infractions causales qui (comme les dispositions pénales du chapitre 8 de la LPD) sont conçues comme des délits intentionnels, la question de savoir s'il suffit que l'employeur n'ait pas empêché l'infraction ou n'en ait pas annulé les effets par simple négligence pour que la responsabilité de l'employeur soit applicable et donc pour que celui-ci soit punissable est controversée. Selon l'opinion défendue ici, pour que la responsabilité de l'employeur soit applicable à de tels actes, il faut que l'employeur ait violé son devoir de garant au moins par dol éventuel. Si l'auteur direct (qui a commis l'infraction) n'a agi que par négligence, la responsabilité de l'apporteur d'affaires est d'emblée exclue pour de tels actes occasionnels.

Si le chef d'entreprise, l'employeur, le mandant ou le représenté est une personne morale, une société en nom collectif ou en commandite, une entreprise individuelle ou une collectivité de personnes sans personnalité juridique, l'art. 6 al. 2 DPA s'applique "aux organes, membres d'organes, associés gérants, personnes effectivement dirigeantes ou liquidateurs coupables" (art. 6 al. 3 DPA ; cf. aussi art. 29 CP). 8

B. Condamnation de l'entreprise à une amende (al. 2)

1. généralités

L'art. 64 al. 2 se base sur la disposition de l'art. 7 al. 1 DPA, mais adapte le champ d'application à l'amende maximale prévue par la LPD et parle de manière plus générique de "l'entreprise commerciale" au lieu de la "personne morale", de la "société en nom collectif ou en commandite" et de la "raison individuelle" (cf. aussi ci-dessus, n. 3 et n. 5). 9

Selon l'art. 64 al. 2, une amende peut être infligée à une entreprise (en lieu et place des personnes physiques punissables) en cas d'infraction pénale 10

commise dans le cadre de l'exploitation de l'entreprise (par une ou plusieurs personnes physiques ; cf. ci-dessous, n. 11 s.), si

- une amende de 50 000 francs au maximum entre en ligne de compte (cf. ci-dessous, n. 13 s.) et (de manière cumulative)
- l'identification des personnes punissables selon l'art. 6 DPA nécessiterait des mesures d'instruction qui seraient disproportionnées par rapport à la peine infligée (à ce sujet, n. 15 s. infra).

2. Infraction dans l'exploitation commerciale

11 Pour que l'entreprise soit condamnée à une amende, il faut tout d'abord qu'il y ait une "infraction dans l'exploitation de l'entreprise". Tous les éléments constitutifs objectifs et subjectifs de l'infraction pour laquelle l'entreprise doit être condamnée à une amende doivent être remplis et il ne doit pas y avoir de motifs de justification ou d'exclusion de la culpabilité. Concernant la notion d'"entreprise commerciale", voir ci-dessus, n. 5.

12 Dans la pratique, les éléments subjectifs de l'infraction ne pourront toutefois pas être prouvés, car les personnes physiques punissables ne sont justement pas identifiables. Pour surmonter cet obstacle et ne pas exclure d'emblée l'application de l'art. 64, il convient d'"objectiver" la faute ou d'assouplir les exigences en matière de preuve des éléments subjectifs de l'infraction, par exemple en permettant à l'autorité pénale de se contenter de constater "que l'intention ressort clairement de l'acte commis". En tout état de cause, il n'y a pas de place pour l'application de l'article 64 s'il est établi que l'élément subjectif de l'infraction n'est pas réalisé chez les personnes présumées coupables au sein de l'entreprise.

3. Amende de 50 000 francs au maximum

13 Selon l'art. 7 al. 1 DPA, le montant de l'amende jusqu'à concurrence duquel il est possible de condamner une entreprise plutôt qu'une personne physique au paiement d'une amende est de 5 000 francs. Cette limite supérieure correspond à la moitié du montant maximal de l'amende de 10 000 francs prévu par l'art. 106 al. 1 CP. En dérogation à l'art. 106 al. 1 CP, le montant maximal de l'amende dans le domaine d'application de la LPD (selon les art. 60 à 63) est de 250 000 francs. Compte tenu de ce montant maximal nettement plus élevé, il s'imposait d'augmenter également la limite supérieure

du montant de l'amende jusqu'à laquelle une condamnation d'une entreprise commerciale est possible. Selon l'art. 64 al. 2, ce plafond est de 50 000 francs, ce qui correspond à 1/5 du montant maximal de l'amende de 250 000 francs.

Selon l'art. 106 al. 3 CP, le juge doit, pour déterminer le montant de l'amende, tenir compte de la situation de l'auteur "afin que celui-ci subisse la peine correspondant à sa faute". Comme l'auteur de l'infraction ne peut justement pas être identifié, l'amende doit être calculée sur la base d'une faute objective. Les circonstances de l'infraction concrète sont déterminantes, comme par exemple l'absence de structuration interne de l'entreprise en différents domaines de responsabilité. 14

4. Les mesures d'enquête visant à identifier les personnes punissables seraient disproportionnées.

Les circonstances du cas d'espèce sont également importantes pour déterminer si des mesures d'enquête visant à identifier les personnes punissables seraient disproportionnées par rapport à la peine prononcée. L'article 64, al. 2, étant une disposition "potestative", les autorités pénales disposent d'un pouvoir d'appréciation relativement important pour déterminer si cette disposition doit être appliquée (et donc aussi pour répondre à la question de savoir si des mesures d'enquête visant à identifier les personnes punissables seraient disproportionnées). Il n'existe pas de droit à l'application de l'art. 64 al. 2, mais l'autorité pénale ne peut pas non plus simplement choisir entre une action contre les personnes physiques punissables et contre l'entreprise commerciale. Avant que l'autorité pénale compétente puisse envisager de sanctionner l'entreprise commerciale sur la base de l'article 64, elle doit procéder à "un minimum de mesures d'enquête" pour identifier les personnes physiques punissables ; il n'est pas acceptable que l'autorité pénale se fonde sur l'article 64 par pure commodité. La question de savoir si des mesures d'enquête (supplémentaires) seraient disproportionnées doit également être évaluée au regard du montant de l'amende (potentielle) infligée, pour laquelle les investigations doivent en tout cas être suffisamment poussées pour que le montant puisse être évalué au moins grossièrement. 15

En ce qui concerne les infractions à la LPD passibles de sanctions pénales, il sera souvent possible de déterminer clairement, du point de vue de l'organisation, ou du moins relativement facilement dans le cas concret, qui a 16

effectué les actes concernés (p. ex. réponse à une demande de renseignements ou validation de la déclaration de protection des données). Dans cette mesure, la pertinence pratique de la disposition de l'article 64 devrait être plutôt faible ; les condamnations d'entreprises commerciales au paiement d'une amende devraient rester l'exception.

5. Transfert de l'amende

17 Si les conditions susmentionnées sont remplies, l'autorité pénale compétente peut répercuter l'amende sur l'entreprise. Lors de la détermination du montant de l'amende, ce sont la faute et la situation financière de la ou des personnes physiques réellement punissables qui sont déterminantes, et non pas celles de l'entreprise commerciale.

18 Si seules certaines personnes physiques responsables de l'infraction peuvent être identifiées, mais pas d'autres, il est contestable qu'il soit possible de répercuter l'amende sur les personnes non identifiées. Il est plus juste d'exiger qu'un transfert soit également possible dans cette constellation.

BIBLIOGRAPHIE

Beretta Allison, Sanctionner en vertu des art. 6 et 7 DPA, in: Jusletter vom 8.7.2019, 64, https://jusletter.weblaw.ch/juslissues/2019/986/sanctionner-en-vertu_20314b3ff6.html, besucht am 8.8.2023.

Macaluso Alain/Garbarski Andrew M., Kommentierung zu Art. 7 VStrR, in: Frank Friedrich/Eicker Andreas/Markwalder Nora/Achermann, Jonas (Hrsg.), Basler Kommentar, Verwaltungsstrafrecht, Basel 2020.

Rosenthal David/Gubler Seraina, Die Strafbestimmungen des neuen DSG, SZW 1/2021, S. 52 ff.; Schwob Renate, Kommentierung zu Art. 6 VStrR, in: Frank Friedrich/Eicker Andreas/Markwalder Nora/Achermann, Jonas (Hrsg.), Basler Kommentar, Verwaltungsstrafrecht, Basel 2020.

Wohlers Wolfgang, Kommentierung zu Art. 64 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski, Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 S. 6941 ff. (zit. Botschaft 2017), abrufbar unter https://www.admin.ch/opc/de/federal-gazette/2017/6941.pdf, besucht am 8.8.2023.

Erläuternder Bericht des Bundesamts für Justiz BJ zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016, abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf.download.pdf/vn-ber-d.pdf (zit. Erläuternder Bericht VE-DSG), besucht am 8.8.2023.

Zusammenfassung des Bundesamts für Justiz BJ der Ergebnisse des Vernehmlassungsverfahrens vom 10.8.2017 betreffend Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016 (zit. Zusammenfassung Vernehmlassung VE-DSG), abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/ve-ber-d.pdf.download.pdf/ve-ber-d.pdf, besucht am 8.8.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 65 LPD

Un commentaire de Jonas D. Gassmann

PROPOSITION DE CITATION

Jonas D. Gassmann, Kommentierung zu Art. 65 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Gassmann, N. XXX zu Art. 65 DSG.

Art. 65 Compétence

[1] La poursuite et le jugement des infractions incombent aux cantons.

[2] Le PFPDT peut dénoncer des infractions aux autorités de poursuite pénale compétentes et faire valoir les droits d'une partie plaignante dans la procédure.

TABLE DES MATIÈRES

En bref 845
I. Généralités 845
II. Compétence en matière de poursuite pénale et de juridiction 846
A. Compétence cantonale (al. 1) 846
B. Compétence multiple 846
III. Droits du PFPDT (al. 2) 847
A. Droit de dénonciation 847
B. Constitution de partie civile 847
Bibliographie 847
Matériaux 848

EN BREF

Comme le prévoient déjà la Constitution fédérale et le code de procédure pénale, la poursuite et le jugement des actes punissables relèvent de la compétence des cantons, conformément au chapitre 8 de la loi sur la protection des données. Le PFPDT dispose d'un droit de dénonciation et peut se constituer partie civile dans la procédure pénale.

I. GÉNÉRALITÉS

La disposition de l'art. 65 al. 1 découle de l'art. 123 al. 2 Cst. selon lequel la compétence pour rendre la justice en matière pénale ainsi que pour l'exécution des peines et des mesures incombe en premier lieu et principalement aux cantons. Elle se recoupe avec la disposition de l'art. 22 CPP. L'art. 65 al. 1 est de nature purement déclaratoire dans la mesure où cette disposition ne consacre pas une compétence fédérale et ne s'écarte donc pas de la compétence cantonale déjà prévue par les dispositions susmentionnées. En d'autres termes, même en l'absence d'une norme explicite, les cantons seraient compétents pour la poursuite et le jugement des actes punissables selon le chapitre 8. 1

La disposition de l'art. 65 al. 1 était déjà prévue ainsi dans l'avant-projet. Lors de la procédure de consultation, la majorité des cantons s'est opposée à ce que la poursuite et le jugement des infractions continuent d'incomber aux cantons. Cette opposition était motivée par la crainte que les procédures pénales n'augmentent en raison du nombre plus élevé de comportements illicites et de sanctions plus sévères, ce qui nécessiterait l'engagement de collaborateurs spécialisés. Il a également été avancé que la compétence cantonale rendrait difficile une mise en œuvre uniforme du droit de la protection des données. 2

L'art. 65 al. 2 renforce la position du PFPDT en lui accordant expressément le droit de déposer une plainte pénale et de se constituer partie civile dans la procédure pénale au sens des art. 118 CPP et suivants. 3

La disposition de l'art. 65 al. 2 ne figurait pas encore dans l'avant-projet, mais seulement dans le projet. Lors de la procédure de consultation, il a été demandé à plusieurs reprises d'habiliter le PFPDT à infliger des sanctions 4

administratives. Contrairement au droit européen, il a toutefois été décidé de ne pas donner au PFPDT la possibilité de prononcer des sanctions. Au lieu de cela, l'absence de compétence pour infliger des sanctions administratives a été compensée par l'introduction d'autres dispositions dans la LPD. Il s'agit notamment de l'art. 65 al. 2, qui permet au PFPDT de porter plainte auprès de l'autorité pénale cantonale et d'exercer les droits de la partie civile dans la procédure pénale, ou des dispositions pénales de l'art. 60 al. 2 et de l'art. 63.

II. COMPÉTENCE EN MATIÈRE DE POURSUITE PÉNALE ET DE JURIDICTION

A. Compétence cantonale (al. 1)

5 Tant la poursuite que le jugement des actes punissables selon le chapitre 8 relèvent de la compétence des cantons (juridiction cantonale dite d'origine).

6 La loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA) n'est donc en principe pas applicable (pour qu'elle le soit, il faudrait que la compétence mentionnée relève d'une autorité administrative de la Confédération, art. 1 DPA). En vertu d'un renvoi explicite à l'art. 64 al. 1, les articles 6 et 7 DPA s'appliquent toutefois aux infractions commises dans les entreprises. Ce renvoi ne change rien à la compétence cantonale mentionnée.

7 La compétence à raison du lieu est régie par les règles générales de for des art. 31 ss CPP. CPP.

B. Compétence multiple

8 L'art. 65 ne s'exprime pas sur la situation dans laquelle une affaire pénale relève à la fois de la juridiction cantonale et de la juridiction fédérale. On peut penser ici à un auteur qui ne viole pas seulement une ou plusieurs infractions du chapitre 8, mais aussi une ou plusieurs infractions relevant de la juridiction fédérale.

9 En l'absence de réglementation explicite, il convient ici de se référer à l'art. 26 al. 2 CPP : Selon cette disposition, le Ministère public de la Confédération "peut ordonner la jonction des procédures entre les mains des autorités fédérales ou cantonales".

III. DROITS DU PFPDT (AL. 2)

A. Droit de dénonciation

Le PFPDT a le droit (mais pas l'obligation) de porter plainte auprès de l'autorité de poursuite pénale compétente. Il n'a toutefois pas le droit de déposer une plainte pénale. Seule la personne concernée dont les droits (tels que le droit à l'information, le droit d'accès, le droit de transférer en toute sécurité ses propres données personnelles à des tiers) ont été violés a le droit de déposer une plainte pénale. 10

Il appartient à l'autorité pénale compétente d'ouvrir une enquête pénale lorsqu'elle dispose d'indices concrets qu'une infraction a pu être commise (art. 7 al. 1 CPP). Dans le cadre de l'art. 8 CPP, le ministère public peut renoncer à la poursuite pénale et notamment classer une procédure pénale déjà ouverte, par exemple s'il s'agit d'un cas de peu d'importance ou si l'auteur a réparé le dommage causé et qu'il n'existe pas d'intérêts s'opposant au classement de la procédure pénale. 11

B. Constitution de partie civile

Le PFPDT a également le droit de se constituer partie civile (et donc partie, art. 104 al. 1 let. b CPP) dans la procédure pénale cantonale au sens de l'art. 118 CPP. Si cela lui semble nécessaire dans l'intérêt d'une application uniforme de la LPD, le PFPDT peut ainsi par exemple 12

- contester les ordonnances de classement (art. 322 al. 2 CPP) et faire recours contre les jugements cantonaux (art. 382 al. 1 CPP) ;
- demander à consulter le dossier (art. 101 al. 1 CPP) ;
- participer aux actes de procédure (art. 107 al. 1 let. b CPP) et à l'administration des preuves (art. 147 ss. CPP) ; et
- faire des demandes de preuves (art. 107 al. 1 let. e CPP).

BIBLIOGRAPHIE

Kipfer Daniel, Kommentierung zu Art. 22 StPO, in: Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Basler Kommentar,

Strafprozessordnung/Jugendstrafprozessordnung (StPO/JStPO), 2. Aufl., Basel 2014.

Rosenthal David/Gubler, Seraina, Die Strafbestimmungen des neuen DSG, SZW 1/2021, S. 52 ff.; Wohlers Wolfgang, Kommentierung zu Art. 65 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski, Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 S. 6941 ff. (zit. Botschaft 2017), abrufbar unter https://www.admin.ch/opc/de/federal-gazette/2017/6941.pdf, besucht am 8.8.2023.

Zusammenfassung des Bundesamts für Justiz BJ der Ergebnisse des Vernehmlassungsverfahrens vom 10.8.2017 betreffend Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016 (zit. Zusammenfassung Vernehmlassung VE-DSG), abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/ve-ber-d.pdf.download.pdf/ve-ber-d.pdf, besucht am 8.8.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 66 LPD

Un commentaire de Jonas D. Gassmann

PROPOSITION DE CITATION

Jonas D. Gassmann, Kommentierung zu Art. 66 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Gassmann, N. XXX zu Art. 66 DSG.

Art. 66 Prescription de l'action pénale

L'action pénale se prescrit par cinq ans.

TABLE DES MATIÈRES

En bref 851
I. Généralités 851
II. Prescription de l' action pénale 851
A. Durée 851
B. Début de la prescription 852
C. Contraventions répétées 852
III. Prescription de l'exécution 853
Bibliographie 853
Matériaux 853

EN BREF

Les infractions à la loi sur la protection des données, qui sont punissables, sont des contraventions. Contrairement à la disposition générale de l'art. 109 CP, l'action pénale ne se prescrit pas par trois ans, mais par cinq ans. Cela s'explique par le fait que les enquêtes sur d'éventuelles violations du droit de la protection des données sont généralement complexes sur le plan technique, qu'elles requièrent des connaissances spécialisées et que les procédures pénales ne doivent pas échouer en raison d'un délai de prescription trop court. Il convient de distinguer la prescription de l'action publique de la prescription de l'exécution, qui est de trois ans.

I. GÉNÉRALITÉS

L'art. 66 établit une disposition spéciale sur la prescription de l'action pénale pour les infractions à la loi sur la protection des données. Cette disposition s'applique aux infractions à la loi sur la protection des données qui sont punissables conformément au chapitre 8 (art. 60 à 63). Par rapport aux contraventions "ordinaires", elle est plus longue de deux ans. Il s'agit ainsi de tenir compte de la nature technique de ces contraventions et de l'expérience généralement limitée des autorités cantonales de poursuite pénale en matière de protection des données. 1

L'art. 66 est nouveau. Sous l'ancien droit, l'action pénale se prescrivait par trois ans en vertu de l'art. 333, al. 1, CP, conformément à la disposition correspondante du droit pénal général (art. 109 CP). Lors de la procédure de consultation, certains participants se sont prononcés contre une prolongation du délai de prescription. Le texte de l'avant-projet est resté inchangé après les débats parlementaires. 2

II. PRESCRIPTION DE L' ACTION PÉNALE

A. Durée

Les infractions à la loi sur la protection des données, punissables en vertu du chapitre 8, prévoient l'amende comme peine et sont donc qualifiées de contraventions en vertu de l'art. 333 al. 3 CP. 3

4 Conformément à l'art. 109 CP, l'action pénale en matière de contraventions se prescrit par trois ans. Les enquêtes sur d'éventuelles violations de la loi sur la protection des données présupposent régulièrement des connaissances sur les processus techniques sous-jacents, et il n'est pas rare que de telles enquêtes soient complexes. Les autorités cantonales de poursuite pénale compétentes pour l'application des dispositions pénales selon l'art. 65 al. 1 (contrairement aux autorités de surveillance de la protection des données compétentes pour infliger des amendes en vertu du RGPD) n'ont généralement pas ou peu d'expérience dans les questions de protection des données (cf. aussi ci-dessus, n. 1). Afin que les procédures pénales correspondantes n'échouent pas en raison de délais de prescription trop courts, le délai de prescription de l'action pénale a été augmenté de deux ans par rapport à la disposition générale de l'art. 109 CP, pour passer à cinq ans.

B. Début de la prescription

5 Conformément à l'art. 104 CP, le début de la prescription de l'action pénale est déterminé par l'art. 98 CP : Pour les infractions conçues comme des délits d'activité, la prescription commence à courir le jour où la contravention a été commise ou le dernier jour où les éléments constitutifs de l'infraction ont été réalisés. S'il s'agit d'un délit permanent, la prescription commence à courir le jour où le comportement punissable prend fin. Pour les infractions conçues comme des délits d'omission, la prescription ne commence pas à courir tant que l'omission se poursuit ; le moment déterminant est celui où l'obligation d'agir prend fin. Si plusieurs personnes sont impliquées dans une infraction, le délai de prescription commence à courir uniformément pour toutes les personnes concernées à partir du dernier acte partiel.

C. Contraventions répétées

6 Il faut distinguer les contraventions répétées qui visent le même bien juridique des délits permanents. Celles-ci se prescrivent individuellement après l'expiration du délai de prescription de cinq ans. Si, par exemple, un auteur d'infraction au sens de l'art. 61 let. b LPD confie à plusieurs reprises le traitement de données à un sous-traitant sans remplir les conditions de l'art. 9 al. 1 et 2 LPD, les différentes contraventions se prescrivent indépendamment les unes des autres.

III. PRESCRIPTION DE L'EXÉCUTION

L'art. 66 régit uniquement la prescription de l'action pénale et non la prescription de l'exécution. Cette dernière est régie par la disposition générale de l'art. 109 CP. Elle est de trois ans à compter du jour où la décision d'amende est exécutoire (art. 333 al. 1 en relation avec l'art. 109 en relation avec l'art. 100 CP), c'est-à-dire à compter du jour où la décision est entrée en force. Un recours contre la décision d'amende auprès du Tribunal fédéral n'a pas d'effet suspensif (cf. art. 103 LTF), de sorte que la décision d'amende entre en force dès son prononcé par la dernière instance cantonale. 7

BIBLIOGRAPHIE

Heimgartner Stefan, Kommentierung zu Art. 109 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafrecht (StGB/JStGB), 4. Aufl., Basel 2018.

Niggli Marcel Alexander/Maeder Stefan, Kommentierung zu Art. 34 und 35 aDSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Basler Kommentar, Datenschutzgesetz / Öffentlichkeitsgesetz, 3. Aufl., Basel 2014.

Rosenthal David/Gubler Seraina, Die Strafbestimmungen des neuen DSG, SZW 1/2021, S. 52 ff.; Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008; Wohlers Wolfgang, Kommentierung zu Art. 66 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski, Dominika (Hrsg.), Stämpflis Handkommentar, Datenschutzgesetz, 2. Aufl., Bern 2023.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 S. 6941 ff. (zit. Botschaft 2017), abrufbar unter https://www.admin.ch/opc/de/federal-gazette/2017/6941.pdf, besucht am 8.8.2023.

Zusammenfassung des Bundesamts für Justiz BJ der Ergebnisse des Vernehmlassungsverfahrens vom 10.8.2017 betreffend Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016 (zit. Zusammenfassung Vernehmlassung VE-DSG), abrufbar unter https://

www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/ve-ber-d.pdf.download.pdf/ve-ber-d.pdf, besucht am 8.8.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 67 LPD

Un commentaire de Nula Katharina Frei

PROPOSITION DE CITATION

Nula Frei, Kommentierung zu Art. 67 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Frei, N. XXX zu Art. 67 DSG.

Chapitre 9 Conclusion de traités internationaux

Art. 67

Le Conseil fédéral peut conclure des traités internationaux concernant:

a. la coopération internationale entre autorités chargées de la protection des données;

b. la reconnaissance réciproque d'un niveau de protection adéquat pour la communication de données personnelles à l'étranger.

TABLE DES MATIÈRES

En bref 857
I. Généralités 857
A. But de l'art. 67 LPD 857
B. Historique 858
II. Compétence du Conseil fédéral pour conclure des traités internationaux 859
A. Coopération internationale entre autorités de protection des données (let. a) . 862
1. Coopération 862
2. Autorités de protection des données 864
B. Reconnaissance mutuelle d'un niveau de protection adéquat (lit. b) 865
C. Traités internationaux à d'autres fins 867
Bibliographie 868
Matériaux 870

EN BREF

Compte tenu des flux de données de plus en plus internationaux, une protection des données efficace doit également régler les questions transfrontalières. Pour ce faire, des accords avec d'autres Etats ou organisations internationales peuvent être nécessaires. Afin de faciliter la conclusion de tels accords, l'art. 67 LPD autorise le Conseil fédéral à conclure des accords internationaux sans l'approbation du Parlement dans deux domaines spécifiques, à savoir la coopération entre les autorités de protection des données et la reconnaissance mutuelle d'un niveau de protection adéquat. La norme de délégation doit être interprétée de manière stricte.

I. GÉNÉRALITÉS

A. But de l'art. 67 LPD

A l'ère de la mise en réseau électronique ubiquitaire, le traitement transfrontalier de données personnelles est devenu monnaie courante. C'est pourquoi la protection des données a depuis longtemps une dimension internationale et est donc devenue un objet de la politique étrangère. 1

La Suisse a conclu de nombreux accords bilatéraux et multilatéraux dans le domaine de la protection des données. On peut distinguer entre les accords généraux, qui normalisent ou constitutionnalisent la protection des données pour l'ensemble des domaines juridiques, et les accords sectoriels, qui établissent des règles pour certains domaines de coopération. Actuellement, seule la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108), dont la Suisse ratifiera prochainement la version modernisée (STE 108+), appartient à la première catégorie. Des règles de protection des données spécifiques à certains domaines se trouvent dans de nombreux accords dans le domaine de la coopération policière et de l'entraide judiciaire en matière pénale, de la délivrance de visas, de la gestion des migrations et de la réadmission des ressortissants étrangers, de la coopération en matière d'asile et de l'échange de données relatives aux passagers aériens. 2

L'Union européenne est un acteur important en matière de protection des données. Sa législation en matière de protection des données influence 3

considérablement le droit suisse. Outre les influences indirectes et l'effet extraterritorial du règlement général sur la protection des données (RGPD), qui ne sont pas approfondis ici, il existe également plusieurs accords entre la Suisse et l'UE ayant un contenu en matière de protection des données. L'association à Schengen, dans le cadre de laquelle la Suisse reprend certains actes juridiques de l'UE, notamment la directive 2016/680 sur la protection des données dans les domaines de la police et de la justice, qui doit être mise en œuvre par la Confédération et les cantons, est d'une importance pratique majeure.

4 Par rapport à la réglementation générale relative à la conclusion de traités internationaux en Suisse (infra n. 10 ss), l'art. 67 LPD facilite la conclusion de traités internationaux en conférant au Conseil fédéral la compétence de conclure des traités de manière autonome, sans l'approbation de l'Assemblée fédérale, dans deux domaines spécifiques, à savoir à des fins de coopération entre autorités de protection des données et de reconnaissance mutuelle d'un niveau adéquat de protection des données.

B. Historique

5 L'art. 67 LPD remplace l'art. 36, al. 5, aLPD, qui était considéré comme trop vague au regard des principes en vigueur en matière de délégation de compétences, notamment l'interdiction des délégations en blanc. L'art. 36, al. 5, aLPD prévoyait que le Conseil fédéral pouvait conclure des traités internationaux sur la protection des données s'ils étaient conformes aux principes de la LPD.

6 Les autres alinéas de l'art. 36 aLPD, qui autorisaient le Conseil fédéral à édicter des dispositions d'exécution aussi bien générales que relatives à des domaines spécifiques, ne sont pas reconduits dans la nouvelle LPD.

7 L'art. 67 LPD n'a pas été contesté lors du processus législatif. La suggestion émise lors de la procédure de consultation de limiter la compétence du Conseil fédéral de conclure des traités en ce sens qu'il ne peut pas conclure de traités internationaux sur l'exécution en Suisse de sanctions prononcées par des autorités de surveillance étrangères n'a été entendue ni dans le message ni lors des débats parlementaires. Par rapport à l'avant-projet et au projet du Conseil fédéral, l'art. 67 n'a pas été modifié lors des débats

parlementaires (à l'exception de la numérotation) et n'a pas non plus été discuté, comme le montrent les procès-verbaux du Conseil.

II. COMPÉTENCE DU CONSEIL FÉDÉRAL POUR CONCLURE DES TRAITÉS INTERNATIONAUX

Un traité international est un accord conclu par écrit entre deux ou plusieurs sujets de droit international public au sens de l'art. 38, al. 1, let. a du Statut de la CIJ et de l'art. 2, al. 1, let. a de la Convention de Vienne sur le droit des traités. 8

Alors que l'art. 67 LPD utilise le terme "traité international", l'art. 16, al. 2, let. a LPD parle de "traité international". Malgré une terminologie différente, il s'agit de la même chose. 9

En Suisse, la conclusion de traités internationaux relève en principe de la compétence conjointe du Conseil fédéral et de l'Assemblée fédérale. Alors que le Conseil fédéral négocie et signe les traités internationaux dans le cadre de ses compétences en matière de politique extérieure (art. 184, al. 1 et 2, Cst.), le Parlement approuve les traités par arrêté fédéral (art. 166, al. 2, première phrase, Cst.) avant que le Conseil fédéral ne puisse les ratifier (art. 184, al. 2, Cst.). Cela s'explique par le fait que les traités internationaux, tout comme les lois fédérales, contiennent des dispositions fixant des règles de droit et nécessitent donc une légitimation démocratique au moins a posteriori. Dans certains cas, le référendum facultatif ou obligatoire sur les traités internationaux est prévu en plus de l'approbation du Parlement. Lorsqu'un traité international est soumis au référendum, qu'il concerne des intérêts essentiels des cantons ou qu'il a une grande portée politique, financière, économique, écologique, sociale ou culturelle, une consultation doit être organisée au préalable. 10

Le Parlement peut toutefois se décharger de cette compétence par le biais d'une délégation. De même, l'obligation d'approbation ne s'applique pas aux traités dont le Parlement a délégué la conclusion au Conseil fédéral par le biais d'une loi fédérale ou d'un traité international qu'il a approuvé. L'idée est de décharger l'Assemblée fédérale de l'approbation de traités "non dignes du Parlement" et de ne l'occuper que de questions qui nécessitent une légitimation démocratique renforcée. 11

12 Cette compétence autonome de conclure des traités est précisée à l'art. 7a LOGA, qui mentionne trois cas de figure dans lesquels le Conseil fédéral peut ratifier un traité sans l'approbation préalable du Parlement.

- Premièrement, sur la base d'une habilitation dans une loi fédérale spécifique (art. 7a, al. 1 LOGA). L'article 67 LPD constitue une telle habilitation. Des principes parallèles à ceux qui régissent les délégations législatives au Conseil fédéral sont déterminants à cet égard : les principales appréciations politico-juridiques doivent être formulées avec suffisamment de précision dans la loi parlementaire. Les "délégations en blanc" ne sont pas compatibles avec le principe de légalité, car elles pourraient avoir pour effet de soustraire à l'exigence d'approbation un nombre imprévisible de traités internationaux de contenus différents.
- Deuxièmement, une habilitation dans un traité international approuvé par l'Assemblée fédérale (art. 7a, al. 1, LOGA). Dans ce cas, les principes de délégation sont pour l'essentiel parallèles à ceux qui s'appliquent aux délégations de compétences dans une loi fédérale.
- Troisièmement, le Conseil fédéral peut ratifier des traités dits de portée mineure sans approbation parlementaire préalable (art. 7a, al. 2, LOGA). Il s'agit d'une clause générale subsidiaire, car elle s'applique à tous les traités de portée mineure, quel que soit le domaine concerné. Selon l'art. 7a, al. 3, LOGA, sont notamment considérés comme des traités de portée limitée les traités qui ne créent pas de nouvelles obligations ou n'entraînent pas de renonciation à des droits existants (art. 7a, al. 3, let. a, LOGA), les traités qui servent uniquement à l'exécution de traités approuvés par l'Assemblée fédérale et qui ne font que préciser les droits, les obligations ou les principes d'organisation déjà fixés dans le traité de base (let. b) ainsi que les traités qui s'adressent aux autorités et règlent des questions administratives et techniques (let. c). Cette liste est exemplative : c'est par interprétation qu'il faut déterminer si un contrat a effectivement une portée limitée. La loi précise également quels sont les traités qui ne sont en principe pas considérés comme ayant une portée limitée (art. 7a, al. 4, LOGA). C'est notamment le cas lorsque le traité est soumis au référendum facultatif en matière de traités internationaux selon l'art. 141, al. 1, let. d, Cst. (let. a), qu'il contient des dispositions qui relèvent de compétences cantonales (let. b) ou qu'il entraîne des dépenses élevées (let. c). Les autres critères sont de savoir si un traité porte atteinte aux intérêts juridiquement protégés de

particuliers, s'il nécessite une modification de la loi ou s'il s'intègre "sans problème" dans le contexte général de la politique intérieure et extérieure et de l'économie.

D'un point de vue purement quantitatif, la grande majorité (plus de 90%) des traités conclus par la Suisse sont conclus par le Conseil fédéral de manière autonome. Le Conseil fédéral présente chaque année à l'Assemblée fédérale un rapport sur les traités qu'il a conclus de manière autonome (art. 48a, al. 2, LOGA). Sous cette forme, un contrôle parlementaire a lieu a posteriori. 13

Le Conseil fédéral peut également déléguer à un département la compétence de conclure des traités internationaux. S'il s'agit d'un traité de portée mineure au sens de l'art. 7a, al. 2, LOGA, il peut en outre déléguer cette compétence à un groupe ou à un office fédéral (art. 48a, al. 1, LOGA). 14

La réglementation précédente, l'art. 36, al. 5 aLPD, stipulait que le Conseil fédéral pouvait conclure de manière autonome des traités internationaux "pour autant qu'ils soient conformes aux principes de la loi". La doctrine a interprété cette disposition comme signifiant que les traités internationaux devaient respecter les principes généraux de la protection des données, à savoir les principes de la légalité, de la bonne foi, de la reconnaissabilité, de la proportionnalité, de la finalité, de l'exactitude des données, de la sécurité des données, du respect des droits des personnes concernées et de l'interdiction de communiquer des données à l'étranger en cas de risque d'atteinte grave à la personnalité. Bien que cette exigence n'ait pas été reprise dans la nouvelle disposition, elle continue de découler, pour l'art. 67 LPD, de la nature de la délégation et, en fin de compte, du principe de la séparation des pouvoirs : en l'absence d'une réglementation expresse, le Conseil fédéral n'est pas habilité à conclure des contrats contraires aux règles générales de la loi sans l'approbation du Parlement. Comme les principes de protection des données découlent directement de la Constitution (art. 5, 13, 36 Cst.) et des prescriptions de droit international de la Convention sur la protection des données (art. 5 STE 108+), même une approbation parlementaire ne changerait rien au fait que les traités internationaux contraires aux principes de protection des données ne peuvent en principe pas être conclus. 15

A. Coopération internationale entre autorités de protection des données (let. a)

16 Selon l'article 67, lettre a LPD, le Conseil fédéral peut conclure des traités internationaux qui règlent la collaboration internationale entre les autorités de protection des données. Des questions de délimitation se posent en ce qui concerne la notion de "coopération" (a) ainsi que le cercle des autorités concernées (b).

1. Coopération

17 Le caractère de plus en plus transfrontalier des traitements de données rend la coopération internationale entre les autorités de protection des données indispensable. La coopération est donc l'un des piliers de la Convention STE 108+ modernisée du Conseil de l'Europe, qui oblige les États contractants, dans son chapitre V, à coopérer et à s'entraider (cf. art. 16, par. 1, STE 108+). De même, dans son droit modernisé de la protection des données, l'Union européenne accorde une grande importance à la coopération institutionnalisée entre les autorités nationales de protection des données (cf. art. 60 ss. RGPD ainsi que les art. 50 ss. de la directive sur la protection des données, contraignants pour la Suisse dans le domaine de la police et de la poursuite pénale. RL 2016/680).

18 La coopération entre les autorités de protection des données peut prendre différentes formes. L'article 17 de la Convention STE 108+ cite à titre d'exemple les formes de coopération suivantes : L'assistance mutuelle, notamment sous forme d'échange d'informations, la coordination d'enquêtes ou d'interventions ou la mise en œuvre de mesures communes, ainsi que la mise à disposition réciproque d'informations et de documents sur le droit national et la pratique administrative.

19 La Convention STE 108+ oblige les Parties à créer un réseau d'autorités de contrôle pour organiser leur coopération (art. 17, par. 3). D'autres détails de la coopération, notamment en ce qui concerne les formes et les procédures ainsi que les langues à utiliser, doivent être fixés directement entre les Parties concernées (art. 21, par. 3). La conclusion d'accords internationaux est nécessaire pour régler ces questions. L'art. 67 let. a LPD permet au Conseil fédéral de conclure de tels traités de manière simplifiée et met ainsi

également en œuvre cette obligation conformément à la Convention STE 108+.

Au niveau national, la collaboration avec les autorités étrangères compétentes en matière de protection des données fait partie des tâches du PFPDT définies par la loi (à art. 58 al. 1 let. b LPD). Dans la pratique, le PFPDT coopère notamment avec certaines autorités nationales et supranationales de protection des données, en particulier avec les autorités de protection des données des Etats membres de Schengen ainsi qu'avec le Comité européen de la protection des données (CEPD). Il s'engage également dans des instances internationales telles que le Conseil de l'Europe, la Conférence européenne et la Conférence internationale des commissaires à la protection des données, l'Association francophone des autorités de protection des données ainsi que l'OCDE. 20

Le PFPDT a également la compétence d'accorder l'entraide administrative aux autorités étrangères de protection des données, pour autant que les conditions de l'art. 55 LPD soient remplies. Dans ce cas également, un traité international peut être nécessaire, que le Conseil fédéral peut conclure plus facilement conformément à l'art. 67, let. a. 21

Par rapport aux compétences légales du PFPDT mentionnées ci-dessus, l'art. 67, let. a, LPD constitue la base légale pour le cas où la coopération internationale va au-delà d'une coopération purement informelle (p. ex. l'échange de bonnes pratiques) et doit donc être fondée sur une base formelle. La conclusion d'un traité international est notamment nécessaire lorsque des droits et des obligations réciproques doivent être établis durablement et lorsque des données personnelles ou des données protégées d'une autre manière (par exemple des secrets d'affaires) doivent être échangées avec d'autres États. Pour la transmission de données personnelles, les conditions de l'article 16 LPD doivent en outre être respectées. 22

A ce jour, aucun accord de coopération de ce type n'a été conclu dans le domaine de la protection des données. Le message cite d'ailleurs comme modèle d'accord de coopération un accord conclu dans un autre domaine juridique, à savoir l'accord du 17 mai 2013 entre la Confédération suisse et l'Union européenne concernant la coopération dans l'application de leur droit de la concurrence. Le contenu de cet accord donne un aperçu du contenu possible de futurs accords de coopération dans le domaine de la protection 23

des données : les parties s'y engagent par exemple à ce que leurs autorités de la concurrence s'informent mutuellement des mesures d'exécution qui, selon elles, pourraient affecter des intérêts importants de l'autre partie (art. 3), à ce qu'elles coordonnent les mesures d'exécution concernant des opérations liées entre elles (art. 4) ou à ce qu'elles puissent se demander mutuellement d'engager des mesures d'exécution (art. 6).

24 En outre, les accords qui délimitent les compétences des différentes autorités de protection des données relèvent du champ d'application de l'article 67, lettre a LPD. Un tel accord aurait une pertinence pratique en ce qui concerne la délimitation des compétences entre les autorités suisses et européennes de protection des données, car le RGPD s'applique certes aussi aux responsables du traitement ou aux sous-traitants non établis dans l'UE, ce qui signifie que les compétences des autorités de surveillance des États membres de l'UE s'étendent aux responsables du traitement en Suisse, mais que ces derniers ne peuvent pas prendre de mesures d'exécution en Suisse. Une motion parlementaire demandant la conclusion d'un accord de coordination correspondant avec l'UE a déjà été adoptée par les Chambres en 2017, mais n'a pas encore été mise en œuvre, sans doute principalement parce qu'aucun nouvel accord ne peut être conclu actuellement avant que les questions institutionnelles avec l'UE ne soient clarifiées. En tout état de cause, le Conseil fédéral pourrait conclure un accord de coordination correspondant sur la base de l'article 67 LPD sans l'approbation du Parlement.

2. Autorités de protection des données

25 L'autorisation de conclure plus facilement des accords de coopération internationale selon l'art. 67 LPD se réfère exclusivement à la coopération entre "autorités de protection des données". Tant la Convention STE 108 (art. 1 du Protocole additionnel de 2001, resp. art. 12bis STE 108+) que la directive européenne 2016/180 (art. 41 de la directive 2016/680), contraignante pour la Suisse, obligent les Etats parties à mettre en place une ou plusieurs autorités de surveillance de la protection des données indépendantes.

26 Inversement, cela signifie que la base d'habilitation de l'art. 67 let. a LPD ne s'étend pas aux contrats de coopération entre d'autres autorités en matière de protection des données, par exemple l'échange de données personnelles entre les autorités judiciaires, policières ou migratoires. De tels contrats doivent

être approuvés par le Parlement, à moins qu'une autre loi fédérale ne l'autorise.

La compétence de conclure l'accord de coopération est réservée au Conseil fédéral. Selon le libellé de la loi, le PFPDT, même s'il est la personne directement concernée par de tels contrats, n'a pas la compétence de les conclure de manière autonome. Le Conseil fédéral aurait certes la possibilité de subdéléguer au PFPDT sa compétence de conclure seul des traités internationaux (cf. art. 48a, al. 1, LOGA et n. 14 ci-dessus), mais il ne l'a pas fait jusqu'à présent. Dans cette mesure, le PFPDT est tributaire, pour son activité, de la conclusion de tels contrats par le Conseil fédéral, ce qui est dans un certain rapport de tension avec son indépendance institutionnelle (à l'art. 43, al. 4, LPD). 27

B. Reconnaissance mutuelle d'un niveau de protection adéquat (lit. b)

Le deuxième objectif pour lequel le Conseil fédéral peut conclure des accords internationaux sans l'approbation préalable du Parlement est la reconnaissance mutuelle d'un niveau de protection adéquat selon l'art. 67 let. b LPD. 28

Cette disposition doit être comprise en relation avec l'art. 16 LPD, qui règle les conditions de communication de données personnelles à l'étranger. L'une de ces possibilités est l'existence d'un traité international : selon l'art. 16, al. 2, let. a, une communication à l'étranger est possible lorsqu'un traité international garantit une protection des données appropriée. 29

La convention modernisée sur la protection des données du Conseil de l'Europe reconnaît également la possibilité de garantir l'existence d'un niveau de protection adéquat dans un Etat tiers au moyen d'un accord international (cf. art. 12 al. 3 let. b STE 108+). De même, le droit de l'UE prévoit des dispositions correspondantes (cf. art. 46, al. 2, let. a, RGPD et art. 37, al. 2, let. a, de la directive 2016/680, contraignante pour la Suisse). 30

Un traité international au sens de l'art. 16 al. 2 let. a LPD peut être une convention générale sur la protection des données, comme la convention STE 108+, ou tout autre accord sectoriel dans un domaine particulier qui régit la transmission de données personnelles entre les parties contractantes. Il convient de noter qu'un traité international n'est couvert par l'habilitation de 31

l'art. 67, let. b LPD que s'il est limité au but de la reconnaissance mutuelle d'un niveau de protection adéquat ; s'il va au-delà, le Conseil fédéral ne peut pas conclure le traité de manière autonome ou a besoin d'une autre base d'habilitation.

32 La possibilité de reconnaître un niveau de protection adéquat par le biais d'un traité international est pertinente lorsque la législation de l'État ou de l'organe international concerné n'offre pas une protection adéquate au sens de l'art. 16, al. 1, LPD et qu'il n'existe donc pas de décision de constatation correspondante du Conseil fédéral. Par le biais d'un accord, les Etats concernés peuvent convenir d'un système de protection des données conforme au traité international, qui compense les lacunes du système juridique national, de sorte que la reconnaissance mutuelle d'un niveau de protection adéquat soit possible.

33 L'exemple le plus important est celui des accords conclus avec les Etats-Unis, dont le niveau de protection des données n'est pas considéré comme adéquat au sens de l'art. 16, al. 1, LPD, notamment en raison des droits d'accès étendus du président américain et des services secrets nationaux aux données détenues par des entreprises américaines et des possibilités de protection juridique limitées pour les ressortissants non américains. Les accords conclus avec les Etats-Unis illustrent cependant aussi les limites de l'accord international sur les normes de protection des données, notamment la difficulté politique réelle de modifier la répartition des compétences au niveau national au moyen du droit international : Suite à l'arrêt Schrems, le PFPDT n'a plus reconnu comme base pour les transferts de données vers les Etats-Unis le cadre U.S.-Swiss Safe Harbor, qui était encore cité comme exemple dans le rapport explicatif relatif à l'avant-projet de LPD (mais plus dans le message) et qui était calqué sur le cadre UE-USA Safe Harbor, lequel a dû être remplacé suite à l'arrêt de la CJCE dans l'affaire Schrems. Le Privacy Shield UE-US qui a suivi a également été jugé insuffisant par la CJCE dans l'affaire Schrems II. Le Swiss-US Privacy Shield est certes toujours formellement en vigueur, mais il est également jugé insuffisant par le PFPDT. L'UE et les États-Unis ont annoncé en mars 2022 qu'ils s'étaient mis d'accord sur un cadre transatlantique de protection des données ; la Suisse devrait toutefois encore s'entendre avec les États-Unis sur un accord parallèle. Il reste à voir si le cadre transatlantique de protection des données permettra de surmonter les difficultés politiques réelles mentionnées.

La reconnaissance mutuelle d'un niveau adéquat de protection des données est également possible dans le cadre d'accords sectoriels. Ainsi, dans le cadre de conventions de double imposition conclues avec des pays ne disposant pas d'une protection suffisante des données, les parties contractantes peuvent constater que la protection des données est considérée comme suffisante dans le cadre de l'octroi de l'assistance administrative en matière fiscale, du moins en ce qui concerne les données pertinentes sur le plan fiscal, sur la base des assurances données dans les conventions internationales. Il en va de même pour la transmission de données personnelles dans le cadre de la coopération entre les autorités policières, douanières, de poursuite pénale ou de migration, domaines dans lesquels la Suisse a conclu de nombreux accords. Comme nous l'avons déjà mentionné, la base d'habilitation de l'article 67, lettre b LPD est limitée à la question de la reconnaissance mutuelle d'un niveau de protection équivalent. Les accords de coopération qui, dans la pratique, règlent généralement d'autres questions allant au-delà, nécessitent par conséquent - à moins qu'une autre loi fédérale ne prévoie une base d'habilitation - une approbation préalable par le Parlement. 34

C. Traités internationaux à d'autres fins

La base d'habilitation de l'article 67 LPD est limitée aux deux finalités des lettres a et b. La norme de délégation doit être interprétée de manière stricte. 35

Le Conseil fédéral peut également conclure des traités internationaux à d'autres fins dans le domaine de la protection des données, mais la compétence n'est alors pas déterminée par cet article, mais par les dispositions générales (voir ci-dessus N. 10 ss). En d'autres termes, s'il s'agit d'un traité de portée limitée ou s'il existe une norme d'habilitation dans une autre loi fédérale que la LPD, le Conseil fédéral peut également le ratifier sans l'approbation du Parlement. Dans tous les autres cas, une approbation parlementaire est nécessaire avant la ratification. 36

Les traités qui ont pour objet la transmission de données personnelles à des autorités étrangères ne sont pas, à mon avis, de portée limitée, car ils portent atteinte aux intérêts juridiquement protégés de personnes privées. Il s'agit notamment des nombreux accords de coopération dans les domaines de la police, de la justice, de l'entraide judiciaire, de la migration et de la fiscalité que la Suisse a conclus avec d'autres Etats et qui contiennent des dispositions relatives à l'échange de données. En font également partie les accords 37

internationaux ou les échanges de notes sur la mise en œuvre du développement de l'acquis de Schengen (dans la mesure où ils règlent plus que de simples détails techniques) ainsi que les accords avec d'autres États sur l'accès aux données des passagers aériens (passenger name records, PNR). Comme l'art. 67 ne prévoit pas d'autorisation pour de tels accords, une délégation dans une loi fédérale sectorielle ou une approbation parlementaire est toujours nécessaire. C'est donc à juste titre que le Conseil fédéral a demandé l'approbation préalable de l'Assemblée fédérale avant de ratifier la convention STE 108+ et de reprendre la directive 2016/680. Les deux actes juridiques sont des instruments de grande portée au sens de l'énumération exemplative de l'art. 7a, al. 4, LOGA.

38 Il convient de noter que la base d'habilitation de l'art. 67 LPD autorise le Conseil fédéral à conclure des contrats de portée limitée ou plus large dans le cadre des objectifs mentionnés. L'opinion juridique exprimée dans la doctrine à propos de l'ancienne norme de délégation de l'art. 36, al. 5, aLPD, selon laquelle celle-ci ne comprendrait que des contrats de portée limitée, méconnaît à mon avis le rapport entre les différentes bases d'habilitation de l'art. 7a LOGA. Une délégation sectorielle dans une loi fédérale constitue une lex specialis et permet a fortiori de conclure aussi bien des traités de portée limitée que des traités de portée plus large.

39 C'est le Conseil fédéral qui décide s'il y a un traité de portée limitée ou s'il relève de la délégation de l'art. 67, let. a et b. Afin de contrôler que celui-ci n'outrepasse pas ses compétences, l'art. 48a, al. 2, LOGA oblige le Conseil fédéral à présenter chaque année à l'Assemblée fédérale un rapport sur les traités conclus, modifiés ou résiliés par lui-même, par les départements, par les groupements ou par les offices. Si l'Assemblée fédérale n'est pas d'accord avec la répartition effectuée par le Conseil fédéral, elle peut demander par voie de motion que le Conseil fédéral soumette le contrat à une approbation ultérieure.

BIBLIOGRAPHIE

Cattaneo Gianni, Kommentierung zu Art. 67 DSG, in: Métille Sylvain/Meier Philippe (Hrsg,), Loi sur la protection des données LPD.

Dauag Apollo, Kommentierung zu Art. 67 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2022.

EDÖB, 29. Tätigkeitsbericht 2021/22, Bern 2022, abrufbar unter https://www.edoeb.admin.ch/edoeb/de/home/deredoeb/taetigkeitsberichte.html , besucht am 11.4.2023 (zit. 29. Tätigkeitsbericht).

EDÖB, Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau, 8.9.2020, abrufbar unter https://www.edoeb.admin.ch/edoeb/de/home/kurzmeldungen/nsb_mm.msg-id-80318.html , besucht am 13.4.2023 (zit. Datenübermittlung).

Epiney Astrid, Kommentierung zu Art. 166 BV, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar, Bundesverfassung, Basel 2015.

Epiney Astrid/Frei Nula, Die völker- und europarechtliche Einbettung des DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar Datenschutzgesetz, Zürich 2023, S. 33-57 (zit. DSG).

Epiney Astrid/Frei Nula, Zur Übernahme weiterentwickelten EU-Rechts durch den Bundesrat. Selbständige Vertragsschlusskompetenzen im Rahmen der Bilateralen Abkommen, am Beispiel der Liberalisierung des internationalen Schienenpersonenverkehrs, in: Jusletter 12.8.2019 (zit. Vertragsschlusskompetenzen).

Fey Marco, Kommentierung zu Art. 67 aDSG, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, Bern 2015.

Fischer Philipp, Kommentierung zu Art. 16 DSG, in: Métille Sylvain/Meier Philippe (Hrsg,), Loi sur la protection des données LPD.

Frei Nula, Die Revision des Datenschutzgesetzes aus europarechtlicher Sicht, in: Jusletter 17.9.2018 (zit. Revision DSG).

Frei Nula, Die Datenschutz-Grundverordnung und die Schweiz, in: Epiney Astrid/Rovelli Sophia (Hrsg.), Datenschutz und Gesundheitsrecht, Zürich 2019 (zit. DSGVO).

Jauslin Carl/Spenlé Christoph, Kommentierung zu Art. 67 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar Datenschutzgesetz, Zürich 2023.

Kerboas Cécile/Lennman Catherine, Kommentierung zu Art. 55 DSG, in: Métille Sylvain/Meier Philippe (Hrsg,), Loi sur la protection des données LPD.

Kunz Christian, Kommentierung zu Art. 16 DSG, in: Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar Datenschutzgesetz, Zürich 2023.

Métille Sylvain/Ackermann Annelise, RGPD : application territoriale et extraterritoriale, in: Epiney Astrid/Rovelli Sophia (Hrsg.), Datenschutzgrundverordnung (DSGVO): Tragweite und erste Erfahrungen, Zürich 2020.

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008.

Rudin Beat/Husi-Stämpfli Sandra, Kommentierung zu Art. 36 DSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014.

Schmid Evelyne, Kommentierung zu Art. 166 BV, in: Martenet Vincent/Dubey Jacques (Hrsg.), Commentaire romand Constitution fédérale, Basel 2021.

Thürer Daniel, Kommentierung zu Art. 166 BV, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J./Vallender Klaus A. (Hrsg.), Bundesverfassung St. Galler Kommentar, 4. Aufl., Zürich 2023.

Tschannen Pierre, Staatsrecht der Schweizerischen Eidgenossenschaft, 4. Aufl., Bern 2016.

MATÉRIAUX

Botschaft zum Bundesgesetz über die Kompetenz zum Abschluss völkerrechtlicher Verträge von beschränkter Tragweite und über die vorläufige Anwendung völkerrechtlicher Verträge (Änderung des Regierungs- und Verwaltungsorganisationsgesetzes und des Parlamentsgesetzes) vom 4.7.2012, BBl 2012 7465 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2012/1138/de, besucht am 11.4.2023 (zit. Botschaft RVOG und ParlG).

Vorentwurf zum Bundesgesetz über den Datenschutz vom 21.12.2016, abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vorentw-d.pdf.download.pdf/vorentw-d.pdf, besucht am 11.4.2023 (zit. VE-DSG).

Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21.12.2016, abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf.download.pdf/vn-ber-d.pdf, besucht am 11.4.2023 (zit. Erläuternder Bericht DSG).

Bundesamt für Justiz, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 10.8.2017, abrufbar unter https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/ve-ber-d.pdf.download.pdf/ve-ber-d.pdf, besucht am 11.4.2023 (zit. Vernehmlassungsergebnisse DSG).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 13.4.2023 (zit. Botschaft DSG).

Entwurf zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 7193 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2058/de, besucht am 11.4.2023 (zit. E-DSG).

Botschaft zur Genehmigung des Protokolls vom 10.10.2018 zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 6.12.2019, BBl 2020 565 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2020/60/de, besucht am 13.4.2023 (zit. Botschaft SEV 108+).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 69 LPD

Un commentaire de Rehana C. Harasgama / Dario Haux

PROPOSITION DE CITATION

Rehana C. Harasgama/Dario Haux, Kommentierung zu Art. 69 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Harasgama/Haux, N. XXX zu Art. 69 DSG.

Art. 69 Disposition transitoire concernant les traitements en cours

Les art. 7, 22 et 23 ne sont pas applicables aux traitements qui ont débuté avant l'entrée en vigueur de la présente loi, pour autant que les finalités du traitement restent inchangées et que de nouvelles données ne soient pas collectées.

TABLE DES MATIÈRES

En bref 875
I. Généralités 875
A. Aperçu 875
B. Historique 875
C. Objectif de la norme 876
II. Contenu 876
A. Conditions 876
B. Défis à relever 879
Bibliographie 880
Matériaux 880

EN BREF

La LPD totalement révisée entrera en vigueur le 1er septembre 2023 sans période de transition générale. L'article 69 stipule toutefois que certains articles sélectionnés ne sont pas applicables à certains traitements de données. La norme stipule toutefois que cela ne s'applique que si ces traitements de données ont commencé avant l'entrée en vigueur de la LPD totalement révisée et si, après cette entrée en vigueur, ni la finalité du traitement ni de nouvelles données n'ont été collectées. En ce sens, l'article exclut les mesures préventives des articles 7, 22 et 23 dans certains cas. Le législateur a voulu éviter de cette manière que les responsables puissent être mis en cause ultérieurement et qu'il en résulte des efforts et des coûts supplémentaires.

I. GÉNÉRALITÉS

A. Aperçu

La LPD totalement révisée ne prévoit pas de délais transitoires dont les responsables ou autres personnes concernées devraient tenir compte. Dans ce sens, elle sera en principe applicable à partir du 1er septembre 2023. Le chapitre 10, consacré aux dispositions finales, contient toutefois quelques dispositions transitoires pertinentes. Elles sont concrètement contenues dans les articles 69 à 72. Le présent article 69 prévoit spécifiquement que les articles 7, 22 et 23 ne sont pas applicables aux traitements de données dans certains cas. Il s'agit des traitements qui ont commencé avant l'entrée en vigueur de la LPD révisée le 1er septembre 2023 et dont la finalité du traitement n'a pas été modifiée après l'entrée en vigueur, ni de nouvelles données ajoutées au processus de traitement des données. 1

B. Historique

Dès l'entrée en vigueur de la LPD totalement révisée le 1er septembre 2023, les normes s'appliqueront dans toute la Suisse et seront donc applicables dans la mesure où les art. 2 et 3 al. 1 sont remplis. Comme c'est généralement le cas dans d'autres lois, il existe toutefois des exceptions à ce principe ou du moins des dispositions transitoires visant à simplifier la transition entre l'ancien et le 2

nouveau catalogue de normes. Cette dernière était prévue dans un article 64 de la P-LPD. Celui-ci prévoyait trois exceptions, à savoir un effet rétroactif du droit d'accès des personnes concernées pour les traitements de données déjà achevés (al. 1), un délai transitoire pour l'adaptation des traitements de données en cours (al. 2) et la non-applicabilité de certaines dispositions pour les traitements de données qui se poursuivent sans changement (al. 3). L'al. 4 établit le principe de l'application des dispositions dès leur entrée en vigueur. Finalement, tous les al. ont été supprimés, à l'exception de l'al. 3, qui se retrouve dans le présent article 69.

C. Objectif de la norme

3 L'art. 69 garantit qu'en présence de conditions spécifiques, une application rétroactive des art. 7, 22 et 23 est empêchée. Le législateur facilite ainsi la transition entre la LPD préexistante et la LPD totalement révisée et épargne aux responsables de traitement des efforts et des coûts supplémentaires. En outre, l'art. garantit que les responsables ne se voient pas imposer des obligations a posteriori. Un effet rétroactif de la loi, problématique dans certains cas, est ainsi évité. En même temps, l'importance de cet article est limitée, d'autant plus que la LPD ne prévoit en général pas de délais de transition pertinents.

II. CONTENU

A. Conditions

4 Sur le plan du contenu, l'art. 69 se réfère aux art. 7, 22 et 23. Alors que l'art. 7 consacre les principes du privacy by design (protection des données par la technique) et du privacy by default (paramétrage par défaut du droit de la protection des données) (voir à ce sujet le CO-Claus relatif à l'art. 7 LPD), les art. 22 et 23 se réfèrent à l'analyse d'impact relative à la protection des données (AIPD) (voir à ce sujet le CO-Harasgama/Haux relatif à l'art. 22 LPD). L'art. 22 fixe les bases de la réalisation de l'AIPD et 23 certaines conditions de consultation du PFPDT, dans la mesure où il est reconnu, dans le cadre d'une AIPD, qu'il existe un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, malgré les mesures prises pour réduire les risques.

Ces obligations doivent en principe être prises en compte avant le traitement respectif des données et ne doivent pas être imposées rétroactivement au responsable du traitement par le biais de cette disposition transitoire. Au sens de ce principe de non-rétroactivité, la norme présuppose que le traitement des données a commencé avant son entrée en vigueur. Il doit donc avoir commencé avant le 1er septembre 2023 et ne doit être ni planifié (au sens de l'art. 7 al. 1 LPD) ni déjà terminé. Alors que la délimitation entre la simple planification et l'exécution effective d'un traitement de données peut être déterminée au cas par cas, la question se pose de savoir comment distinguer l'exécution de la fin du traitement des données. Il faut tenir compte du fait qu'une fin ne peut être supposée qu'à partir du moment où l'objectif du traitement est atteint. La situation dans laquelle la finalité n'est de facto plus réalisable est assimilée. 5

La deuxième condition est que le but du traitement défini précédemment reste inchangé. Cela signifie que la finalité a été suffisamment déterminée et concrétisée au début du traitement des données et qu'elle subsiste sans changement au moment de l'entrée en vigueur de la LPD totalement révisée (voir le commentaire de l'art. 6 al. 3 LPD pour plus de détails sur la détermination de la finalité du traitement). Dans ce cadre, la question se pose de savoir ce qui s'applique dans la mesure où seules certaines finalités de traitement sont poursuivies, alors que d'autres sont abandonnées. Ce serait le cas si, par exemple, une base de données contenant des données de patients issues d'essais cliniques était initialement traitée pour d'autres essais cliniques dans le même domaine de recherche (finalité 1) et pour l'entraînement d'un outil de prévision basé sur l'intelligence artificielle (IA) (finalité 2) et si, après l'entrée en vigueur de la LPD totalement révisée, le traitement des données n'avait plus lieu que pour des essais cliniques, c'est-à-dire pour la finalité 1. Le fait qu'il n'y ait en tout cas pas d'extension des finalités du traitement plaide en faveur de l'hypothèse que cela est couvert par le libellé de l'article 69. Au contraire, les objectifs existants sont poursuivis - même si c'est sous une forme réduite. 6

Troisièmement, l'ensemble des données du traitement de données concerné doit rester inchangé. Selon le texte de la loi, "aucune nouvelle donnée ne doit avoir été collectée". Le processus de "collecte" est "un acte actif, ciblé et conscient de collecte des données personnelles concernées". C'est l'action ciblée et active qui est déterminante. L'obtention passive de données n'est en 7

revanche pas comprise. D'autres auteurs parviennent à une conclusion similaire en se basant sur le caractère planifié de l'opération.

8 Il n'est toutefois pas clair comment interpréter le passage "pas de nouvelles données". Une interprétation étroite aurait pour conséquence que la disposition transitoire ne s'appliquerait pas à un processus de traitement de données constant avec des catégories de données fixes, dans la mesure où des données (points) supplémentaires concernant d'autres personnes sont collectées alors que les catégories de données restent inchangées. Cela serait indépendant de l'impact de ces données (points) supplémentaires sur le processus ou le but du traitement. Cette estimation pourrait se justifier par le fait que le stock de données ou le volume des données existantes serait modifié ou augmenté. Prenons l'exemple d'un outil RH basé sur l'IA d'une entreprise qui traiterait des données (points) supplémentaires de nouveaux candidats ou collaborateurs après le 1er septembre 2023. Le stock de données ou l'étendue de ce stock serait donc modifié ou augmenté, de sorte que si les autres conditions de l'article 69 étaient remplies, une nouvelle analyse d'impact sur la protection des données devrait être effectuée selon cette interprétation étroite. Alors que le message suggère une telle interprétation, une interprétation aussi étroite ne correspond pas au sens et au but de la disposition. Dans les faits, cela signifierait que tous les processus de traitement de données continus pour lesquels il est possible que des données concernant des personnes supplémentaires soient collectées après le 1er septembre 2023 ne seraient pas couverts par la disposition. Le champ d'application de l'article 69 serait donc réduit de manière négligeable. Cette interprétation restrictive n'est pas suivie dans le cas présent. Dans ce contexte, deux variantes d'interprétation sont possibles : (1) l'art. 69 ne s'applique que si de nouvelles catégories de données sont collectées, mais pas en cas de simple modification ou extension de l'étendue des catégories de données ou des points de données qui restent inchangés. Ce serait le cas, par exemple, si un formulaire en ligne mis à disposition pour un jeu-concours permettait, après le 1er septembre 2023, de ne plus collecter uniquement le nom, les coordonnées et la réponse à la question du jeu-concours, mais de demander des informations plus détaillées sur les intérêts et les hobbies. Ou encore : (2) l'article 69 n'est pas applicable à tout processus de traitement de données lorsque - selon le message interprété de manière restrictive - le stock ou le volume de données est en soi augmenté ou modifié, bien que les

catégories de données collectées restent inchangées et qu'une modification de la finalité du traitement ou du processus qui en résulte ne peut être exclue.

La question de savoir si des données déjà collectées au préalable, mais ajoutées ultérieurement, excluent l'applicabilité de l'article 69 LPD est également discutée. En se basant sur le texte, certains auteurs affirment que le traitement de ces données tombe sous le coup de l'exception, en tout cas dans la mesure où elles ont été collectées dans le même but. Toutefois, le fait que le contexte des traitements de données soit si profondément marqué par les innovations technologiques que l'exception de l'article 69 LPD ne devrait s'appliquer qu'à des conditions strictes et doit donc être interprétée de manière restrictive s'y oppose. Si de nouvelles données sont ajoutées à la base de données, cette dernière ne peut guère être qualifiée de "inchangée", c'est-à-dire de constante, si ces données ont déjà été collectées dans le cadre d'une autre finalité de traitement des données. Il n'est pas certain que cette question gagne en importance et en contours dans l'application pratique, d'autant plus que l'on peut supposer que la pertinence pratique de cette norme est plutôt faible. D'autant plus que le principe de l'article 7 découlait déjà en partie des articles 4 et 7 de l'aDSG avant son entrée en vigueur et que les responsables étaient en partie également tenus de le faire en vertu du RGPD. Il en va de même pour les articles 22 et 23 (voir à ce sujet le commentaire détaillé de Harasgama/Haux sur l'article 22 LPD). 9

B. Défis à relever

Avec l'entrée en vigueur de la LPD totalement révisée, les responsables de traitement sont confrontés à de nombreux défis. Bien que le libellé de l'article 69 LPD soit bref et risque de passer inaperçu, il convient de lui accorder l'attention nécessaire dans ce cadre. Alors que les traitements de données en cours avant l'entrée en vigueur et qui remplissent les autres conditions relèvent sans aucun doute de la réglementation d'exception, il faut toujours demander un conseil juridique pour les questions de détail et pour l'utilisation de nouvelles technologies dans les processus de traitement des données qui ont déjà été planifiés et/ou testés avant l'entrée en vigueur de la LPD totalement révisée. Il s'agit de déterminer avec précision si les données ou les finalités du traitement sont restées inchangées ou si des modifications ont été apportées ou doivent l'être. Si c'est le cas, il faut partir du principe, en cas de doute, que la norme n'est pas applicable. 10

BIBLIOGRAPHIE

Dauag Apollo, Kommentierung zu Art. 69 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Stämpflis Handkommentar zum DSG, 2. Aufl., Zürich/Basel, 2023.

Rosenthal David, Das neue Datenschutzgesetz, Jusletter, 16. November 2020.

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. HK-DSG).

MATÉRIAUX

Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 S. 6941 ff., abrufbar unter: https://fedlex.data.admin.ch/eli/fga/2017/2057, besucht am 5.6.2023.

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 72 LPD

Un commentaire de Danielle Schneider / Carl Jauslin

PROPOSITION DE CITATION

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 72 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Schneider/Jauslin, N. XXX zu Art. 72 DSG.

Art. 72 Disposition transitoire relative à l'élection et à la fin des rapports de travail du préposé

[1] L'ancien droit s'applique à l'élection et à la fin des rapports de travail du préposé jusqu'à la fin de la législature au cours de laquelle la présente loi entre en vigueur.

[2] Si, lors de la première élection du préposé par l'Assemblée fédérale (Chambres réunies), l'ancien titulaire du poste est élu, le nouveau mandat du préposé commence le jour suivant l'élection.

TABLE DES MATIÈRES

En bref 883
I. Généralités 883
II. Droit transitoire concernant l'élection et la fin du mandat (al. 1) 883
III. Droit transitoire concernant la réélection éventuelle du titulaire actuel du mandat (al. 2) 884
Matériaux 884

EN BREF

Le nouveau droit de la protection des données entrera en vigueur le 1er septembre 2023. Pour l'élection et la fin du mandat du préposé, l'ancien droit s'applique toutefois encore jusqu'à la fin de la 51e législature. Selon ce dernier, c'est l'Assemblée fédérale (Chambres réunies) qui est l'organe d'élection et qui est compétente pour les décisions patronales les plus importantes.

I. GÉNÉRALITÉS

La révision totale de la LPD modifie la procédure de nomination du préposé. Désormais, l'Assemblée fédérale (Chambres réunies) sera le seul organe de nomination et sera compétente pour les principales décisions de l'employeur. De cette manière, l'indépendance et la légitimité démocratique du préposé seront renforcées. Des dispositions transitoires sont donc nécessaires pour l'élection et la fin du mandat du préposé. 1

L'art. 72 al. 1 LPD a été introduit dans le cadre des débats parlementaires sur la révision totale de la LPD. Cette disposition n'était pas encore prévue dans le projet du Conseil fédéral, qui avait maintenu la procédure actuelle de nomination du préposé (nomination par le Conseil fédéral et approbation par l'Assemblée fédérale conformément à l'art. 26 al. 1 aLPD) ainsi que les compétences actuelles en matière de décisions de l'employeur (notamment l'art. 26a, al. 3, concernant la révocation du préposé par le Conseil fédéral). 2

L'art. 72 al. 2 LPD n'a été intégré dans la LPD totalement révisée qu'au cours des travaux relatifs à l'initiative parlementaire CIP-N 21.443. Cela a été nécessaire pour combler une lacune involontaire concernant l'éventuelle réélection du préposé actuel (cf. n. 6 s.). 3

II. DROIT TRANSITOIRE CONCERNANT L'ÉLECTION ET LA FIN DU MANDAT (AL. 1)

L'art. 72 al. 1 LPD prévoit que la nomination du préposé et la fin de son mandat sont régies par l'ancien droit jusqu'à la fin de la législature au cours de laquelle la LPD totalement révisée entre en vigueur. 4

5 Le Conseil fédéral a fixé l'entrée en vigueur du nouveau droit de la protection des données au 1er septembre 2023. Cela signifie que le préposé pourra être élu pour la première fois par l'Assemblée fédérale (Chambres réunies) à partir de la session d'hiver 2023. La Commission judiciaire a annoncé qu'elle prévoyait d'élire le préposé pour la prochaine période administrative lors de la session d'hiver 2023. Dans ce cas, la nouvelle durée de mandat du préposé commencerait en principe le 1er janvier 2024 (cf. art. 44 al. 1, 2e phrase LPD).

III. DROIT TRANSITOIRE CONCERNANT LA RÉÉLECTION ÉVENTUELLE DU TITULAIRE ACTUEL DU MANDAT (AL. 2)

6 Le préposé actuel a été confirmé par le Conseil fédéral le 10 avril 2019 pour une deuxième période administrative allant jusqu'à la fin de la 51e législature, le 4 décembre 2023. Il se porte candidat pour un troisième (et dernier) mandat. L'élection doit être effectuée par l'Assemblée fédérale (Chambres réunies) (art. 43 al. 1 LPD). En cas de réélection, un début de mandat au 1er janvier 2024 entraînerait une lacune non souhaitée (notamment du point de vue du droit du personnel). En effet, entre le 4 décembre 2023 et le 1er janvier 2024, le titulaire actuel du mandat n'aurait pas de rapport de travail en tant que préposé. Par conséquent, il n'aurait en principe pas non plus de droits ou d'obligations découlant de ce rapport de travail (notamment pas de droit au salaire).

7 Pour la première élection par l'Assemblée fédérale (Chambres réunies), l'art. 72 al. 2 LPD avance exceptionnellement le début du mandat au lendemain de l'élection. Cette disposition ne s'applique toutefois qu'en cas de réélection du titulaire actuel de la fonction. Certes, cette solution ne permet pas non plus d'assurer une transition sans heurts. Le préposé actuel pourrait toutefois reprendre ses rapports de travail le plus rapidement possible. Durant la période transitoire, le PFPDT serait dirigé par le suppléant du préposé.

Les opinions exprimées reflètent l'opinion personnelle des auteurs et n'engagent pas l'Office fédéral de la justice.

MATÉRIAUX

Botschaft des Bundesrates vom 15.9.2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 S. 6941).

Bericht der SPK-N vom 27.1.2022 zur parlamentarischen Initiative 21.443 «Verordnung über das Arbeitsverhältnis der Leiterin oder des Leiters des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten» (BBl 2022 S. 345).

ATTENTION : Cette version du commentaire est une traduction automatique de l'original. Le commentaire original est en allemand. La traduction a été faite avec www.deepl.com. Seule la version originale fait foi. La version traduite du commentaire ne peut pas être citée.

COMMENTAIRE

Art. 72a LPD

Un commentaire de Danielle Schneider / Carl Jauslin

PROPOSITION DE CITATION

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 72a DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Citation abrégée: OK-Schneider/Jauslin, N. XXX zu Art. 72a DSG.

Art. 72a Disposition transitoire concernant les rapports de travail du préposé

Les rapports de travail du préposé établis en vertu de l'ancien droit sont régis par celui-ci.

TABLE DES MATIÈRES

En bref 889
I. Généralités 889
II. Disposition transitoire concernant les rapports de travail du préposé 889
Matériaux 890

EN BREF

Avec la révision totale de la LPD, l'Assemblée fédérale devient l'organe de nomination et l'employeur du préposé. Cela a des conséquences sur les rapports de travail. Les nouvelles dispositions relatives aux rapports de travail du préposé ne s'appliqueront qu'après sa première élection par l'Assemblée fédérale (Chambres réunies). Après l'entrée en vigueur du nouveau droit de la protection des données le 1er septembre 2023, l'ancien droit continuera donc de s'appliquer aux rapports de travail jusqu'à l'élection du préposé par l'Assemblée fédérale réunie.

I. GÉNÉRALITÉS

Avec la révision totale de la LPD, l'Assemblée fédérale devient l'organe de nomination et l'employeur du préposé. Elle est donc compétente pour régler les rapports de travail de ce dernier (cf. art. 43 al. 3bis LPD). Dans le cadre de l'initiative parlementaire CIP-N 21.443, elle a édicté des dispositions d'exécution correspondantes. Par ailleurs, la LPD contient également diverses règles relatives aux rapports de travail du préposé, notamment en ce qui concerne la durée du mandat et sa fin (art. 44 LPD), le droit disciplinaire (art. 44a LPD) ou l'activité accessoire (art. 47 LPD). L'art. 72a LPD précise à partir de quand ces nouvelles dispositions s'appliquent au préposé. 1

II. DISPOSITION TRANSITOIRE CONCERNANT LES RAPPORTS DE TRAVAIL DU PRÉPOSÉ

La nomination du préposé et la fin de son mandat sont régies par l'ancien droit jusqu'à la fin de la législature au cours de laquelle la LPD entre en vigueur (art. 72 al. 1 LPD). Ce n'est que lorsque le préposé sera élu par l'Assemblée fédérale (Chambres réunies) que ses rapports de travail pourront être régis par le nouveau droit. L'art. 72a LPD prévoit donc que les rapports de travail du préposé fondés sur l'ancien droit sont régis par ce dernier. 2

Cela signifie qu'après l'entrée en vigueur du nouveau droit de la protection des données le 1er septembre 2023, les rapports de travail du préposé resteront régis par l'ancien droit jusqu'à la première nomination par l'Assemblée fédérale (Chambres réunies). Ensuite, les dispositions totalement 3

révisées ou nouvellement créées concernant les rapports de travail du préposé s'appliqueront.

Les opinions exprimées reflètent l'opinion personnelle des auteurs et n'engagent pas l'Office fédéral de la justice.

MATÉRIAUX

Bericht der SPK-N vom 27.1.2022 zur parlamentarischen Initiative 21.443 «Verordnung über das Arbeitsverhältnis der Leiterin oder des Leiters des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten» (BBl 2022 S. 345).