Legge federale sulla protezione dei dati

Ultima modifica: 27.07.2026

PDF creato il: 06.10.2026

COMMENTARIO ONLINE
IL COMMENTARIO GIURIDICO
IN OPEN ACCESS

INDICE

Vorb. zu Art. 1 LPD 7
Art. 1 LPD 15
Art. 2 LPD 21
Art. 3 LPD 31
Art. 4 LPD 37
Art. 5 lett. d LPD 49
Art. 5 lett. c LPD 59
Art. 5 lit. f und g LPD 75
Art. 6 cpv. 3-5 LPD 93
Art. 6 cpv. 6 e 7 LPD 115
Art. 7 LPD 137
Art. 10 LPD 161
Art. 11 LPD 181
Art. 12 LPD 197
Art. 14 LPD 215
Art. 15 LPD 225
Art. 18 LPD 231
Art. 19 LPD 239
Art. 20 LPD 265
Art. 21 LPD 283
Art. 22 LPD 323
Art. 23 LPD 347
Art. 25 LPD 363
Art. 26 LPD 379
Art. 27 LPD 389
Art. 28 LPD 397
Art. 29 LPD 421
Art. 31 cpv. 2 lit. e LPD 431
Art. 33 LPD 441

Art. 34 LPD 447
Art. 35 LPD 467
Art. 38 LPD 477
Art. 39 LPD 495
Art. 40 LPD 507
Art. 41 LPD 521
Art. 42 LPD 533
Art. 43 LPD 539
Art. 44 LPD 555
Art. 44a LPD 565
Art. 45 LPD 571
Art. 46 LPD 579
Art. 47 LPD 585
Art. 47a LPD 593
Art. 48 LPD 599
Art. 49 LPD 607
Art. 50 LPD 619
Art. 51 LPD 637
Art. 52 LPD 653
Art. 54 LPD 671
Art. 55 LPD 701
Art. 57 LPD 737
Art. 58 LPD 753
Art. 60 LPD 771
Art. 61 LPD 783
Art. 62 LPD 797
Art. 63 LPD 807
Art. 64 LPD 815
Art. 65 LPD 825
Art. 66 LPD 831

Art. 67 LPD 837
Art. 69 LPD 855
Art. 72 LPD 863
Art. 72a LPD 869

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Vorb. zu Art. 1 LPD

Un commentario di Sandra Husi-Stämpfli

CITAZIONE SUGGERITA

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

Breve citazione: OK-Husi-Stämpfli, N. XXX zu Vorb. zu Art. 1 DSG.

STRUTTURA

In breve 9
I. Il giuramento di Ippocrate come primo segreto professionale 9
II. XX secolo: La legge sulla protezione dei dati entra nell'ordinamento giuridico 9
III. XXI secolo: Protezione dei dati e digitalizzazione 10
A. Impulso: la revisione della protezione dei dati nell'UE 11
B. Il percorso svizzero verso una moderna legge sulla protezione dei dati personali 11
Bibliografia 13

IN BREVE

La legge sulla protezione dei dati ha le sue origini nel segreto professionale (antico) sviluppato per la prima volta da Ippocrate: L'idea era quella di mantenere segrete le informazioni sui pazienti. Da questo concetto, con il crescente progresso tecnico, la relativa complessità e la globalizzazione dello scambio di informazioni, a partire dal 1970 si sono sviluppate le prime codificazioni generali della legge sulla protezione dei dati - prima nei singoli Paesi, poi gradualmente anche a livello transfrontaliero da parte di organizzazioni internazionali e infine dalla Comunità Europea. La prima legge sulla protezione dei dati in Svizzera è entrata in vigore nel 1992, quella totalmente rivista (nuova) il 1° settembre 2023.

I. IL GIURAMENTO DI IPPOCRATE COME PRIMO SEGRETO PROFESSIONALE

La prima normativa codificata sulla protezione dei dati personali può essere fatta risalire al periodo compreso tra il 460 e il 370 a.C.: Con il Giuramento di Ippocrate, i medici si impegnano ancora oggi a mantenere segrete le informazioni sui loro pazienti. A questo si aggiunsero vari segreti professionali, come il segreto dell'ostetrica, il segreto del confessionale o il segreto dell'avvocato. 1

II. XX SECOLO: LA LEGGE SULLA PROTEZIONE DEI DATI ENTRA NELL'ORDINAMENTO GIURIDICO

Le disposizioni originariamente legate alla professione per la protezione delle informazioni personali, come il segreto medico, il segreto ostetrico o persino il segreto professionale, si basano sulla convinzione che le violazioni possano essere individuate immediatamente e che i responsabili possano essere chiamati a risponderne senza ulteriori sforzi. 2

Questo concetto di chiarezza delle responsabilità è stato superato dal progresso tecnico, dalla relativa complessità e dalla crescente globalizzazione dello scambio di informazioni già nel secolo scorso. Così, negli anni '70, sono sorte le prime domande su come gestire l'elaborazione "automatizzata" dei dati, cioè l'uso dei computer e le relative responsabilità e sfide per la sicurezza 3

dei dati - improvvisamente, ad esempio, non era più "solo" il medico a scrivere una nota a mano nella cartella clinica fisica del paziente - i dati erano memorizzati su un PC, che nella migliore delle ipotesi era gestito da una società informatica esterna, ecc. Le nuove sfide associate a questo fenomeno hanno portato alla creazione delle prime codifiche generali della legge sulla protezione dei dati intorno al 1970, prima nei singoli Paesi, poi gradualmente a livello transfrontaliero da parte di organizzazioni internazionali e infine da parte della Comunità Europea.

4 Esempi:

- 1973: Svezia.
- 1977: Repubblica Federale Tedesca.
- 1978: Austria e Francia.
- 1980: Linee guida dell'OCSE per la protezione della privacy e dei flussi transfrontalieri di dati personali.
- 1981: Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato dei dati personali.
- 1995: Direttiva UE sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati.
- 2000: Carta dei diritti fondamentali dell'Unione Europea (CGUE) con l'articolo 8 "Protezione dei dati personali".

In Svizzera, il movimento di codificazione è iniziato a livello cantonale e federale negli anni '70 ed è infine culminato nella Legge federale sulla protezione dei dati nel 1992.

III. XXI SECOLO: PROTEZIONE DEI DATI E DIGITALIZZAZIONE

5 La LPD, nata in un'epoca in cui il "trattamento automatizzato dei dati" era un'eccezione, non era sempre più in grado di soddisfare le esigenze del mondo digitalizzato. La revisione della LPD è stata influenzata in modo significativo dalla revisione della protezione dei dati nell'UE:

A. Impulso: la revisione della protezione dei dati nell'UE

Nel 2012 l'Unione europea ha avviato un dibattito sulla moderna normativa in materia di protezione dei dati. Dopo intensi negoziati, il Parlamento europeo e il Consiglio dell'Unione europea hanno infine adottato il Regolamento generale sulla protezione dei dati (DSGVO) e la Direttiva 2016/680 nel 2016. 6

- Il DSGVO regolamenta principalmente la protezione dei dati trattati nel contesto del mercato interno europeo, ma si applica anche al settore pubblico. È entrato in vigore il 25 maggio 2018.
- La direttiva 2016/680 è volta a proteggere i dati personali trattati a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, compresa la salvaguardia e la prevenzione di minacce alla sicurezza pubblica. La direttiva 2016/680 è allineata alla formulazione del DSGVO per ottenere un vocabolario di base coerente per quanto riguarda i principi generali in tutta l'area dell'UE. È entrata in vigore il 5 maggio 2016.

B. Il percorso svizzero verso una moderna legge sulla protezione dei dati personali

Il 9 dicembre 2011, il Consiglio federale ha approvato un rapporto sulla valutazione della LPD e ha incaricato il Dipartimento federale di giustizia e polizia (DFGP) di esaminare misure legislative per rafforzare la protezione dei dati, tenendo conto dei risultati della valutazione e degli sviluppi in corso nell'UE e nel Consiglio d'Europa. In quell'occasione, il Consiglio federale si è chiesto in che misura fosse necessario aumentare la trasparenza del trattamento dei dati e sensibilizzare le persone interessate ai nuovi rischi. In particolare, la revisione della necessità di azioni legali dovrebbe tenere conto del fatto che i minori sono particolarmente vulnerabili quando si tratta del trattamento dei loro dati. Allo stesso tempo, però, il Consiglio federale ha anche sottolineato che l'esame delle misure legislative deve tenere conto del fatto che le misure di protezione dei dati possono entrare in conflitto con altri interessi. Pertanto, oltre alla protezione della privacy, devono essere presi in considerazione anche gli interessi dell'economia, il diritto alla libertà di opinione e di informazione, nonché altri interessi privati e pubblici. Questo lavoro è stato svolto con il coinvolgimento di un gruppo consultivo, che ha definito la necessità di un intervento legislativo entro il 2014. 7

8 Dopo aver preso atto del rapporto del gruppo consultivo il 1° aprile 2015, il Consiglio federale ha incaricato il DFGP di preparare un progetto preliminare di revisione della LPD entro la fine di agosto 2016. Questo progetto preliminare di revisione totale della LPD e di modifica di altre leggi sulla protezione dei dati è stato inviato in consultazione il 21 dicembre 2016.

9 Il Consiglio federale ha infine adottato il messaggio sulla "nuova" legge sulla protezione dei dati il 15 settembre 2017. L'obiettivo del Consiglio federale era quello di "adattare la protezione dei dati all'era di Internet e rafforzare la posizione dei cittadini". Allo stesso tempo, il livello svizzero di protezione dei dati doveva essere allineato a quello dell'UE al fine di preservare la decisione di adeguatezza, importante per il libero trasferimento dei dati tra le aziende svizzere e quelle dell'UE.

10 Le consultazioni parlamentari sono state difficili; a volte vi erano opinioni fondamentalmente divergenti sulla portata della nuova legge sulla protezione dei dati. Allo stesso tempo, il tempo stringeva: singole disposizioni della nuova legge sulla protezione dei dati erano "rilevanti per Schengen" e dovevano essere attuate entro due anni dall'entrata in vigore della corrispondente legge Schengen. Il Parlamento ha quindi deciso di dividere il disegno di legge: La cosiddetta "legge sulla protezione dei dati Schengen" è stata adottata il 28 settembre 2018 ed è entrata in vigore il 1° marzo 2019. È stata nuovamente abrogata o reintegrata nella legge sulla protezione dei dati quando è entrata in vigore la nuova legge sulla protezione dei dati. La "legge sulla protezione dei dati Schengen" disciplinava il trattamento dei dati personali da parte degli organi federali ai fini della prevenzione, dell'indagine o del perseguimento di reati o dell'esecuzione di pene, compresa la protezione e la prevenzione di minacce alla sicurezza pubblica.

11 In una seconda fase, sono stati discussi gli aspetti della revisione della protezione dei dati non pertinenti all'area Schengen e fortemente influenzati dal DSGVO. Si trattava in particolare delle innovazioni per il trattamento dei

dati personali da parte dei privati (cioè principalmente delle aziende). Le discussioni si sono concentrate sui seguenti argomenti:

- Rafforzamento dei diritti degli interessati: Estensione del diritto all'informazione (OC-Steiger sull'art. 25 LPD) e introduzione del diritto alla portabilità dei dati (si veda il commento dell'OC sull'art. 28 LPD).
- Estensione degli obblighi dei responsabili e degli incaricati del trattamento: introduzione del principio della privacy by design e default (OC Claus sull'art. 7 LPD) e dell'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati per determinate forme di trattamento (OC Harasgama sull'art. 22 LPD) e di segnalare le violazioni della protezione dei dati all'autorità di controllo (OC de la Cruz sull'art. 24 LPD).
- Introduzione di un catalogo di sanzioni (OK-Gassmann sull'art. 60 e segg. LPD) e rafforzamento delle competenze dell'IFPD (OK-Reinle sull'art. 49 LPD; OK-Fanger/Oehri sull'art. 50 LPD).

Infine, dopo tre anni, la revisione della legge sulla protezione dei dati è stata adottata il 25 settembre 2020. Il referendum è decaduto non utilizzato, per cui la legge è entrata in vigore il 1° settembre 2023 insieme all'ordinanza di attuazione (DPO), anch'essa totalmente rivista. 12

L'autrice fornisce la sua valutazione personale in questo commento.

BIBLIOGRAFIA

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

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 1 LPD

Un commentario di Sandra Husi-Stämpfli

CITAZIONE SUGGERITA

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

Breve citazione: OK-Husi-Stämpfli, N. XXX zu Art. 1 DSG.

Capitolo 1:
Scopo e campo d'applicazione nonché autorità federale di vigilanza

Art. 1 Scopo

Scopo della presente legge è proteggere la personalità e i diritti fondamentali delle persone fisiche i cui dati personali sono oggetto di trattamento.

STRUTTURA

In breve 17
I. Primo: le varie forme di protezione della personalità 17
A. Protezione costituzionale dell'autodeterminazione informativa ai sensi dell'art. 13 cpv. 2 Cost. 17
B. Protezione della personalità nel diritto civile 18
II. Protezione della personalità ai sensi della legge sulla protezione dei dati 19
A. Storia delle origini Art. 1 LPD 19
B. Scopo della LPD 19
C. Natura giuridica dell'art. 1 LPD 20
Bibliografia 20

IN BREVE

Insieme alla protezione della personalità in base al diritto civile, la legge sulla protezione dei dati garantisce l'attuazione della protezione della personalità in base ai diritti fondamentali: la LPD serve a proteggere la personalità e i diritti fondamentali delle persone fisiche, ma non più la protezione delle persone giuridiche, come avveniva con la vecchia LPD. Lo scopo della LPD è quindi più ristretto rispetto a quello del DSGVO, ad esempio, che mira anche a consentire la libera circolazione dei dati. Con la formulazione scelta, il legislatore svizzero chiarisce che la legge sulla protezione dei dati è la protezione della personalità avant tout, e non la protezione degli operatori economici, della sicurezza pubblica o di altri interessi.

I. PRIMO: LE VARIE FORME DI PROTEZIONE DELLA PERSONALITÀ

Il diritto della protezione dei dati, insieme alla protezione della personalità di diritto civile (art. 27 e art. 28 e segg. del Codice civile, cfr. infra, n. 3), garantisce l'attuazione della protezione della personalità nell'ambito dei diritti fondamentali (art. 10 della Cost., cfr. infra, n. 2), e come sua manifestazione della privacy o dell'autodeterminazione informativa (art. 13 cpv. 2 della Cost., cfr. infra, n. 2). L'interazione di questi elementi della protezione della personalità è la seguente: 1

A. Protezione costituzionale dell'autodeterminazione informativa ai sensi dell'art. 13 cpv. 2 Cost.

L'articolo 13 della Cost. protegge la sfera privata come spazio per lo sviluppo e il dispiegamento della personalità individuale. Ogni persona, indipendentemente dal sesso, dall'origine, dall'età, ecc. ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Come aspetto speciale del diritto alla privacy, l'art. 13 cpv. 2 della Cost. garantisce il diritto alla protezione contro l'uso improprio dei dati personali. Secondo la giurisprudenza, la formulazione del cpv. 2 è troppo ristretta: la "protezione dei dati dei diritti fondamentali" deve coprire in linea di principio qualsiasi trattamento dei dati personali da parte dello Stato. 2

B. Protezione della personalità nel diritto civile

3 I diritti della personalità tutelati dall'art. 27 e dagli artt. 28 e segg. Codice civile, che fanno parte del diritto fondamentale della libertà personale di cui all'art. 10 della Cost., sono a disposizione degli individui per se stessi e sono indissolubilmente legati alla loro persona. La maggior parte degli studiosi suddivide l'area protetta dall'art. 28 CC in tre categorie: personalità fisica, personalità affettiva e personalità sociale.

- La personalità fisica riguarda l'integrità corporea e la libertà di movimento.
- La personalità affettiva o psicologica protegge la sfera mentale-emotiva della vita di una persona.
- La tutela sociale della personalità contribuisce all'organizzazione armoniosa delle relazioni sociali e societarie e protegge tutti i beni a cui una persona deve avere diritto per poter vivere una vita armoniosa nella società: Si tratta, in particolare, del diritto al proprio nome, del diritto all'onore, del diritto alla propria immagine, della protezione dei dati, della libertà economica e del diritto al rispetto e all'osservanza della vita privata.

4 Le disposizioni di base per la tutela di diritto privato di cui agli artt. 27 e segg. CC si applicano quando si verifica una violazione dei diritti della personalità da parte di un'altra persona privata e il caso non può essere regolato da una norma speciale di diritto privato. Dall'art. 28 CC si ricava uno schema di esame in due fasi:

- In primo luogo, si esamina se c'è stata una violazione dei diritti della personalità.
- Poi, in una seconda fase, si deve esaminare se esiste una giustificazione ai sensi dell'art. 28 cpv. 2 CC, in modo che la violazione possa essere valutata come non illegale. Se, tuttavia, dopo l'esame dell'art. 28 cpv. 2 CC, non vi è alcuna giustificazione, la violazione dei diritti della personalità è considerata illegittima.

II. PROTEZIONE DELLA PERSONALITÀ AI SENSI DELLA LEGGE SULLA PROTEZIONE DEI DATI

A. Storia delle origini Art. 1 LPD

L'art. 1 LPD è stato ripreso senza modifiche dalla vecchia LPD, anche se, almeno durante il processo di consultazione, diverse parti hanno espresso il desiderio che, analogamente all'art. 1 LPD, anche il traffico transfrontaliero di dati e la protezione della competitività fossero inclusi nello scopo della LPD. Tuttavia, la disposizione è rimasta indiscussa nel dibattito parlamentare. 5

B. Scopo della LPD

Sia la LPD che le leggi cantonali sulla protezione dei dati (delle informazioni e dei dati) affermano nelle loro disposizioni sullo scopo che la protezione dei dati non deve essere intesa come un fine in sé, ma come uno strumento per salvaguardare i diritti fondamentali o la protezione della personalità delle persone fisiche i cui dati sono trattati - i dati delle persone giuridiche non sono più coperti dalla LPD (cfr. OK-Husi-Stämpfli Art. 2 N. 12). 6

In questo senso, la legge svizzera sulla protezione dei dati si differenzia chiaramente dal DSGVO, che, oltre alla protezione della personalità, indica anche la libera circolazione dei dati come scopo del regolamento. In altre parole: la legge svizzera sulla protezione dei dati è proprio la protezione della personalità avant tout, e non la protezione degli operatori economici, della sicurezza pubblica o di altri interessi. 7

La protezione della personalità è finalizzata principalmente al trattamento dei dati da parte di privati, mentre la protezione dei diritti fondamentali è finalizzata alla tutela dalle interferenze delle autorità statali. Dato che, da un punto di vista costituzionale, la protezione della personalità è una conseguenza del dovere dello Stato di proteggere e attuare i diritti fondamentali non solo da parte dello Stato, ma anche tra privati (art. 35 cpv. 3 Cost.), sarebbe stato più coerente da un punto di vista giuridico elencare prima la protezione dei diritti fondamentali e poi la protezione della personalità. 8

Inoltre, i "diritti fondamentali" menzionati nell'art. 1 LPD non comprendono solo l'art. 13 cpv. 2 Cost. o l'art. 8 CEDU. Piuttosto, l'art. 1 LPD deve essere 9

inteso come comprensivo di tutti i diritti fondamentali che possono essere influenzati dal trattamento dei dati, come la libertà di espressione, il divieto di discriminazione, ecc. L'azione dello Stato deve essere conforme non solo alla LPD, ma anche ai diritti fondamentali (art. 36 Cost.).

C. Natura giuridica dell'art. 1 LPD

10 L'art. 1 LPD è una disposizione programmatica: non stabilisce diritti e obblighi, ma deve essere inteso come una linea guida per l'interpretazione delle disposizioni successive.

In questo commento, l'autrice fornisce la sua personale valutazione.

BIBLIOGRAFIA

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 2 LPD

Un commentario di Sandra Husi-Stämpfli

CITAZIONE SUGGERITA

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

Breve citazione: OK-Husi-Stämpfli, N. XXX zu Art. 2 DSG.

Art. 2 Campo d'applicazione personale e materiale

[1] La presente legge si applica al trattamento di dati personali concernenti persone fisiche da parte di:

a. privati;

b. organi federali.

[2] Non si applica al trattamento di dati personali da parte:

a. di persone fisiche per uso esclusivamente personale;

b. delle Camere federali e delle commissioni parlamentari nell'ambito delle loro deliberazioni;

c. dei beneficiari istituzionali di cui all'articolo 2 capoverso 1 della legge del 22 giugno 2007 sullo Stato ospite che godono dell'immunità di giurisdizione in Svizzera.

[3] Il trattamento di dati personali e i diritti delle persone interessate nei procedimenti giudiziari e nei procedimenti secondo gli ordinamenti procedurali federali sono retti dal diritto processuale applicabile. Le disposizioni della presente legge si applicano alle procedure amministrative di primo grado.

[4] I registri pubblici relativi ai rapporti di diritto privato, in particolare l'accesso a tali registri e i diritti delle persone interessate, sono retti dalle disposizioni speciali del diritto federale applicabile. In assenza di disposizioni speciali si applica la presente legge.

STRUTTURA

In breve 24
I. Aspetti generali 24
A. Scopo della legge 24
B. Competenza normativa 24
II. Ambito di applicazione personale (art. 2 cpv. 1 LPD) 26
III. Campo di applicazione materiale: dati di persone fisiche 26
IV. Eccezioni 26
A. Uso a fini privati (art. 2 cpv. 2 lett. a LPD) 26
B. Trattamento da parte dell'Assemblea federale e delle commissioni parlamentari (art. 2 cpv. 2 lett. b LPD) 27
C. Trattamento dei dati da parte di missioni diplomatiche e organizzazioni internazionali (art. 2 cpv. 2 lett. c LPD) 27
D. Procedimenti giudiziari o federali in corso (art. 2 cpv. 3 LPD) 28
E. Registri pubblici dei negozi giuridici privati 29
Bibliografia 30

IN BREVE

La LPD si applica al trattamento dei dati di persone fisiche da parte di organi federali e privati. Tuttavia, la LPD non si applica in modo assoluto: alcuni casi, in particolare il trattamento dei dati esclusivamente per uso personale o nell'ambito di procedimenti giudiziari o federali in corso, sono esclusi dalla LPD o sono disciplinati da disposizioni (procedurali) specifiche e separate.

I. ASPETTI GENERALI

A. Scopo della legge

1 L'art. 2 LPD definisce il campo di applicazione della Legge federale sulla protezione dei dati e le relative eccezioni. Il campo di applicazione della LPD è stato parzialmente ampliato in sede di revisione, in particolare per soddisfare i requisiti dell'ERK 108+: Ad esempio, sono state adattate le eccezioni relative ai procedimenti civili in corso, ai procedimenti penali, ai procedimenti di assistenza giudiziaria internazionale e ai procedimenti di diritto statale e amministrativo (art. 2 cpv. 2 lett. c LPD) e quelle relative ai registri pubblici dei negozi giuridici privati (art. 2 cpv. 2 lett. d LPD).

B. Competenza normativa

2 La competenza a regolamentare la legge sulla protezione dei dati deriva dall'ordine generale delle competenze della Confederazione: secondo gli articoli 3 e 42 della Cost. la Confederazione ha un potere individuale limitato, mentre i Cantoni esercitano tutti i compiti che non sono assegnati alla Confederazione.

3 La Confederazione ha quindi il diritto di regolamentare il trattamento dei dati negli ambiti in cui può in linea di principio legiferare, in particolare nell'ambito dell'organizzazione e della procedura delle autorità federali (art. 164 n. 1 lett. g Cost.). Nell'incipit della LPD si fa riferimento all'art. 95 ("Attività del settore privato"), all'art. 122 ("Diritto civile") e all'art. 173 cpv. 2 Cost. ("Altri compiti e competenze"). Anche se questi articoli non menzionano esplicitamente la competenza della Confederazione in materia di protezione dei dati, è indiscutibile che essi includono la competenza di emanare disposizioni in materia di protezione dei dati.

Il fatto che il trattamento dei dati personali soddisfi i requisiti della legge sulla protezione dei dati è determinato, da un lato, dalle disposizioni delle leggi sulla (informazione e) protezione dei dati (la cosiddetta legge "generale" sulla protezione dei dati) e, dall'altro, dalle disposizioni di quelle leggi speciali che regolano il trattamento dei dati in casi specifici di applicazione (legge "speciale" sulla protezione dei dati). 4

In una prima fase, sia gli enti pubblici che i privati devono attenersi alla legge "generale" sulla protezione dei dati se desiderano trattare dati personali: 5

- Gli organi federali e i privati devono attenersi ai requisiti di trattamento della legge federale sulla protezione dei dati.
- Se gli enti pubblici cantonali trattano dati personali, devono attenersi alle leggi cantonali sulla protezione dei dati.

La legge "generale" sulla protezione dei dati regola - a livello cantonale e federale - tra l'altro i seguenti argomenti: scopo della legge, campo di applicazione, definizioni, principi di trattamento, norme sulla responsabilità, diritti degli interessati, ecc. In linea con la sua natura di legislazione di base, la legge "generale" sulla protezione dei dati contiene solitamente anche disposizioni eccezionali che definiscono in quali casi prevalgono requisiti legali speciali. 6

In una seconda fase, gli enti pubblici devono verificare se sono autorizzati a trattare i dati personali in questione per adempiere ai loro doveri legali, ossia se le rispettive leggi sostanziali (la legge settoriale o "speciale" sulla protezione dei dati) regolano specificamente il trattamento dei dati. 7

La legge settoriale o "speciale" sulla protezione dei dati deve soddisfare i requisiti della legge generale sulla protezione dei dati e, oltre alla finalità del trattamento (cioè il compito specifico per il quale i dati personali devono essere trattati), deve specificare, tra l'altro, le responsabilità e gli eventuali obblighi di divulgazione. 8

I privati, da parte loro, devono garantire in questa seconda fase di avere una giustificazione per il trattamento dei dati in questione, nella misura in cui il trattamento viola i diritti personali. 9

II. AMBITO DI APPLICAZIONE PERSONALE (ART. 2 CPV. 1 LPD)

10 La legge federale sulla protezione dei dati si applica al trattamento dei dati di persone fisiche da parte di organi federali (cfr. N. 11 Commento all'art. 5 lett. i e OK-Zysset art. 34 LPD) e di privati (cfr. OK-dal Molin art. 30 LPD). Per il trattamento dei dati personali da parte di enti pubblici cantonali si applica la rispettiva legge cantonale sulla protezione dei dati (informazione e protezione dei dati) (cfr. N. 5).

III. CAMPO DI APPLICAZIONE MATERIALE: DATI DI PERSONE FISICHE

11 Ogni essere umano è considerato una persona fisica in senso giuridico e ogni essere umano ha capacità giuridica (art. 11 cpv. 1 CC). Ogni essere umano ha quindi la capacità di avere diritti e doveri (art. 11 cpv. 2 CC) - questi diritti comprendono anche il diritto della personalità dal punto di vista del diritto civile e del diritto della protezione dei dati (art. 28 e segg. CC o art. 1 in particolare in combinato disposto con l'art. 30 LPD e l'art. 34 LPD).

12 Con l'ultima revisione della protezione dei dati, il campo di applicazione materiale è stato ristretto: I dati delle persone giuridiche non sono più coperti dalla LPD, ma ciò è comunque insignificante nella pratica, perché le persone giuridiche possono ancora rivendicare violazioni dei diritti della personalità ai sensi degli artt. 28 e segg. Codice civile (ad esempio, danni alla reputazione). Esse godono inoltre della protezione della Legge federale contro la concorrenza sleale, della Legge sul diritto d'autore o delle disposizioni specifiche sul segreto professionale, commerciale o di fabbricazione.

IV. ECCEZIONI

13 La LPD non è assoluta. L'art. 2 cpv. 2-4 LPD menziona varie eccezioni alle quali la LPD non si applica.

A. Uso a fini privati (art. 2 cpv. 2 lett. a LPD)

14 La LPD non si applica se i dati personali in questione sono trattati da una persona fisica esclusivamente per uso personale (art. 2 cpv. 2 lett. a LPD). Ne è un esempio una raccolta di lettere o e-mail che una coppia di coniugi si è

scritta nel corso degli anni e che contiene anche osservazioni e aneddoti su altre persone. Anche gli album fotografici privati con immagini di feste di famiglia, vacanze di amici, ecc. sono esenti dalla LPD, a condizione che le foto non vengano ulteriormente diffuse (ad esempio digitalizzate e pubblicate).

B. Trattamento da parte dell'Assemblea federale e delle commissioni parlamentari (art. 2 cpv. 2 lett. b LPD)

I dati personali sono trattati dall'Assemblea federale e dalle commissioni parlamentari nell'ambito delle loro deliberazioni (art. 2 cpv. 2 lett. b LPD). Questa disposizione è stata ripresa senza modifiche dalla vecchia LPD. Secondo il messaggio, la deroga alla LPD è motivata dal fatto che il Parlamento non sarebbe in grado di adempiere ai propri doveri costituzionali se dovesse rispettare in ogni caso i principi della protezione dei dati - il messaggio cita esplicitamente i requisiti per la divulgazione dei dati personali. Tuttavia, sembra molto più plausibile sostenere che la legge speciale che disciplina le procedure aziendali dei Consigli (la "legge speciale sulla protezione dei dati") contiene disposizioni dettagliate sul trattamento delle informazioni (e quindi dei dati personali), motivo per cui la subordinazione alla LPD non è semplicemente necessaria. 15

C. Trattamento dei dati da parte di missioni diplomatiche e organizzazioni internazionali (art. 2 cpv. 2 lett. c LPD)

Non rientrano nella LPD anche i trattamenti effettuati da una rappresentanza diplomatica o consolare di un altro Stato o da un'organizzazione internazionale. In altre parole, questa eccezione riguarda i beneficiari istituzionali di cui all'art. 2 cpv. 1 della Legge sullo Stato ospite del 22 giugno 2007, che godono dell'immunità dalla giurisdizione in Svizzera: godono dell'indipendenza e della libertà d'azione basate sul diritto internazionale e sulla DDA per poter svolgere le loro funzioni internazionali, e di conseguenza non ci si può aspettare che si sottomettano alle regole del diritto svizzero per quanto riguarda i dati trattati dalle loro rappresentanze diplomatiche o consolari. 16

D. Procedimenti giudiziari o federali in corso (art. 2 cpv. 3 LPD)

17 La LPD non si applica nemmeno ai procedimenti giudiziari o federali in corso, poiché questi sono disciplinati dal rispettivo diritto processuale, che contiene disposizioni dettagliate sul trattamento dei dati personali (delle parti, dei ricorrenti, ecc.).

18 Il termine "procedimento giudiziario" comprende tutti i procedimenti dinanzi ai tribunali penali, civili e amministrativi cantonali e federali, ma anche dinanzi ai tribunali arbitrali con sede in Svizzera. A differenza dell'aDSG, l'art. 2 cpv. 3 LPD non utilizza il termine "procedimento pendente", poiché solo il diritto processuale civile fa riferimento alla litispendenza e questo termine ha talvolta causato problemi di delimitazione.

19 L'unico fattore decisivo è ora il fatto che il procedimento si svolga davanti a un tribunale o sia regolato da un codice di procedura federale. Il procedimento si svolge davanti a un tribunale quando quest'ultimo viene investito per la prima volta di una causa avviando un procedimento secondo le norme procedurali applicabili. I procedimenti sono disciplinati dalle norme procedurali federali quando una determinata questione è trattata da un'autorità in conformità alle disposizioni di una di queste leggi.

20 I codici di procedura federali che contengono disposizioni sul trattamento dei dati personali o sui diritti delle persone interessate nell'ambito di tali procedure comprendono in particolare

- la Legge federale sulla procedura amministrativa del 20 dicembre 1968 (PA, nella misura in cui non riguarda i procedimenti amministrativi di primo grado),
- il Codice di procedura civile del 19 dicembre 2008 (CPC),
- la Legge federale dell'11 aprile 1889 sul recupero crediti e sul fallimento (LEF),
- il Codice di procedura penale del 5 ottobre 2007 (CCP),
- la Legge federale del 22 marzo 1974 sul diritto penale amministrativo (ACC), oppure
- la Legge federale sull'assistenza internazionale in materia penale del 20 marzo 1981 (IMAC).

Il trattamento dei dati da parte dei servizi amministrativi dei tribunali e delle autorità non rientra nell'ambito di applicazione delle rispettive leggi procedurali, pertanto l'art. 2 cpv. 3 LPD non si applica. 21

Di norma, le norme procedurali pertinenti restano applicabili anche dopo la conclusione del procedimento: Ad esempio, si applicano disposizioni speciali per la tenuta dei fascicoli, l'ispezione dei fascicoli, la correzione dei fascicoli o la conservazione dei fascicoli. Tuttavia, non è escluso che la legge processuale applicabile dichiari la LPD applicabile dopo la conclusione del procedimento (cfr. art. 99 del Codice di procedura penale). 22

E. Registri pubblici dei negozi giuridici privati

Infine, il trattamento dei dati nell'ambito dei registri pubblici di transazioni giuridiche private gestiti sulla base del diritto federale e da organi federali è escluso dall'ambito di applicazione della LPD. In questo caso si applica la rispettiva legge speciale. Questi registri comprendono in particolare 23

- il registro elettronico dello stato civile Zefix
- il registro degli aeromobili dell'Ufficio federale dell'aviazione civile, e
- i registri dell'Istituto federale della proprietà intellettuale (in particolare il registro dei marchi, dei brevetti e dei disegni).

I registri pubblici dei negozi giuridici privati, di cui sono responsabili i Cantoni, sono soggetti alla legge cantonale sulla protezione dei dati. I registri cantonali comprendono, ad esempio. 24

- il registro fondiario
- il registro navale
- i registri commerciali e
- i registri delle esecuzioni e dei fallimenti.

L'autrice fornisce la sua valutazione personale in questo commento.

BIBLIOGRAFIA

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 3 LPD

Un commentario di Sandra Husi-Stämpfli

CITAZIONE SUGGERITA

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

Breve citazione: OK-Husi-Stämpfli, N. XXX zu Art. 3 DSG.

Art. 3 Campo d'applicazione territoriale

[1] La presente legge si applica alle fattispecie che generano effetti in Svizzera, anche se si verificano all'estero.

[2] Alle pretese di diritto civile si applica la legge federale del 18 dicembre 1987 sul diritto internazionale privato. Sono fatte salve inoltre le disposizioni concernenti il campo d'applicazione territoriale del Codice penale.

STRUTTURA

In breve 33
I. Aspetti generali 33
A. Contesto e finalità 33
B. Storia delle origini 34
II. Applicabilità della LADP secondo il principio dell'effetto (art. 3 cpv. 1 LPD) 34
III. Norme di conflitto per i trattamenti di dati di diritto privato (art. 3 cpv. 2 LPD) 34
IV. Conflitto di leggi nel diritto penale (art. 3 cpv. 2 LPD) 35
Bibliografia 35

IN BREVE

L'art. 3 LPD stabilisce il cosiddetto "principio dell'impatto", secondo il quale le disposizioni della LPD si applicano se le operazioni di trattamento dei dati sono "percepibili" in Svizzera. Ciò significa che non solo le operazioni di trattamento dei dati puramente "svizzere" rientrano nel campo di applicazione della LPD, ma anche quelle costellazioni in cui il trattamento dei dati viene avviato all'estero, ma le conseguenze del trattamento hanno un impatto in Svizzera.

I. ASPETTI GENERALI

A. Contesto e finalità

Il diritto pubblico non dispone di un regime di conflitto di leggi codificato, a differenza del diritto privato e penale. In pratica, quindi, il principio di territorialità si applica alle costellazioni transfrontaliere di diritto pubblico: Il diritto pubblico svizzero si applica sempre quando una situazione si verifica in Svizzera. 1

I criteri utilizzati per determinare il diritto applicabile includono, in particolare, il luogo di domicilio o residenza, il luogo di attività o il luogo di effetto. Secondo la giurisprudenza del Tribunale federale, il cosiddetto principio di effetto è una "manifestazione speciale" del principio di territorialità: Fatti avvenuti all'estero possono essere presi in considerazione dalle autorità svizzere se "hanno un impatto sufficiente sul territorio svizzero". Tuttavia, la prassi non definisce in modo uniforme quando si ha un collegamento sufficiente con la Svizzera nel senso del principio dell'impatto: in genere si richiede che l'impatto sia notevole, significativo, sostanziale o considerevole. 2

L'art. 3 LPD disciplina l'applicazione locale della LPD in conformità ai principi generali di applicazione del diritto pubblico e in particolare al principio dell'impatto. 3

B. Storia delle origini

4 La vecchia LPD non conteneva disposizioni sull'applicazione locale, così come il progetto della nuova LPD. Durante le consultazioni parlamentari, tuttavia, è stato chiesto di introdurre una disposizione sull'ambito territoriale di applicazione, che idealmente corrisponderebbe all'art. 3 (1) e (2) del DSGVO. Di conseguenza, la LPD avrebbe dovuto applicarsi anche nel caso in cui un responsabile del trattamento o un incaricato del trattamento con uno stabilimento al di fuori della Svizzera trattasse i dati di persone in Svizzera per offrire loro (a pagamento o gratuitamente) beni o servizi o per osservare il loro comportamento in Svizzera.

5 Alla luce delle norme di conflitto esistenti, in particolare nel diritto privato, il legislatore è giunto alla conclusione, durante la consultazione, che le preoccupazioni delle persone interessate dal trattamento (internazionale) dei dati potevano essere prese sufficientemente in considerazione ancorando il principio dell'effetto definito dalla giurisprudenza e un riferimento esplicito alle disposizioni della legge federale del 20 marzo 1981 sull'assistenza internazionale in materia penale (IMAC, RS 351.1) o al diritto penale. Di conseguenza, la discussa regolamentazione analoga all'art. 3 cpv. 1 e 2 DSGVO è stata abbandonata.

II. APPLICABILITÀ DELLA LADP SECONDO IL PRINCIPIO DELL'EFFETTO (ART. 3 CPV. 1 LPD)

6 Le disposizioni della LPD sono applicabili in base al principio dell'effetto se le rispettive operazioni di trattamento dei dati hanno un effetto in Svizzera. Ciò significa che rientrano nel campo di applicazione della LPD non solo le operazioni di trattamento dei dati puramente "svizzere", ma anche quelle costellazioni in cui il trattamento dei dati viene avviato all'estero, ma le conseguenze del trattamento sono "percepibili" in Svizzera.

III. NORME DI CONFLITTO PER I TRATTAMENTI DI DATI DI DIRITTO PRIVATO (ART. 3 CPV. 2 LPD)

7 Nell'ambito del diritto privato, la LDIP disciplina il diritto applicabile ai tribunali svizzeri nelle relazioni internazionali; nell'ambito del diritto della protezione dei dati, deve essere osservato l'art. 139 cpv. 1 LDIP. In base a

questo articolo, la persona danneggiata ha un ampio diritto di scegliere la legge applicabile al suo caso. In particolare, la persona lesa ha la possibilità di decidere se si applica la legge dello Stato,

- in cui risiede abitualmente (cpv. 1 lett. a),
- in cui l'autore della violazione ha il suo stabilimento o la sua residenza abituale (cpv. 1 lett. b), oppure
- in cui si verifica il risultato dell'atto di violazione (cpv. 1 lett. c).

In questo modo la parte lesa ha la possibilità di scegliere la legge a lei più favorevole. Per preservare questo vantaggio, la LPD stabilisce esplicitamente che la LDIP si applica alle richieste di risarcimento di diritto privato. 8

IV. CONFLITTO DI LEGGI NEL DIRITTO PENALE (ART. 3 CPV. 2 LPD)

Le disposizioni penali della LPD (art. 60 e segg.) fanno parte del diritto penale derivato, pertanto la loro applicazione territoriale è determinata dai principi della CP (cfr. art. 333 cpv. 1 in combinato disposto con l'art. 104 e gli artt. 3 e segg. CP): In base al principio della protezione individuale sancito dal CP, chiunque violi gli interessi giuridici di cittadini svizzeri all'estero è in linea di principio perseguibile. In considerazione di questa regola di conflitto già esistente, la LPD fa riferimento al Codice penale e non contiene specifiche proprie sull'ambito territoriale di applicazione nel contesto del diritto penale. 9

L'autrice fornisce la sua personale valutazione in questo commento.

BIBLIOGRAFIA

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 4 LPD

Un commentario di Michael Reinle

CITAZIONE SUGGERITA

Michael Reinle, Commentario all'art. 4 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Reinle, art. 4 LPD N. XXX.

Art. 4 Incaricato federale della protezione dei dati e della trasparenza

[1] L'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) vigila sull'applicazione delle disposizioni federali sulla protezione dei dati.

[2] Non sono sottoposti alla vigilanza dell'IFPDT:

a. l'Assemblea federale;

b. il Consiglio federale;

c. i tribunali della Confederazione;

d. il Ministero pubblico della Confederazione, per quanto riguarda il trattamento di dati personali nell'ambito di un procedimento penale;

e. le autorità federali, per quanto riguarda il trattamento di dati personali nell'ambito della loro attività giurisdizionale o di procedure di assistenza giudiziaria internazionale in materia penale.

STRUTTURA

In breve 40
I. Considerazioni generali 40
A. Scopo della norma e contesto 40
B. Genesi 41
II. Sorveglianza da parte dell'IFPDT 42
A. Sorveglianza sull'applicazione delle disposizioni di diritto federale in materia di protezione dei dati (cpv. 1) 42
B. Eccezioni alla sorveglianza (cpv. 2) 43
1. Assemblea federale (lett. a) 43
2. Consiglio federale (lett. b) 44
3. Tribunali federali (lett. c) 44
4. Ministero pubblico della Confederazione (lett. d) 45
5. Autorità federali nell'esercizio della loro funzione giurisdizionale o nell'ambito di procedure di assistenza giudiziaria internazionale in materia penale (lett. e) ... 45
Bibliografia 46
I materiali 47

IN BREVE

L'IFPDT vigila sull'applicazione delle norme federali in materia di protezione dei dati. Sono soggette alla sorveglianza dell'IFPDT le persone fisiche e giuridiche private nonché gli organi federali. Per quanto riguarda la sorveglianza degli organi federali, esistono delle eccezioni fondate sul principio della separazione dei poteri e volte a garantire l'indipendenza della magistratura. L'esclusione dalla sorveglianza non significa che gli organi federali esenti non debbano rispettare le disposizioni della LPD nel trattamento dei dati. Le eccezioni al campo d'applicazione materiale della LPD sono disciplinate all'articolo 2 LPD.

I. CONSIDERAZIONI GENERALI

A. Scopo della norma e contesto

1 La sorveglianza generale dell'IFPDT sull'applicazione delle norme di diritto federale in materia di protezione dei dati non costituisce una novità rispetto alla precedente LPD (art. 27 cpv. 1 aDSG). La novità principale è che l'art. 4 LPD fa riferimento all'IFPDT e non più al preposto, come era il caso nell'art. 27 aDSG. Ciò è dovuto al fatto che la LPD riveduta distingue tra l'IFPDT in qualità di autorità e il/la preposito/a in qualità di persona che dirige l'autorità. Il concetto di preposito è tuttavia definito solo all'art. 43 cpv. 1 LPD.

2 L'art. 4 LPD acquista significato principalmente grazie alle eccezioni alla sorveglianza dell'IFPDT di cui all'art. 4 cpv. 2 LPD. Nel diritto precedente, solo il Consiglio federale era esentato dalla sorveglianza dell'IFPDT (art. 27 cpv. 1 aDSG). Ora l'eccezione alla sorveglianza dell'IFPDT non vale più solo per il Consiglio federale, ma anche per altri organi federali. L'elenco delle eccezioni di cui all'art. 4 cpv. 2 LPD è esaustivo. La LPD non prevede eccezioni alla sorveglianza dell'IFPDT sui privati.

3 Il Consiglio federale è stato esentato dalla sorveglianza dell'IFPDT perché quest'ultimo non può essere l'organo di controllo della propria autorità di sorveglianza e di nomina.

4 Le nuove eccezioni inserite al cpv. 2 per l'Assemblea federale, i tribunali federali, il Ministero pubblico della Confederazione e altre autorità federali in

caso di trattamenti specifici di dati seguono considerazioni analoghe. Esse servono ad attuare il principio della separazione dei poteri e a garantire l'indipendenza della magistratura.

B. Genesi

Nel progetto di revisione della legge sulla protezione dei dati del 29 ottobre 2014, la sorveglianza dell'IFPDT sugli organi federali era sì un tema, ma all'epoca non era stata affrontata la questione delle eccezioni a tale sorveglianza. 5

L'art. 2 cpv. 3 e 4 PD-LPD conteneva eccezioni alla sorveglianza dell'IFPDT per i tribunali federali (cpv. 3) e per il Consiglio federale e l'Assemblea federale (cpv. 4). L'eccezione relativa ai tribunali federali era motivata dal fatto che, secondo il progetto di LPD, l'IFPDT avrebbe acquisito la competenza di emanare decisioni nei confronti degli organi federali. Ciò avrebbe potuto compromettere l'indipendenza dei tribunali e la separazione dei poteri. Inoltre, il Tribunale amministrativo federale e il Tribunale federale sono autorità di ricorso contro le decisioni dell'IFPDT. Ciò avrebbe potuto comportare che questi due tribunali dovessero esaminare decisioni dell'IFPDT che li riguardavano direttamente. 6

Inoltre, secondo l'art. 2 cpv. 2 lett. c P-LPD, il trattamento di dati personali da parte di autorità giudiziarie federali indipendenti nell'ambito della loro attività giurisdizionale doveva essere escluso dall'ambito di applicazione della LPD e quindi anche dalla sorveglianza dell'IFPDT. Anche questa eccezione è stata motivata dal fatto che sottoporre tali autorità giudiziarie alla sorveglianza dell'IFPDT potrebbe compromettere il principio della separazione dei poteri e l'indipendenza della magistratura. 7

L'art. 2 cpv. 2 lett. c e gli art. 3 e 4 LPD sono stati discussi e criticati nel corso della procedura di consultazione. Tra le critiche mosse figuravano la mancanza di chiarezza di alcuni concetti («autorità giudiziarie indipendenti»), che le deroghe sarebbero in contrasto con la Convenzione SEV 108, che l'IFPDT dovrebbe continuare a esercitare la sorveglianza sui tribunali, ma che questi ultimi potrebbero solo formulare raccomandazioni o che le deroghe di cui all'art. 2 cpv. 3 e 4 LPER dovrebbero essere sistematicamente disciplinate nella sezione dedicata all'IFPDT e non in relazione al campo di applicazione materiale della LPD. 8

9 Le critiche formulate nella consultazione sul progetto di LPD sono state prese in considerazione nella misura in cui nel messaggio LPD 2017 è stato introdotto un nuovo art. 3 P-LPD che tratta esclusivamente della sorveglianza da parte dell'IFPDT. Con questa decisione, la questione della sorveglianza è stata separata da quella del campo d'applicazione materiale della LPD, il che è corretto dal punto di vista dogmatico. Il contenuto dell'articolo 3 L-LPD corrisponde senza differenze al nuovo articolo 4 LPD.

10 L'art. 3 P-LPD e l'art. 4 LPD non sono stati discussi in sede di deliberazione parlamentare. La proposta del Consiglio federale (art. 3 P-LPD) è stata invece approvata senza interventi.

II. SORVEGLIANZA DA PARTE DELL'IFPDT

A. Sorveglianza sull'applicazione delle disposizioni di diritto federale in materia di protezione dei dati (cpv. 1)

11 L'art. 4 cpv. 1 LPD stabilisce che l'IFPDT è incaricato di sorvegliare l'applicazione delle disposizioni di diritto federale in materia di protezione dei dati. Sono sottoposti alla sorveglianza dell'IFPDT le persone private, sia fisiche che giuridiche, nonché gli organi federali.

12 La formulazione «disposizioni di diritto federale in materia di protezione dei dati» sottolinea che l'IFPDT non sorveglia solo l'applicazione delle disposizioni della LPD. Come previsto dall'art. 27 cpv. 1 aDSG, l'IFPDT sorveglia anche le norme di protezione dei dati specifiche di settore della Confederazione ai sensi dell'art. 4 cpv. 1 LPD. Si intendono così le disposizioni rilevanti per la protezione dei dati contenute in altri atti normativi federali, nonché i trattati internazionali specifici in materia di protezione dei dati.

13 La questione della sorveglianza degli organi federali da parte dell'IFPDT va distinta dall'applicazione materiale della LPD al trattamento concreto dei dati da parte degli organi federali. Gli organi federali possono essere sottoposti alla sorveglianza dell'IFPDT anche se alcuni dei loro trattamenti di dati sono esclusi dal campo di applicazione della LPD ai sensi dell'articolo 2 LPD. Viceversa, taluni organi federali possono essere esclusi dalla sorveglianza dell'IFPDT (art. 4 cpv. 2 LPD), anche se i loro trattamenti di dati non sono esclusi dal campo d'applicazione materiale della LPD ai sensi dell'art. 2 LPD.

Ciò vale ad esempio per il Consiglio federale. Quest'ultimo è esonerato dalla sorveglianza dell'IFPDT ai sensi dell'art. 4 cpv. 2 lett. b LPD, ma deve comunque rispettare la LPD per determinati trattamenti di dati. Lo stesso vale per l'Assemblea federale. Quest'ultima è ora esonerata dalla sorveglianza. Ai sensi dell'art. 2 cpv. 2 lett. b LPD, anche determinati trattamenti di dati dell'Assemblea federale sono esclusi dal campo d'applicazione materiale della LPD, ma non tutti.

B. Eccezioni alla sorveglianza (cpv. 2)

1. Assemblea federale (lett. a)

L'Assemblea federale è esentata dalla sorveglianza dell'IFPDT, poiché altrimenti potrebbe essere compromesso il principio della separazione dei poteri. 14

Per quanto riguarda l'eccezione dell'Assemblea federale dalla sorveglianza dell'IFPDT, si pone la questione della portata di tale eccezione. I materiali non si pronunciano su questo punto. 15

Con riferimento all'art. 2 cpv. 2 lett. b LPD, si nota che il legislatore, quando menziona il Parlamento, distingue tra Assemblea federale, Consigli federali e commissioni parlamentari. Ciò depone a favore dell'interpretazione secondo cui con Assemblea federale si intende il collegio ai sensi dell'art. 148 Cost. Secondo l'art. 148 cpv. 2 Cost., l'Assemblea federale comprende il Consiglio nazionale e il Consiglio degli Stati. Pertanto, con Assemblea federale non si intende solo l'Assemblea federale riunita in seduta plenaria come organo specifico, ma anche il Consiglio nazionale, il Consiglio degli Stati e l'Assemblea federale riunita in seduta plenaria. 16

Non è chiaro se siano escluse dalla sorveglianza dell'IFPDT anche le commissioni parlamentari e i servizi parlamentari. Le deliberazioni delle commissioni parlamentari sono escluse dall'LPD (art. 2 cpv. 2 lett. b LPD). Questa eccezione vale tuttavia solo per le deliberazioni stesse e non, ad esempio, per i resoconti su tali deliberazioni e per le pubblicazioni. Alla luce della motivazione dell'eccezione prevista per l'Assemblea federale, è tuttavia opportuno escludere dalla sorveglianza dell'IFPDT anche le commissioni parlamentari. Per quanto riguarda i servizi parlamentari, è determinante se si tratta di trattamenti di dati direttamente connessi con l'attività parlamentare. I 17

trattamenti di dati che non sono direttamente connessi con l'attività parlamentare sono soggetti alla sorveglianza dell'IFPDT.

2. Consiglio federale (lett. b)

18 Secondo il messaggio, il Consiglio federale è stato esentato dalla sorveglianza dell'IFPDT perché altrimenti sarebbe stato compromesso il principio della separazione dei poteri.

19 Per Consiglio federale si intende il collegio. Sono invece soggetti alla sorveglianza dell'IFPDT i dipartimenti e la Cancelleria federale.

20 L'esclusione del Consiglio federale dalla sorveglianza dell'IFPDT era motivata all'art. 27 cpv. 1 aDSG dal fatto che l'organo di nomina del/della preposito/a non doveva essere sottoposto alla sua sorveglianza. Ora però il/la preposito/a è eletto/a dall'Assemblea federale riunita in riunioni delle Camere (art. 43 segg. LPD). L'art. 39 P-LPD prevedeva inoltre che il/la preposito/a fosse nominato/a dal Consiglio federale, con riserva di approvazione da parte dell'Assemblea federale. Pertanto, l'art. 3 cpv. 2 P-LPD escludeva dalla sorveglianza sia il Consiglio federale che l'Assemblea federale. Il Consiglio nazionale si è poi espresso a maggioranza a favore dell'elezione da parte dell'Assemblea federale riunita in seduta plenaria e non più da parte del Consiglio federale. Il Consiglio degli Stati si è allineato a questa decisione. Poiché il Consiglio federale non è più l'organo di elezione del/della delegato/a, non è chiaro perché il Consiglio federale debba continuare ad essere esentato dalla sorveglianza dell'IFPDT. Il fatto che il Consiglio federale continui ad essere esonerato dalla sorveglianza dell'IFPDT ai sensi dell'art. 4 cpv. 2 lett. b LPD è probabilmente dovuto al fatto che il Parlamento aveva approvato l'art. 3 P-LPD prima di occuparsi della nomina del/della delegato/a.

3. Tribunali federali (lett. c)

21 I tribunali federali sono esenti dalla sorveglianza dell'IFPDT, poiché altrimenti potrebbero essere compromesse la separazione dei poteri e l'indipendenza della magistratura. Ciò è dovuto al fatto che l'IFPDT è ora competente a emanare decisioni nei confronti degli organi federali (art. 51 LPD). Inoltre, il Tribunale amministrativo federale e il Tribunale federale sono le autorità di ricorso contro le decisioni dell'IFPDT. Senza l'eccezione alla sorveglianza, essi dovrebbero giudicare in qualità di autorità di ricorso le decisioni dell'IFPDT che li riguardano.

Per soddisfare i requisiti della direttiva (UE) 2016/680 e dell'E-SEV 108, i tribunali federali devono istituire una propria autorità di sorveglianza indipendente in materia di protezione dei dati. Tale autorità di controllo deve essere strutturata in modo analogo all'IFPDT, a meno che le circostanze concrete non richiedano deroghe. 22

4. Ministero pubblico della Confederazione (lett. d)

Il Ministero pubblico della Confederazione è escluso dalla sorveglianza dell'IFPDT solo quando tratta dati personali nell'ambito di procedimenti penali. Per altri trattamenti di dati (ad es. nel settore del personale), il Ministero pubblico della Confederazione è soggetto alla sorveglianza dell'IFPDT. Anche in questo caso l'ecceione è motivata dalla separazione dei poteri e dall'indipendenza della magistratura. 23

Restano soggette alla sorveglianza dell'IFPDT le autorità di polizia federali, anche quando agiscono su incarico del Ministero pubblico della Confederazione. L'IFPDT applica le disposizioni sulla protezione dei dati del diritto procedurale applicabile (art. 2 cpv. 3 LPD). 24

5. Autorità federali nell'esercizio della loro funzione giurisdizionale o nell'ambito di procedure di assistenza giudiziaria internazionale in materia penale (lett. e)

Anche questa eccezione è motivata dal principio della separazione dei poteri e dall'indipendenza della magistratura. 25

Inoltre, nei lavori legislativi l'eccezione è stata motivata dal fatto che i diritti delle parti e dei partecipanti al procedimento sono disciplinati dal diritto processuale, che offre loro una protezione equivalente a quella garantita dalla LPD. 26

Non sono invece contemplati dall'eccezione e quindi soggetti alla sorveglianza dell'IFPDT i trattamenti di dati che non hanno un nesso concreto con l'attività giurisdizionale o con procedure di assistenza giudiziaria internazionale in materia penale. Sono quindi soggetti alla sorveglianza dell'IFPDT i trattamenti di dati effettuati dai servizi amministrativi di queste autorità, come ad esempio il trattamento di dati relativi al personale. 27

28 Il concetto di «attività giurisdizionale» sostituisce quello di «procedimento pendente» di cui all'art. 2 cpv. 2 lett. c aDSG.

29 L'eccezione riguarda principalmente il Ministero pubblico della Confederazione e l'Ufficio federale di giustizia. Secondo la dichiarazione del Consiglio federale relativa all'articolo 1 della Convenzione europea di assistenza giudiziaria in materia penale del 20 aprile 1959, l'Ufficio federale di giustizia è da considerarsi un'autorità giudiziaria svizzera ai sensi della Convenzione. L'eccezione ha tuttavia portata limitata. L'IFPDT può verificare la legittimità di un trattamento di dati se una persona interessata fa valere i propri diritti ai sensi dell'articolo 11c E-AIMP.

30 I trattamenti di dati effettuati dalle autorità federali nell'ambito di un procedimento penale amministrativo non rientrano in questa deroga.

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 5 lett. d LPD

Un commentario di Hannes Meyle

CITAZIONE SUGGERITA

Hannes Meyle, Commentario all'art. 5 lett. d LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Meyle, art. 5 lett. d LPD N. XXX.

Capitolo 2: Disposizioni generali

Sezione 1: Definizioni e principi

Art. 5 Definizioni

Nella presente legge s'intende per:

d. *trattamento*: qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati, segnatamente la raccolta, la registrazione, la conservazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione, la cancellazione o la distruzione di dati;

STRUTTURA

I. Considerazioni generali 51
II. Trattamento come presupposto per l'applicazione della LPD 51
III. Forme di trattamento nominate 53
A. Acquisizione 53
B. Memorizzazione 54
C. Conservazione 54
D. Utilizzo 55
E. Modifica 55
F. Divulgazione 55
G. Archiviazione 55
H. Cancellazione o distruzione 56
Bibliografia 57

I. CONSIDERAZIONI GENERALI

Il concetto di trattamento deve essere inteso in senso molto ampio e comprende **qualsiasi trattamento** di dati personali - "in parole povere: tutto ciò che si fa con i dati personali". A titolo esemplificativo, l'art. 5 lett. d cita le forme di trattamento "raccolta, conservazione, utilizzo, modifica, comunicazione, archiviazione, cancellazione o distruzione". I termini "salvare" e "cancellare" sono stati aggiunti per avvicinare la formulazione dell'art. 5 lett. d LPD a quella dell'art. 4 n. 2 DSGVO. Tuttavia, in termini di contenuto, il concetto di elaborazione rimane invariato a seguito della revisione della legge. Il termine di raccolta dei dati secondo la legge precedente è stato incorporato nel termine di elaborazione. 1

Per «motivi di praticabilità» non è stato effettuato un completo allineamento terminologico al DSGVO. Così, mentre la LPD parla di *trattamento* o di *trattamento*, il DSGVO parla invece di *elaborazione | elaborazione*. Inoltre, gli esempi dell'art. 5 lett. d LPD differiscono chiaramente da quelli di cui all'art. 4 n. 2 DSGVO. Tuttavia, nonostante le differenze redazionali, i termini "*trattamento*" ai sensi della LPD e "*trattamento*" ai sensi del DSGVO devono essere intesi **come identici**. Nell'interpretazione del termine "trattamento" ai sensi dell'art. 5 lett. d LPD, la giurisprudenza relativa all'art. 4 n. 2 DSGVO può quindi essere utilizzata come riferimento in ogni caso. 2

Un principio fondamentale della LPD è il suo carattere tecnologicamente neutro. 3
Per questo motivo, per stabilire se si è in presenza di un trattamento, è **irrilevante quali mezzi e procedure** vengano utilizzati. I trattamenti ai sensi della LPD possono quindi essere sia manuali che automatizzati. Dal carattere tecnologicamente neutro deriva inoltre che la LPD copre o coprirà anche forme di trattamento future, non ancora note.

II. TRATTAMENTO COME PRESUPPOSTO PER L'APPLICAZIONE DELLA LPD

Il concetto di trattamento è di fondamentale importanza, poiché la LPD è applicabile solo se i dati personali vengono trattati da un'entità coinvolta nella gestione dei dati personali. Gli obblighi che ne derivano dipendono dal fatto che l'entità in questione sia (congiuntamente) responsabile o incaricata del 4

trattamento. Il trattamento presuppone un'azione che ha lo scopo e la conseguenza di fare qualcosa con i dati, o un'azione che **oggettivamente si riferisce ai dati**. Le azioni che riguardano solo indirettamente i dati, invece, non sono trattamenti, come il trasporto di passeggeri in autobus o in treno se questi passeggeri portano con sé dati personali memorizzati su supporti dati, ad esempio. È irrilevante se i dati personali in questione siano effettivamente noti a una persona o meno, motivo per cui è incluso anche il trattamento mediante programmi informatici. Il trattamento di dati personali in termini puramente mentali non è un trattamento ai sensi dell'art. 5 lett. d. Di conseguenza, le informazioni che sono presenti solo nella memoria di una persona non sono coperte dal diritto di accesso ai sensi della legge sulla protezione dei dati.

5 A volte, la **delimitazione del concetto di trattamento** o l'assegnazione di trattamenti di dati a determinate persone crea difficoltà, come dimostra il caso relativo alla conservazione di documenti deciso da un tribunale tedesco: a seguito di una procedura di insolvenza, una società immobiliare è diventata proprietaria di un immobile ospedaliero dismesso, in cui si trovavano cartelle cliniche. La proprietaria si oppose all'ordine delle autorità di conservare i documenti in un luogo particolarmente protetto. Il tribunale ha infine stabilito che non vi era alcun trattamento da parte della proprietaria, in quanto non aveva conservato lei stessa i documenti e non li aveva trattati in altro modo. Naturalmente, ciò non ha stabilito se un altro ente non abbia trattato o fatto trattare i dati in qualità di responsabile o incaricato del trattamento.

6 Recentemente, si pongono anche domande sulla portata del concetto di trattamento in relazione ai sistemi di IA. Il fatto che il trattamento delle informazioni - nella misura in cui sono personali - mediante sistemi di IA costituisca un trattamento è una conseguenza dell'ampio concetto di trattamento e della struttura tecnologicamente neutra della LPD. Al contrario, la delimitazione delle diverse operazioni di trattamento, come quelle che si verificano quando i sistemi di IA sono utilizzati in modo collaborativo, può essere meno chiara nei singoli casi. Questa delimitazione è rilevante perché ha un impatto su chi è responsabile del rispetto della legge sulla protezione dei dati (in particolare la salvaguardia dei diritti delle persone interessate) e di eventuali violazioni durante il trattamento. Il regolamento UE sull'intelligenza artificiale distingue tra i diversi ruoli degli attori, tra cui i fornitori e gli operatori di sistemi di IA, per definire i loro obblighi. Tali distinzioni non sono

ancora state stabilite nella legislazione sulla protezione dei dati. Tuttavia, sarebbe ovvio distinguere anche in questo caso tra la creazione di un sistema di IA (cioè l'addestramento che ne deriva, nella misura in cui sono coinvolti dati personali) e il suo utilizzo.

III. FORME DI TRATTAMENTO NOMINATE

L'elenco delle forme di trattamento nominate è **a titolo esemplificativo** e i termini si sovrappongono in parte. Solo ad alcune delle forme di trattamento nominate sono associate istruzioni specifiche, come ad esempio l'acquisizione, la divulgazione e la distruzione dei dati. Per il resto, i principi di trattamento previsti dalla legge sulla protezione dei dati devono essere rispettati per qualsiasi trattamento. Se un'attività non può essere attribuita a una forma di trattamento designata, è comunque possibile che si tratti di una forma di trattamento non designata (cfr. capitolo I). Le forme di trattamento designate sono quindi meno centrali per l'applicazione della LPD. 7

A. Acquisizione

Si ha acquisizione di dati quando l'ente che li acquisisce ne viene **volontariamente a conoscenza** o ne giustifica il possesso. Non si è in presenza di una raccolta se i dati vengono forniti dalla persona interessata stessa o da terzi senza richiesta e il destinatario dei dati non intende elaborarli (ad esempio, quando si riceve un'e-mail errata, si ascolta una conversazione, ecc. Al contrario, si è in presenza di una raccolta di dati personali quando l'ufficio in questione intende raccogliere dati in generale e accetta che ciò comporti anche dati personali. Ai sensi dell'art. 6 cpv. 3 LPD, la raccolta di dati può avvenire solo per uno scopo specifico e riconoscibile per la persona interessata e comporta l'obbligo di informazione ai sensi dell'art. 19 LPD. Esempi tipici di atti di acquisizione sono la raccolta di dati da altre fonti, la registrazione o la verbalizzazione di informazioni. È irrilevante se i dati siano protetti o liberamente disponibili. Pertanto, anche una ricerca mirata su Internet può rappresentare un'acquisizione di dati personali e portare all'applicabilità della LPD. Non è necessaria un'effettiva conoscenza del contenuto dei dati, ma è sufficiente che i dati entrino per la prima volta nella sfera di disponibilità di un responsabile. Pertanto, anche le forme automatizzate di raccolta dei dati, come il cosiddetto data scraping, sono considerate acquisizione ai sensi della LPD. I principi di cui sopra si applicano 8

anche in relazione ai sistemi di IA generativa: Se i dati personali vengono raccolti involontariamente, di norma non si è in presenza di una raccolta, e lo stesso vale se i dati personali esistenti vengono semplicemente modificati (ad esempio generando o elaborando un testo). Se, invece, i sistemi di IA generativa vengono utilizzati per ottenere informazioni aggiuntive su una persona o per inventarne di nuove, dal punto di vista della protezione dei dati si è regolarmente in presenza di una raccolta di dati.

B. Memorizzazione

9 Il termine "memorizzazione" è stato introdotto per **avvicinarsi** alla formulazione delle pertinenti fonti giuridiche europee, in particolare l'art. 4 n. 2 DSGVO. Secondo l'art. 4 n. 2 DSGVO, per archiviazione si intende la conservazione di dati in forma fisica su un supporto dati (disco rigido, server, chiavetta USB, ecc.) allo scopo di poterli elaborare ulteriormente in un secondo momento. A seconda dello scopo, anche la conservazione di informazioni in sistemi di IA può essere considerata archiviazione (vedi sopra n. 6).

10 L'**OPDa** fa riferimento al concetto di archiviazione in relazione ai requisiti di sicurezza dei dati (art. 3 cpv. 2 lett. b ed e OPDa) e all'obbligo di registrazione (art. 4 cpv. 2 e 3 OPDa).

C. Conservazione

11 La conservazione può essere descritta come l'attività attraverso la quale i dati sono mantenuti **disponibili nel contesto di elaborazione**. A differenza dell'archiviazione (vedi sotto n. 15), i dati conservati possono quindi essere ancora utilizzati. La conservazione è espressamente soggetta alla LPD come forma di trattamento, poiché anche in questa fase di elaborazione sono ancora possibili violazioni della personalità, ad esempio a causa di carenze nella protezione dei dati. La conservazione è trattata nell'art. 12 cpv. 2 lett. e LPD, secondo il quale il periodo di conservazione deve essere indicato nel registro delle elaborazioni, nonché nell'ambito del diritto di accesso ai sensi dell'art. 25 cpv. 2 lett. d LPD.

D. Utilizzo

Per utilizzo dei dati si intende qualsiasi attività volta a sfruttare il **contenuto informativo** dei dati (compresa la presa di conoscenza dei dati). L'utilizzo dei dati è menzionato nell'art. 5 lett. f LPD (profilazione), nell'art. 21 OPD (requisiti tecnici per l'attuazione della consegna dei dati) e nell'art. 4 cpv. 5 OPD (registrazione). Tuttavia, la LPD o l'OPDa non prevedono istruzioni specifiche per l'utilizzo dei dati. 12

E. Modifica

La modifica dei dati può essere descritta come un'"attività che modifica (**ristruttura nel contenuto**) il contenuto informativo dei dati personali". La LPD non prevede istruzioni particolari per l'azione, a parte il rispetto dei principi di elaborazione, o conseguenze giuridiche; la modifica dei dati è menzionata nell'art. 3 cpv. 3 lett. a OPDa (controllo dell'inserimento) e nell'art. 4 cpv. 2 e 3 OPDa (registrazione). 13

F. Divulgazione

La comunicazione dei dati, trattandosi di una **forma di trattamento particolarmente delicata**, è oggetto di una regolamentazione separata nell'OK-CN, art. 5 lett. e LPD. [Commento in corso di pubblicazione] 14

G. Archiviazione

L'archiviazione consiste nel **mantenere disponibili** i dati indipendentemente dal contesto di trattamento. A differenza della conservazione (vedi sopra n. 11), l'archiviazione comporta il prelievo dei dati dal contesto di trattamento precedente. Ne consegue che l'intensità dell'impatto sulla personalità delle persone interessate è tipicamente ridotta. Ciò si riflette nell'art. 32 cpv. 1 lett. b e nell'art. 41 cpv. 5 LPD, che limitano i diritti degli interessati in caso di trattamento a fini di archiviazione. Inoltre, l'art. 38 LPD (regolamentazione speciale per gli organi federali relativa alla messa a disposizione di determinati dati personali per l'Archivio federale) fa riferimento a scopi di archiviazione o all'archiviazione. 15

H. Cancellazione o distruzione

16 Il termine **"distruzione"** implica che i dati vengono distrutti in modo irreversibile. In caso di archiviazione fisica dei dati su carta, la carta dovrebbe essere bruciata o triturata. Nel caso di dati archiviati elettronicamente, il supporto dati corrispondente dovrebbe essere reso inutilizzabile e tutte le copie dovrebbero essere trattate in modo tale che i dati non siano più leggibili.

17 Il termine **«cancellazione»** è tipicamente utilizzato per il trattamento elettronico dei dati e, di conseguenza, ha un'applicazione meno ampia: per la cancellazione è generalmente sufficiente utilizzare i comandi di cancellazione del rispettivo programma, in modo che i dati non siano più riconoscibili nell'ambito delle normali procedure del programma e possano essere recuperati solo con mezzi sproporzionati. In altre parole, i dati personali sono cancellati quando non è più possibile stabilire un riferimento personale. Un'anonimizzazione efficace è quindi equivalente alla cancellazione o rappresenta un metodo di cancellazione dei dati personali. Parallelamente al concetto di dati personali, deve essere applicato il cosiddetto approccio relativo, il che significa che il punto di vista delle persone o delle entità che hanno accesso ai dati è determinante. Ne consegue però anche che, in singoli casi, può essere difficile valutare se i dati personali siano stati effettivamente cancellati, poiché dopo l'esecuzione degli ordini di cancellazione i dati rimangono nei sistemi e possono essere ripristinati in determinate circostanze. In questi casi, ci si chiede se il ripristino dei dati o l'accesso agli stessi richieda uno sforzo sproporzionato. Ciò può essere valutato solo caso per caso, a seconda delle circostanze tecniche, ma anche dell'interesse che terzi potrebbero avere nel ripristinare il riferimento personale.

18 La distinzione chiaramente stabilita nei materiali legislativi tra i termini cancellazione e distruzione non è **applicata in modo coerente** nella LPD. Ad esempio, l'art. 6 cpv. 4 LPD richiede che i dati siano «*distrutti* o resi anonimi non appena non sono più necessari per lo scopo del trattamento» – sarebbe corretto menzionare anche la cancellazione. Anche se la legge non utilizza i termini in modo coerente, per chiarezza è necessario assicurarsi che i termini cancellazione e distruzione non vengano scambiati accidentalmente nella redazione dei contratti, ad esempio nell'ambito dei contratti di elaborazione degli ordini. In particolare, occorre evitare che, invece di un obbligo di cancellazione, venga concordata per errore la distruzione dei dati,

poiché in caso di trattamento elettronico dei dati la distruzione potrebbe essere difficile da attuare o indesiderata (vedi sopra n. 16).

BIBLIOGRAFIA

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 5 lett. c LPD

Un commentario di Franziska Sprecher

CITAZIONE SUGGERITA

Franziska Sprecher, Commentario all'art. 5 lett. c LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Sprecher, art. 5 lett. c LPD N. XXX.

Capitolo 2: Disposizioni generali

Sezione 1: Definizioni e principi

Art. 5 Definizioni

Nella presente legge s'intende per:

c. *dati personali degni di particolare protezione*:

i dati concernenti le opinioni o attività religiose, filosofiche, politiche o sindacali,
i dati concernenti la salute, la sfera intima o l'appartenenza a una razza o a un'etnia,
i dati genetici,
i dati biometrici che identificano in modo univoco una persona fisica,
i dati concernenti perseguimenti e sanzioni amministrativi e penali,

i dati concernenti le misure d’assistenza sociale;

STRUTTURA

In breve 62
I. Informazioni generali 62
A. Scopo della norma e contesto 62
B. Cronistoria 63
II. Dati personali particolarmente sensibili in generale 63
III. Dati relativi a opinioni o attività religiose, ideologiche, politiche o sindacali (n. 1) 64
IV. Dati relativi alla salute, alla sfera intima o all'appartenenza a una razza o a un'etnia (n. 2) 65
V. Dati genetici (n. 3) 67
VI. Dati biometrici che identificano in modo univoco una persona fisica (n. 4) 68
VII. Dati relativi a procedimenti o sanzioni amministrativi e penali (n. 5) 70
VIII. Dati relativi a misure di assistenza sociale (n. 6) 70
Bibliografia 71
I materiali 73

IN BREVE

I dati personali particolarmente sensibili costituiscono una sottocategoria specifica dei dati personali il cui trattamento è soggetto a particolari esigenze di protezione a causa dell'elevato rischio di discriminazione o stigmatizzazione. Il loro trattamento è consentito solo a condizioni giuridiche rigorose, ad esempio in presenza di un consenso esplicito, dopo aver effettuato una valutazione d'impatto sulla protezione dei dati o sulla base di una legge formale in caso di trattamento da parte di un'autorità.

I. INFORMAZIONI GENERALI

1 I dati personali particolarmente sensibili costituiscono una **sottocategoria privilegiata dei dati personali** (art. 5 lett. a LPD). Sono classificati come particolarmente sensibili in considerazione della tutela dei diritti fondamentali e della personalità degli interessati (rischio di discriminazione o stigmatizzazione sulla base di queste caratteristiche) (cfr. N. 6 segg.). L'art. 5 lett. c LPD elenca in modo *esaustivo* le categorie di dati personali particolarmente sensibili. Fatte salve le disposizioni di leggi speciali, i dati personali particolarmente sensibili sono inclusi ovunque la legge faccia riferimento ai dati personali.

2 L'**ammissibilità del trattamento** di questo tipo privilegiato di dati personali è subordinata dal legislatore a condizioni particolari. Il legislatore impone infatti requisiti più severi per il consenso al trattamento di dati personali particolarmente sensibili. In particolare, il consenso deve essere *esplicito* (ad es. art. 6 cpv. 7 lett. a LPD). Esiste inoltre l'obbligo di effettuare una *valutazione d'impatto sulla protezione dei dati* (ad es. art. 22 cpv. 2 lett. a LPD). Per il trattamento di dati personali particolarmente sensibili, gli organi della Confederazione necessitano di una *base legale in senso formale* (art. 34 cpv. 2 lett. a LPD).

A. Scopo della norma e contesto

3 Con la creazione delle *categorie astratte e formali* dei dati personali particolarmente sensibili, il legislatore parte dal presupposto che esistono determinati tipi o categorie di dati che, a causa del loro stretto legame con la sfera privata o la vita privata di una persona, sono particolarmente sensibili.

La **sensibilità** di questi dati comporta un rischio particolare per i diritti della personalità delle persone interessate (ad es. rischio di stigmatizzazione a causa delle caratteristiche), il che rende questi dati particolarmente degni di protezione. Questa opinione è condivisa dalla LPD con la Convenzione ER 108+ (art. 6), dalla direttiva 2016/680 (art. 10) e dal DSGVO (art. 9).

B. Cronistoria

La categoria dei dati personali particolarmente sensibili era già contenuta nella aDSG (art. 3 lett. c aDSG) e, secondo la volontà del Consiglio federale, doveva essere mantenuta anche dopo la revisione totale della LPD. Nel quadro della revisione, il Consiglio federale ha ritenuto che la protezione dei «dati personali sensibili» fosse fondamentale «per il mantenimento della decisione di adeguatezza dell'UE» e ha sottolineato che «il catalogo del Consiglio federale [...] soddisfa quindi i requisiti minimi della Convenzione 108 plus sulla protezione dei dati e della direttiva UE relativa alla protezione dei dati in materia penale rilevante per Schengen». 4

I tentativi di ridurre il catalogo già esistente ai sensi dell'aDSG sono falliti nelle deliberazioni parlamentari (cfr. N. 12, N. 32). Nell'ambito della revisione totale della LPD, il concetto di dati personali particolarmente sensibili è stato esteso ai **dati genetici** e ai **dati biometrici** che identificano in modo univoco un individuo, nonché ai **dati relativi all'origine etnica**, allineando così la LPD all'art. 6 cpv. 1 ER-Conv-108+ e all'art. 10 della direttiva UE 2016/680. 5

II. DATI PERSONALI PARTICOLARMENTE SENSIBILI IN GENERALE

I dati personali particolarmente sensibili sono **formalmente e astrattamente categorizzati** nella LPD. Il legislatore parte dal presupposto che i dati personali definiti particolarmente sensibili nell'art. 5 lett. c LPD incidono in modo particolare sui diritti della personalità dell'interessato a causa della loro *sensibilità*, poiché provengono dalla sfera segreta o dalla vita privata della persona e/o possono influenzarne in modo significativo la reputazione. L'oggetto della classificazione come dati personali particolarmente sensibili non è l'esistenza di un pericolo specifico per la personalità o i diritti fondamentali, ma piuttosto il fatto che le informazioni in 6

questione riguardano un aspetto della vita che appartiene a uno dei settori protetti dalla legge.

7 Questo approccio, basato su una categorizzazione *definitiva*, formale e astratta, è *controverso*. Il pericolo per i diritti della personalità non deriva da determinati tipi di dati formali-giuridici, ma dal loro utilizzo per uno scopo specifico o in un contesto specifico, dall'entità del trattamento, ecc. (**contesto di utilizzo**). Occorre fare riferimento alla *effettiva sensibilità* dei dati in relazione alla protezione della personalità di una determinata persona interessata.

8 A ciò si aggiunge il fatto che i termini con cui sono definite in modo esaustivo le categorie di dati personali particolarmente sensibili sono **poco chiari** e la selezione appare statica, antiquata e incompleta. Sebbene questa critica fosse già stata sollevata ai tempi dell'aDSG, nella revisione totale è stata mantenuta la categorizzazione formale e astratta. *Rudin* sottolinea giustamente: «Non è il dato in sé, ma il suo utilizzo in un determinato contesto (il **contesto di utilizzo**) a costituire un pericolo.»

9 Dopo la revisione totale della LPD, i dati delle persone giuridiche non rientrano più nel campo di applicazione della legge. Di conseguenza, il concetto di dati personali (art. 5 lett. a LPD) e quindi anche quello di dati personali particolarmente sensibili (art. 5 lett. c LPD) si applica esclusivamente alle **persone fisiche**.

III. DATI RELATIVI A OPINIONI O ATTIVITÀ RELIGIOSE, IDEOLOGICHE, POLITICHE O SINDACALI (N. 1)

10 Ai sensi dell'art. 5 lett. c n. 1 LPD, i **dati relativi alle opinioni o alle attività religiose, ideologiche, politiche o sindacali** rientrano tra i dati personali particolarmente sensibili. La disposizione si riferisce inoltre all'appartenenza a corrispondenti associazioni. Il punto 1 comprende quindi in particolare i dati relativi alla confessione religiosa o alla denominazione di una persona, alla sua appartenenza a un partito o a un'organizzazione dei lavoratori, a una chiesa libera o a un'associazione che rappresenta una determinata posizione politica o ideologica (tra cui l'associazione massonica, le organizzazioni religiose giovanili). Per *Glass* non è chiaro fino a che punto debba essere interpretato il concetto di dati religiosi o ideologici. Per quanto riguarda la tutela della libertà di credo e di coscienza, sembra tuttavia plausibile registrare tutti i dati che

consentono di trarre conclusioni sul credo, sulla coscienza o sull'orientamento ideologico di una persona. La disposizione è stata ripresa senza modifiche dalla vecchia legge e corrisponde all'art. 3 lett. c n. 1 aDSG.

In considerazione delle conseguenze talvolta di vasta portata che può comportare il trattamento di dati personali particolarmente sensibili (N. 3), occorre verificare in ogni caso se il trattamento di tali dati sia effettivamente necessario e se non sia possibile rinunciarvi (ad esempio omettendo di inserire l'appartenenza religiosa nel fascicolo personale). 11

Nel quadro delle discussioni politiche sulla LPD, è stato tentato senza successo di eliminare le opinioni o le attività sindacali dall'elenco di cui all'art. 5 lett. c n. 1 LPD. 12

IV. DATI RELATIVI ALLA SALUTE, ALLA SFERA INTIMA O ALL'APPARTENENZA A UNA RAZZA O A UN'ETNIA (N. 2)

Ai sensi dell'art. 5 lett. c n. 2 LPD, anche i dati relativi alla salute, alla sfera intima o all'appartenenza a una razza o a un'etnia sono considerati dati personali particolarmente sensibili. 13

Secondo il messaggio relativo all'aDSG (messaggio del 1988), ai sensi del diritto precedente rientravano nei **dati sulla salute** tutte le informazioni che in senso lato costituivano un referto medico e «che potevano avere ripercussioni negative per le persone interessate». Alla luce dell'attuale concezione della salute e dei progressi medici e tecnologici, questa interpretazione (storica) dei dati sulla salute, in particolare il requisito dell'effetto negativo sulla salute, è troppo restrittiva. Inoltre, nella pratica, la caratteristica degli effetti negativi non viene quasi mai presa in considerazione. Oggi si deve quindi partire da una concezione più ampia dei dati sanitari. *Vokinger* mostra che in passato i dati sanitari derivavano principalmente dal rapporto medico-paziente. Oggi sono sempre più i pazienti stessi a raccogliere dati tramite app, dispositivi indossabili o social media. Anche aziende al di fuori del settore sanitario classico (Google, Amazon, Apple...) trattano sempre più spesso dati sanitari. Di conseguenza, questi non si limitano alle informazioni cliniche, ma comprendono sempre più spesso anche dati (genetici) che possono essere disponibili già prima di una manifestazione clinica. La classificazione di determinati dati come dati sanitari non deriva direttamente dai dati stessi, ma dipende in modo 14

determinante dal contesto di utilizzo. Dati identici, come il numero di passi effettuati ogni giorno, possono essere considerati dati relativi allo stile di vita di una persona sana, mentre nel caso di un paziente affetto, ad esempio, di diabete mellito o insufficienza cardiaca, assumono il carattere di dati sanitari.

15 Anche la DSGVO parte da una **definizione ampia di dati sanitari**: «I dati sanitari personali dovrebbero includere tutti i dati relativi allo stato di salute di una persona interessata e che forniscono informazioni sullo stato di salute fisico o mentale passato, presente e futuro della persona interessata».

16 Una concezione ampia dei dati sanitari è opportuna, poiché nell'assistenza sanitaria – in particolare sotto l'influenza delle tecnologie dell'informazione in rapida evoluzione – i confini tra terapia e stile di vita diventano sempre più permeabili (parole chiave: Real World Data e Real World Evidence). Di conseguenza, le informazioni sullo stato di salute di una persona non devono essere qualificate come dati sanitari ai sensi dell'art. 5 lett. c n. 2 LPD solo quando si riferiscono a uno stato di salute negativo. Allo stesso modo, a seconda del **contesto**, anche le informazioni relative al fatto che una persona *non* è affetta da una malattia o conduce un determinato stile di vita possono oggi costituire dati sanitari ai sensi dell'art. 5 lett. c n. 1 LPD. Anche l'*esattezza* di tali dati non è rilevante ai fini della classificazione come dati sanitari particolarmente sensibili, poiché proprio le informazioni inesatte (ad es. una diagnosi errata generata automaticamente da un'interpretazione errata dei dati o da una correlazione inesatta) possono mettere a rischio i diritti della personalità di una persona.

17 Il concetto di dati sanitari si ritrova anche nella LRUm. Nell'**art. 3 lett. f della Legge sulla ricerca sull'essere umano**, i *dati personali relativi alla salute* sono definiti come «informazioni su una persona identificata o identificabile che riguardano la sua salute o la sua malattia, compresi i suoi dati genetici». Secondo il messaggio relativo alla LRUm, i dati personali sono relativi alla salute se «presentano un nesso con una malattia fisica o psichica o forniscono informazioni sulla struttura e sul funzionamento del corpo della persona interessata». Secondo il messaggio relativo alla LRUm, il concetto di dati sanitari coincide con quello della LPD.

18 La **sfera intima** comprende i dati «che una persona comunica solo a pochi eletti e che rivestono per lei un grande significato emotivo». La sfera intima va oltre la vita sessuale, ma non si estende, ad esempio, alla situazione

finanziaria. Rientrano nella sfera intima, tra l'altro, le informazioni relative a terapie, paure o altri sentimenti, comportamenti di dipendenza, ecc. Il concetto di sfera intima si basa sulla «teoria delle tre sfere» del Tribunale federale, che distingue tra sfera intima o segreta, sfera privata e sfera comune o pubblica. La sfera intima comprende le questioni personali dell'interessato che in linea di principio devono rimanere sconosciute a terzi, a meno che non siano gli stessi interessati a divulgare le informazioni. Secondo il messaggio, l'identità sessuale di una persona può essere considerata, a seconda della situazione, sia come parte della sfera intima sia come dato relativo alla salute.

Anche nella versione riveduta, la LPD mantiene il concetto di **dati relativi all'appartenenza a una razza** nell'articolo 5 lettera c numero 2 LPD. Nel messaggio si sottolinea, con riferimento all'UE, che il mantenimento del concetto di appartenenza razziale non significa che il legislatore approvi la teoria razziale, che classifica le persone in una «razza» in base alle loro caratteristiche esteriori in modo valutativo e ideologico. Il mantenimento del termine è avvenuto principalmente in conformità con l'art. 6 cpv. 1 ER-Conv-108+, l'art. 10 della direttiva UE 2016/680 e l'art. 9 cpv. 1 DSGVO ed è stato accettato dal Parlamento senza discussioni. 19

Il concetto di appartenenza razziale di cui all'art. 5 lett. c n. 2 LPD è stato integrato, in occasione della revisione totale, con i **dati relativi all'appartenenza a un'etnia**. Ciò è avvenuto in conformità con l'art. 10 della direttiva (UE) 2016/680 e l'art. 9 cpv. 1 DSGVO. L'origine etnica si riferisce all'appartenenza a un gruppo di persone che, in base alla loro storia, lingua, costumi, cultura, tradizioni ecc., si sentono legate tra loro e si percepiscono come una comunità distinta dal resto della popolazione e/o percepita come diversa dal resto della popolazione. *Rudin* cita come esempio la denominazione «tamil» o «curdo». L'appartenenza etnica non è equiparabile alla nazionalità. In singoli casi (ad es. «serbi»), quest'ultima può coincidere con l'etnia. 20

V. DATI GENETICI (N. 3)

Dalla revisione totale della LPD, i **dati genetici** sono esplicitamente inclusi nei dati personali particolarmente sensibili ai sensi dell'articolo 5 lettera c LPD. I dati genetici sono *informazioni sul patrimonio genetico di una persona* ottenute mediante un esame genetico. Secondo il messaggio, il concetto di dati genetici nella LPD corrisponde alla definizione di cui all'art. 3 lett. l 21

aGUMG, che è stata ora ripresa nell'art. 3 lett. k GUMG. Secondo l'art. 3 lett. g LRUm, «i dati genetici sono informazioni ottenute mediante un esame genetico sulle caratteristiche ereditate o acquisite durante la fase embrionale».

22 I dati genetici possono essere ottenuti con un **esame genetico** da quasi tutti i tipi di materiale biologico (sangue, capelli, saliva, ecc.). Ai sensi dell'articolo 3 lettera a GUMG, gli esami genetici sono «esami citogenetici e di genetica molecolare volti a chiarire le caratteristiche del patrimonio genetico umano, nonché tutti gli altri esami di laboratorio che mirano direttamente a ottenere tali informazioni sul patrimonio genetico umano».

23 Rientrano nei dati genetici anche i **profili del DNA** ai sensi dell'articolo 3 lettera j LGD: un profilo del DNA indica «caratteristiche specifiche del patrimonio genetico di una persona, che vengono chiarite con un esame genetico e utilizzate per chiarire la sua discendenza o per identificarla».

24 Secondo *Rudin*, l'art. 5 lett. c n. 3 LPD si basa su una **concezione ampia** dei dati genetici. Sono quindi inclusi non solo i dati ottenuti dal sequenziamento di singoli genomi, ma anche, tra l'altro, le informazioni ottenute dall'uso di marcatori genetici (ad esempio in oncologia). Tuttavia, rientrano nel campo di applicazione della LPD e in particolare nella definizione di dati personali particolarmente sensibili solo i dati genetici che, ai sensi dell'art. 5 lett. a LPD, sono qualificabili come dati personali. Il materiale cellulare e i campioni biologici non costituiscono dati genetici fintantoché da essi non vengono ricavate informazioni sul patrimonio genetico delle persone interessate. A questo proposito, *Rudin* solleva giustamente la questione di sapere in che misura, allo stato attuale e futuro della scienza, «i dati genetici in un determinato contesto non consentano effettivamente di risalire a una persona specifica».

VI. DATI BIOMETRICI CHE IDENTIFICANO IN MODO UNIVOCO UNA PERSONA FISICA (N. 4)

25 In occasione della revisione totale della LPD, i **dati biometrici** sono stati inseriti nel catalogo dei dati personali particolarmente sensibili di cui all'art. 5 lett. c.

I dati biometrici sono **caratteristiche fisiche** che vengono registrate, misurate e documentate. Si tratta di dati personali «ottenuti mediante una procedura tecnica specifica dalle caratteristiche fisiche, fisiologiche o comportamentali di un individuo e che consentono di identificare in modo univoco la persona in questione o di confermarne l'identità». Essi possono essere modificati solo con grande sforzo (ad es. un intervento chirurgico). Tipicamente, le impronte digitali, i modelli delle vene della mano, le registrazioni della voce, le immagini del viso o dell'iride rientrano tra le caratteristiche biometriche. 26

L'utilizzo di dati biometrici comporta il rischio che il comportamento di una persona possa essere tracciato e che sia possibile creare un profilo completo o che si possano trarre conclusioni su dati personali particolarmente sensibili ai sensi dell'art. 3 lett. c aDSG. Inoltre, in caso di abuso, ad esempio attraverso la falsificazione dell'identità, i dati biometrici sono **compromessi in modo permanente**. Di conseguenza, già prima della revisione e dell'inserimento esplicito nel catalogo dei dati personali particolarmente sensibili, i dati biometrici potevano essere considerati dati particolarmente sensibili ai sensi dell'aDSG. 27

Non tutti i dati biometrici rientrano nella categoria dei dati personali particolarmente sensibili. Affinché i dati biometrici rientrino nell'ambito di applicazione dell'art. 5 lett. c n. 4 LPD, devono essere raccolti mediante una procedura tecnica speciale che consenta l'**identificazione univoca o l'autenticazione di una persona**. Per questo motivo, secondo il messaggio, non sono contemplate, ad esempio, le normali fotografie di una persona, dei volti o di semplici parti del corpo. A meno che non siano state elaborate con una procedura tecnica speciale che consente l'identificazione univoca della persona (ad es. software di riconoscimento facciale). Jacot-Guillarmod sottolinea che i moderni programmi di riconoscimento facciale potrebbero generare da normali fotografie un «modello biometrico» con cui riconoscere la persona raffigurata. Si chiede se abbia senso proteggere tale modello biometrico come dato sensibile senza estendere contemporaneamente la protezione alle foto da cui è stato ricavato il modello. 28

VII. DATI RELATIVI A PROCEDIMENTI O SANZIONI AMMINISTRATIVI E PENALI (N. 5)

29 Anche ai sensi dell'articolo 5 lettera c numero 5 LPD, i **dati relativi a procedimenti o sanzioni amministrativi e penali** continuano a essere classificati come dati personali particolarmente sensibili. Oltre ai procedimenti e alle sanzioni espressamente menzionati nel testo di legge, rientrano in questa disposizione anche i procedimenti disciplinari, le revoche della patente di guida e le misure di esecuzione penale. Ma anche le informazioni relative all'avvio, allo svolgimento e alla conclusione di procedimenti e revoche di autorizzazioni ecc., nonché le relative misure esecutive, rientrano nell'ambito di applicazione dell'art. 5 lett. c n. 5 LPD.

30 Affinché si tratti di dati personali particolarmente sensibili, devono essere **procedimenti o sanzioni di natura sovrana**. Non ha importanza se si tratta di sanzioni o procedimenti penali da parte di autorità svizzere o straniere.

VIII. DATI RELATIVI A MISURE DI ASSISTENZA SOCIALE (N. 6)

31 Rientrano nei dati personali particolarmente sensibili ai sensi dell'art. 5 lett. c n. 6 LPD i **dati relativi a misure di assistenza sociale**. Secondo il messaggio relativo all'art. 3 lett. c aDSG, tali dati comprendono «le prestazioni delle assicurazioni sociali in relazione a malattia e infortunio, nonché le misure di tutela e di assistenza sociale». In primo piano vi sono le prestazioni delle assicurazioni sociali, nella misura in cui consentono di trarre conclusioni sullo stato di salute (cfr. art. 5 lett. c n. 2 LPD). Le misure di assistenza sociale ai sensi dell'art. 5 lett. c n. 6 LPD comprendono, tra l'altro, anche informazioni sul ricorso ai servizi sociali, all'assicurazione contro la disoccupazione, nonché informazioni sulle prestazioni individuali dell'assistenza sociale, sulle misure di assistenza o di protezione dei minori e degli adulti, sul collocamento a scopo assistenziale e su altre prestazioni sociali subordinate al bisogno (riduzioni dei premi dell'assicurazione malattia, contributi per l'affitto, prestazioni complementari all'AVS/AI ecc.).

32 La maggioranza della Commissione delle istituzioni politiche del Consiglio nazionale voleva eliminare le misure di assistenza sociale dal catalogo dei dati personali particolarmente sensibili, il che avrebbe comportato un

indebolimento della protezione dei dati in questo settore, senza tuttavia creare una differenza rispetto alla Convenzione ER 108+ o alla direttiva (UE) 2016/680. La mozione è stata respinta dal Consiglio nazionale con una maggioranza di due terzi.

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 5 lit. f und g LPD

Un commentario di Matthias Glatthaar / Annika Schröder

CITAZIONE SUGGERITA

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

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

Capitolo 2: Disposizioni generali

Sezione 1: Definizioni e principi

Art. 5 Definizioni

Nella presente legge s'intende per:

f. *profilazione*: trattamento automatizzato di dati personali consistente nell'utilizzazione degli stessi per valutare determinati aspetti personali di una persona fisica, in particolare per analizzare o prevedere aspetti concernenti il rendimento professionale, la situazione economica, la salute, le preferenze, gli interessi, l'affidabilità, il comportamento, i luoghi di permanenza e gli spostamenti di tale persona;
g. *profilazione a rischio elevato*: profilazione che comporta un rischio elevato per la personalità o i diritti fondamentali della persona

interessata poiché comporta un collegamento tra dati che permette di valutare aspetti essenziali della personalità di una persona fisica;

STRUTTURA

In breve 78
I. Aspetti generali 78
A. Osservazione preliminare 78
B. Storia 79
C. Sistematica e delimitazione 79
II. Profilazione (lett. f) 80
A. Generale 80
B. Processo di valutazione 80
C. Automazione 81
D. Aspetti personali 82
E. Riferimento personale 83
III. Profilazione ad alto rischio (lett. g) 83
A. Generalità 83
B. Collegamento dei dati 84
C. Valutazione degli aspetti essenziali della personalità 85
D. Necessità di un approccio caso per caso 85
IV. Conseguenze legali 86
A. Profilazione normale 86
B. Profilazione ad alto rischio 87
V. Consigli pratici 89
Bibliografia 90
I Materiali 92

IN BREVE

Il concetto di profilo nella nuova LPD sostituisce il precedente concetto di profilo della personalità. Le disposizioni sulla profilazione sono state ampiamente discusse nelle delibere parlamentari e sono state una delle ragioni del lungo iter legislativo. La profilazione è definita come un trattamento automatizzato dei dati allo scopo di valutare aspetti personali. Tale profilazione è molto comune nella pratica, soprattutto nell'ambito della personalizzazione delle offerte, e non ha particolari conseguenze legali per i responsabili del trattamento dei dati privati. Oltre alla normale profilazione, la nuova LPD riconosce anche una forma qualificata di profilazione "ad alto rischio". L'LPD si discosta quindi dal DSGVO, che riconosce la profilazione qualificata solo in relazione alle decisioni individuali automatizzate. La profilazione ad alto rischio esiste se è possibile valutare aspetti essenziali della personalità collegando i dati. La classificazione come profilazione ad alto rischio dipende fortemente dal singolo caso e fa scattare l'obbligo di condurre una valutazione d'impatto sulla protezione dei dati, ma non comporta un obbligo generale di consenso.

I. ASPETTI GENERALI

A. Osservazione preliminare

1 La profilazione, intesa come valutazione automatizzata degli aspetti personali, è oggi una procedura ampiamente utilizzata, di grande importanza pratica soprattutto come base per la personalizzazione molto diffusa delle offerte nel settore dei clienti finali. I servizi digitali, come i servizi di streaming, i negozi online e le piattaforme di social media in particolare, hanno di solito così tanti "contenuti" che non potrebbero essere utilizzati in modo significativo senza una personalizzazione. Oggi i clienti danno per scontato che tali offerte digitali forniscano una guida mirata, ad esempio sulla base del comportamento di utilizzo precedente.

2 La profilazione è quindi un processo quotidiano che spesso è nell'interesse dei clienti. Tuttavia, poiché la profilazione comporta una valutazione solitamente automatizzata sulla base di correlazioni e probabilità, il processo è considerato rischioso e quindi necessita di una regolamentazione.

Profilazione significa sempre una valutazione generalizzata della personalità basata su determinate caratteristiche, che potrebbe non rendere giustizia alla persona specifica interessata ("pigeonholing"). La maggiore sensibilità della profilazione è particolarmente evidente quando si tratta di applicazioni al di fuori del settore dei consumatori, ad esempio l'uso da parte delle autorità nel settore della sicurezza e dell'applicazione della legge.

B. Storia

Il nuovo termine "profiling" introdotto con la revisione sostituisce il "profilo della personalità" della precedente LPD. Mentre il profilo di personalità descrive uno stato statico, il nuovo termine profiling si riferisce al processo di valutazione in quanto tale. Il concetto di profilo della personalità era una peculiarità svizzera e la sua sostituzione con il termine profiling lo allinea al diritto europeo (anche se il profilo della personalità è rinato mutatis mutandis sotto forma di "profiling ad alto rischio"). La nuova terminologia intende anche riflettere il progresso tecnico, ad esempio nei settori dei big data e dell'intelligenza artificiale, e le relative maggiori possibilità di trattamento dei dati. 3

La profilazione è stata uno dei principali punti di discussione del processo legislativo. Le divergenze sulla profilazione sono state uno dei principali fattori che hanno ritardato l'adozione della legge rivista. Si è discusso in particolare se e in che misura la profilazione debba richiedere il consenso. Nella bozza preliminare della LPD, la profilazione senza il consenso esplicito dell'interessato era ancora elencata tra le violazioni della personalità. Tuttavia, questo requisito del consenso è stato eliminato nel prosieguo del processo legislativo. Anche il diritto di opporsi alla profilazione, che era stato messo in discussione, non è stato accettato dal Parlamento. Anche i dettagli della definizione e in particolare il concetto di "profilazione ad alto rischio", creato solo durante le deliberazioni parlamentari e rimasto controverso fino alla fine, sono stati oggetto di discussione. 4

C. Sistematica e delimitazione

L'art. 5 LPD distingue due forme di profilazione: da un lato, nella lettera f, la profilazione "normale" come trattamento automatizzato dei dati allo scopo di valutare aspetti personali, e dall'altro, nella lettera g, la profilazione qualificata "ad alto rischio" basata sulla profilazione normale. Mentre la definizione di 5

profilazione normale è stata adottata senza modifiche dal DSGVO nella legge svizzera, la profilazione qualificata ad alto rischio è una creazione originale del legislatore svizzero. Con la gradazione, il legislatore ha voluto tenere conto del fatto che le varie applicazioni della profilazione differiscono, talvolta in modo considerevole, in termini di portata ed effetti.

6 La profilazione deve essere distinta dal processo decisionale individuale automatizzato ai sensi dell'art. 21 LPD. La profilazione è il processo di valutazione che può essere alla base di una decisione individuale automatizzata, ma è logicamente a monte di essa. La profilazione porta a una decisione individuale automatizzata solo se la valutazione si manifesta in un effetto esterno concreto e questo effetto esterno si manifesta sotto forma di una conseguenza legale o di una compromissione altrettanto drastica.

II. PROFILAZIONE (LETT. F)

A. Generale

7 Il cambiamento del concetto di profilazione della personalità in profilazione era finalizzato all'allineamento con il diritto europeo e il legislatore ha quindi adottato quasi alla lettera la definizione giuridica dell'art. 4 n. 4 del DSGVO nel diritto svizzero. Essenzialmente, comprende quattro elementi: in primo luogo, un processo di valutazione che, in secondo luogo, è automatizzato e, in terzo luogo, produce dichiarazioni su aspetti personali che, in quarto luogo, si riferiscono a una persona fisica. Questi elementi sono illustrati di seguito con l'esempio dei consigli di lettura personalizzati nelle librerie.

B. Processo di valutazione

8 Il concetto di profiling si concentra sull'elemento della valutazione. In sostanza, il profiling è un processo di valutazione in cui si ricavano nuove conoscenze su una persona attraverso l'analisi o la previsione. "Previsione" esprime il fatto che il profiling di solito mira a una considerazione orientata al futuro, ad esempio, nel caso del commercio di libri, a fare una previsione su quali libri i clienti potrebbero mettere nel loro carrello. L'"analisi", la seconda forma di valutazione menzionata nella definizione legale, invece, rappresenta una valutazione di aspetti passati o presenti, per cui l'analisi di solito non sta in piedi da sola, ma a sua volta costituisce la base per dichiarazioni previsionali.

Una valutazione include sempre una classificazione normativa ed è quindi soggettiva in una certa misura. Se non c'è un margine di giudizio soggettivo e si tratta solo della determinazione oggettiva di un fatto, non c'è valutazione. Il mero calcolo della posizione da parte di un sistema di navigazione, ad esempio, non contiene un elemento di valutazione più di quanto non lo contenga il mero reperimento, il filtraggio o l'ordinamento dei dati in un database. Se una libreria seleziona i suoi clienti in base a caratteristiche come l'età o il luogo di residenza e forma gruppi di clienti corrispondenti, non si tratta di profilazione. Anche se legge gli acquirenti di un certo autore dal suo database di clienti per attirare la loro attenzione su una nuova pubblicazione dello stesso autore, la libreria si limita a filtrare e non a profilare. Se invece il libraio assegna, ad esempio, gli acquirenti di "1984" di George Orwell al segmento di clientela "letteratura distopica", si tratta di una valutazione e quindi di profilazione. 9

C. Automazione

La profilazione ai sensi dell'art. 5 lett. f LPD riguarda solo il trattamento automatizzato dei dati personali. Il trattamento è automatizzato se viene effettuato con l'ausilio di tecniche assistite da computer. Non è automatizzato se la valutazione si basa esclusivamente su un processo di pensiero umano, ossia avviene solo "nella mente di un essere umano". 10

Se, ad esempio, una libraia conosce le preferenze dei suoi clienti e su questa base fa delle raccomandazioni individuali (ad esempio consiglia "Il racconto dell'ancella" di Margaret Atwood a un lettore di "1984"), non si tratta di profilazione ai sensi della legge perché non c'è automazione. Il fatto che il libraio annoti ogni cliente in un database elettronico non cambia la situazione. Se, invece, il libraio fa calcolare le raccomandazioni da un algoritmo, si tratta di un processo automatizzato e quindi costituisce una profilazione. In questo caso, l'automazione non è già annullata dal fatto che il libraio stesso definisca i criteri in una certa misura (ad esempio, assegna autori o libri a determinati generi), purché la valutazione sia assistita da un computer e non si limiti a semplici query "se-quindi". 11

La progettazione tecnica concreta del processo di profilazione non è decisiva. Il concetto di profilazione è neutro dal punto di vista tecnologico e la qualifica di profilazione è indipendente dalle procedure tecniche utilizzate. In pratica, i sistemi di raccomandazione delle offerte digitali, in particolare, sono spesso 12

basati sul cosiddetto "filtraggio collaborativo", in cui le preferenze e il comportamento di altri utenti vengono presi in considerazione in aggiunta alla cronologia e alle informazioni sui contenuti dell'utente stesso. Ad esempio, in una libreria online, se agli utenti A e B piacciono libri simili e l'utente A ha valutato positivamente un particolare libro che l'utente B non ha ancora acquistato, il sistema potrebbe consigliare quel libro all'utente B. Si tratta di un approccio molto utile al filtraggio. Tuttavia, l'uso di questi metodi basati sulla correlazione non è concettualmente essenziale.

D. Aspetti personali

13 Per costituire una profilazione, la valutazione deve portare a nuove conoscenze su aspetti personali delle persone fisiche. L'art. 5 lett. f LPD contiene un elenco di aspetti personali la cui valutazione può giustificare una profilazione: Prestazioni lavorative (ad es. rispetto degli standard di qualità o raggiungimento degli obiettivi di produttività), situazione economica (ad es. situazione reddituale o comportamento di risparmio), salute (ad es. abitudini alimentari o propensione al rischio di determinate malattie), preferenze personali (ad es. preferenze di investimento, generi preferiti o destinazioni di viaggio preferite), interessi (ad esempio, hobby o attività del tempo libero), affidabilità (ad esempio, affidabilità creditizia o tipi di personalità), comportamento (ad esempio, interazioni sociali o comportamento di acquisto), luogo o cambiamento di luogo (ad esempio, modelli di spostamento, percorsi a piedi o comportamento di mobilità).

14 L'elenco di cui all'art. 5 lett. f è molto completo, ma non esaustivo ("in particolare"), e a seconda del contesto possono essere rilevanti anche altri aspetti. L'elemento dell'aspetto della personalità non ha quindi quasi alcun effetto limitante. Ciò che è richiesto è che l'aspetto abbia una certa complessità e sia quindi suscettibile di valutazione nel senso di una valutazione soggettiva. Gli aspetti che non consentono discrezionalità e possono quindi essere determinati in modo puramente oggettivo non rientrano nel profiling (ad esempio, la determinazione del peso corporeo). Tuttavia, come dato futuro, gli stessi aspetti possono richiedere una valutazione (ad esempio, il peso corporeo futuro previsto). Inoltre, gli aspetti puramente oggettivi possono servire come base di dati per la valutazione di altri aspetti discrezionali (ad esempio, il peso corporeo come indicatore di determinati rischi di malattia).

E. Riferimento personale

La profilazione in senso giuridico richiede che le affermazioni fatte si riferiscano a singole persone. Se, invece, le affermazioni si riferiscono solo a gruppi di persone da cui non si possono determinare persone singole, non si ha profilazione, anche se il trattamento si basa su dati personali come "input". Se, ad esempio, una libreria si limita ad analizzare quali autori e generi sono più popolari nelle varie fasce d'età per ottimizzare l'assortimento, senza fare dichiarazioni sui singoli clienti, non sta effettuando una profilazione. Lo stesso vale per l'analisi dell'utilizzo di un sito web allo scopo di migliorare la facilità d'uso, dove non viene effettuata alcuna valutazione personale. 15

Non c'è profilazione nemmeno se il trattamento si basa solo su dati anonimi o aggregati, vale a dire che i "dati di input" in sé non hanno alcun riferimento personale. Non si tratta di un trattamento di dati personali e la legge sulla protezione dei dati non è applicabile (art. 2 cpv. 1 LPD). Tuttavia, se lo scopo del trattamento è quello di deanonimizzare i dati, di per sé anonimi, e di (ri)attribuirli a singole persone, si tratta nuovamente di un trattamento di dati personali soggetto alla legge sulla protezione dei dati. In questo caso, può essere coinvolta la profilazione, il cui scopo è proprio quello di deanonimizzare i dati stabilendo connessioni. 16

III. PROFILAZIONE AD ALTO RISCHIO (LETT. G)

A. Generalità

Con la "profilazione ad alto rischio", l'art. 5 lett. g LPD introduce una forma qualificata di profilazione basata sulla normale profilazione. Il concetto giuridico di "profiling ad alto rischio" è stato creato per la prima volta nel processo legislativo ed è stato oggetto di un intenso dibattito in Parlamento. Tra l'altro, sono state discusse formulazioni che si sarebbero basate sul fatto che la profilazione produce dati personali particolarmente meritevoli di protezione, o sul fatto che la profilazione si estende a varie aree della vita dell'interessato. Infine, è prevalso l'approccio di adottare il precedente concetto giuridico di "profilo della personalità" in termini di contenuto, anche se non di nome. La profilazione ad alto rischio è essenzialmente una profilazione che porta a un profilo della personalità secondo la precedente 17

LPD. Il profilo della personalità è stato abolito solo superficialmente con la nuova LPD.

18 La profilazione ad alto rischio è una specialità svizzera. Il DSGVO non riconosce tale forma qualificata di profilazione e fa dipendere le conseguenze legali speciali in caso di profilazione dal fatto che essa avvenga in connessione con una decisione individuale automatizzata. Si sarebbe potuto ottenere un maggiore allineamento con il DSGVO se il criterio per la "profilazione ad alto rischio" fosse stato definito come se la profilazione avesse effetti legali sull'interessato o lo riguardasse in modo significativo. Il fatto che invece sia stato riproposto il precedente profilo della personalità e sia stata perpetuata una peculiarità svizzera è deplorevole. Si è persa un'occasione per creare una maggiore convergenza con il DSGVO.

19 Affinché si possa parlare di "profilazione ad alto rischio" ai sensi dell'art. 5 lett. g LPD, oltre alla normale profilazione devono essere presenti due elementi: in primo luogo, un collegamento di dati e, in secondo luogo, aspetti essenziali della personalità a cui si riferiscono potenzialmente le dichiarazioni generate dalla profilazione. I due elementi aggiuntivi sono necessari e sufficienti. Ciò significa, innanzitutto, che si presume che il rischio elevato eponimo esista se sono presenti i due elementi citati. Il rischio elevato non costituisce un elemento concettuale aggiuntivo che deve essere esaminato separatamente in ogni singolo caso. Inoltre, ciò significa che la profilazione che non soddisfa la definizione legale non diventa "profilazione ad alto rischio" perché presenta un rischio elevato per gli interessati nel caso specifico per altri motivi (e quindi richiede, ad esempio, la realizzazione di una valutazione d'impatto sulla protezione dei dati).

B. Collegamento dei dati

20 La profilazione ad alto rischio richiede innanzitutto il collegamento dei dati. Per collegamento dei dati si intende il processo di collegamento, fusione o abbinamento di due o più serie separate di dati al fine di ottenere una comprensione più profonda o più ampia. Il collegamento dei dati può essere effettuato in vari modi, ad esempio unendo dati provenienti da fonti diverse che si riferiscono allo stesso individuo o collegando i dati in base a caratteristiche, criteri o variabili comuni.

Il collegamento dei dati sostituisce il precedente termine giuridico "compilazione di dati" ed esprime quindi il fatto che la profilazione non è una semplice raccolta di dati, ma un collegamento mirato di diverse serie di dati. Una semplice raccolta di dati, eventualmente anche per la preparazione di un profilo, non costituisce ancora un collegamento di questo tipo. A differenza del precedente profilo di personalità, una raccolta statica di dati non è sufficiente. 21

C. Valutazione degli aspetti essenziali della personalità

Mentre nel profilo normale sono sufficienti i risultati relativi a qualsiasi aspetto della personalità, nel profilo ad alto rischio devono riguardare gli aspetti essenziali della personalità. Non è necessario che tali tratti essenziali della personalità siano effettivamente valutati. È sufficiente che le dichiarazioni su aspetti essenziali della personalità siano in linea di principio possibili ("consentite") sulla base dei dati trattati e delle modalità della procedura di trattamento. Non è rilevante che l'art. 5 lett. g LPD utilizzi il termine "valutazione" invece di "valutare". I due termini vanno intesi come sinonimi. 22

Secondo la volontà del legislatore, la giurisprudenza "Moneyhouse" del Tribunale amministrativo federale sulla profilazione della personalità dovrebbe continuare a essere la linea guida per determinare quando esiste una valutazione di aspetti essenziali della personalità. Il fattore decisivo è quindi se le informazioni collegate sono condensate in un quadro completo della persona interessata. Criteri essenziali sono la quantità e il tipo di dati utilizzati, il contesto del loro utilizzo e la dimensione temporale, ossia se i dati personali sono raccolti in un periodo di tempo più lungo e quindi forniscono un quadro quasi biografico mostrando un'evoluzione della persona interessata. In questo contesto, anche dati banali possono, attraverso un collegamento sistematico, fornire un quadro generale della persona e trasmettere informazioni potenzialmente sensibili sulla sua identità, sulle sue attività o sulle sue preferenze. 23

D. Necessità di un approccio caso per caso

Come nel caso della profilazione della personalità in passato, la profilazione ad alto rischio nel suo complesso rimane sfuggente. I due elementi concettuali del collegamento dei dati e della valutazione degli aspetti essenziali della 24

personalità forniscono un quadro di base, ma non sono in grado di dare al concetto contorni chiari e richiedono una classificazione caso per caso. Il fatto che alla fine si tratti di una valutazione caso per caso è stato riconosciuto anche dal Tribunale amministrativo federale nella sua giurisprudenza sui profili di personalità. In un certo senso, "lo riconosci quando lo vedi".

25 Nell'esempio del commercio librario, ad esempio, si ipotizzerebbe una profilazione ad alto rischio se i dati sul comportamento di lettura venissero combinati con il comportamento di acquisto di generi alimentari ed eventualmente con altri dati relativi alle transazioni, nonché, ad esempio, con i dati delle app di fitness tracking, al fine di trarre conclusioni sullo stato di salute e di fornire alle persone interessate pubblicità per offerte sanitarie corrispondenti o addirittura per calcolare i premi assicurativi individuali. Si potrebbe parlare di profilazione ad alto rischio anche se il comportamento di lettura fosse collegato ai dati sul comportamento di navigazione e ai dati di geolocalizzazione per ottenere informazioni sulle opinioni ideologiche o sulle credenze religiose. Si potrebbe parlare di profilazione ad alto rischio anche nel caso in cui il comportamento di lettura fosse collegato ai dati delle carte di credito e alle informazioni provenienti dalle piattaforme di networking professionale, al fine di ricavare informazioni sul patrimonio e sulla capacità di pagamento e, in base a ciò, decidere quali prodotti e servizi offrire agli interessati, come e a quali prezzi.

IV. CONSEGUENZE LEGALI

A. Profilazione normale

26 La profilazione normale, vale a dire la profilazione senza "rischio elevato", è in linea di principio rilevante solo per gli organi federali ai sensi della LPD (per cui anche i privati incaricati di compiti pubblici sono considerati organi federali). In primo luogo, esiste una base giuridica sufficiente per la creazione di profili da parte di un organismo federale solo se il profilo è previsto da una legge in senso formale (art. 34 cpv. 2 lett. b LPD). Se non esiste una base giuridica in senso formale e la profilazione si basa sul consenso, questo è valido solo se è esplicito, ossia se fa riferimento alla profilazione in quanto tale (art. 6 cpv. 7 lett. c LPD).

27 Per contro, la normale profilazione non ha particolari conseguenze giuridiche per i responsabili del trattamento privati e si applicano le regole consuete. In

particolare, la profilazione deve essere resa sufficientemente trasparente e gli interessati devono essere informati sulle categorie di dati creati mediante la profilazione (ad esempio, i dati sulle preferenze) (art. 19 cpv. 3 LPD). Tuttavia, la profilazione in sé non deve essere specificamente menzionata o descritta nella dichiarazione sulla protezione dei dati. Solo se le decisioni essenziali sono completamente automatizzate sulla base della profilazione, vi sono obblighi speciali di informazione e divulgazione (art. 21 e art. 25 cpv. 2 lett. f LPD).

Come qualsiasi altro trattamento dei dati, anche la profilazione può richiedere una valutazione d'impatto sulla protezione dei dati se comporta rischi elevati per gli interessati. L'esistenza di rischi elevati deve essere determinata in ogni singolo caso sulla base delle circostanze specifiche e può verificarsi anche se la profilazione non si qualifica come profilazione "ad alto rischio" ai sensi dell'art. 5 lett. g LPD a causa della mancanza di elementi concettuali. 28

Anche nel caso della profilazione, il consenso è necessario solo se vi è una violazione dei principi del trattamento e se non esistono altre giustificazioni per il trattamento dei dati. Sotto questo aspetto, la profilazione non differisce dal "normale" trattamento dei dati. Il tanto discusso requisito del consenso per la profilazione, che era ancora incluso nella bozza preliminare, non è sopravvissuto al processo legislativo. 29

Il DSGVO, inoltre, non prevede conseguenze giuridiche specifiche in caso di profilazione, o solo se la profilazione viene effettuata in relazione a una decisione individuale automatizzata. Senza riferimento al processo decisionale automatizzato, la profilazione è menzionata solo nell'articolo 21, paragrafi 1 e 2, del DSGVO, ma solo a titolo di esempio, poiché la profilazione, come qualsiasi altro tipo di trattamento, sarebbe anche coperta dal diritto di opposizione senza menzione specifica. Si noti inoltre che, nell'ambito di applicazione del DSGVO, qualsiasi trattamento dei dati e quindi anche qualsiasi profilazione deve basarsi su una base giuridica. Tuttavia, le basi giuridiche disponibili non sono limitate e tutte le possibili basi giuridiche dell'art. 6(1) del DSGVO sono disponibili anche per la profilazione. 30

B. Profilazione ad alto rischio

L'intensità con cui sono stati condotti i dibattiti sulla profilazione ad alto rischio contrasta con la scarsa rilevanza giuridica di questa figura giuridica. La 31

nuova LPD prevede solo tre conseguenze legali legate alla profilazione ad alto rischio.

32 In primo luogo, qualsiasi profilazione ad alto rischio deve essere soggetta a una valutazione obbligatoria dell'impatto sulla protezione dei dati, che valuta sistematicamente i rischi per gli interessati e definisce le misure correttive, se necessario. È vero che l'articolo 22 cpv. 2 della LPD non menziona esplicitamente la profilazione ad alto rischio come causa dell'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati. Tuttavia, per definizione si ritiene che la profilazione ad alto rischio comporti un rischio elevato per gli interessati e, ai sensi dell'articolo 22 cpv. 1 LPD, una valutazione d'impatto sulla protezione dei dati è obbligatoria per qualsiasi trattamento che comporti un rischio così elevato. Tuttavia, il "rischio elevato" si riferisce solo al rischio iniziale che determina l'esecuzione di una valutazione d'impatto sulla protezione dei dati. Nell'ambito di tale valutazione, il responsabile del trattamento può concludere che il rischio effettivo nel caso specifico non è elevato o, dopo aver preso in considerazione le misure correttive previste, non è più da classificare come elevato. La profilazione in tale costellazione rimane una "profilazione ad alto rischio" secondo la definizione legale, ma deve essere successivamente trattata come un trattamento di dati senza rischio elevato.

33 In secondo luogo, se i controllori privati effettuano una profilazione ad alto rischio e la basano in primo luogo sul consenso, il consenso concesso in relazione alla profilazione deve essere esplicito ai sensi dell'articolo 6 cpv. 7 lett. b LPD. L'art. 6 cpv. 7 lett. b LPD stabilisce i requisiti per la concessione di un consenso valido, ma non stabilisce un requisito generale di consenso per la profilazione ad alto rischio. Come la profilazione normale, quella ad alto rischio richiede il consenso solo se viene violato un principio di trattamento e non esistono altre giustificazioni.

34 In terzo luogo, e infine, l'interesse prevalente nei controlli del credito non si applica se il controllo si basa su una profilazione ad alto rischio (art. 31 cpv. 2, let. c ch. 1 LPD).

35 Come spiegato, il DSGVO non riconosce la profilazione ad alto rischio, ma prevede alcune conseguenze legali speciali se la profilazione è in connessione con una decisione completamente automatizzata che ha effetti legali per l'interessato o lo riguarda in modo significativo. Tra l'altro, in tali costellazioni

qualificate, il DSGVO richiede anche l'esecuzione di una valutazione d'impatto sulla protezione dei dati (art. 35 (3) (a) DSGVO). Poiché decisioni di così grande importanza vengono prese raramente nella pratica commerciale, la soglia per l'esecuzione obbligatoria di una valutazione d'impatto sulla protezione dei dati in caso di profilazione è piuttosto alta ai sensi del DSGVO rispetto alla LPD svizzera. Il DSGVO prevede anche ulteriori conseguenze legali per la profilazione effettuata in combinazione con una decisione individuale automatizzata, tra cui un obbligo esteso di informazione e divulgazione, che comprende anche informazioni sulla logica coinvolta e sugli effetti per gli interessati.

V. CONSIGLI PRATICI

Nella prassi aziendale, l'identificazione della profilazione ad alto rischio è particolarmente significativa, poiché solo per i responsabili del trattamento privati tali operazioni di profilazione sono soggette a specifiche conseguenze giuridiche, prima fra tutte l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati. Il raggiungimento o meno della soglia per la profilazione ad alto rischio, tuttavia, dipende fortemente dalle circostanze specifiche della profilazione nel singolo caso. Non è quindi facile rendere operativo il concetto di profilazione ad alto rischio e definire criteri generali. Inoltre, le attività di profilazione che non si qualificano come "profilazione ad alto rischio" secondo la definizione legale possono anche comportare un rischio elevato in singoli casi e possono quindi richiedere una valutazione d'impatto sulla protezione dei dati. 36

È opportuno non applicare criteri troppo dettagliati per verificare se sia necessario effettuare una valutazione d'impatto sulla protezione dei dati (la cosiddetta analisi della soglia). È più efficace integrare in generale la valutazione degli aspetti personali come fattore di rischio nei processi di revisione e approvazione dei progetti e, in una seconda fase, verificare sulla base delle circostanze concrete se è presente una profilazione ad alto rischio secondo la definizione legale o una profilazione che comporta un rischio elevato per gli interessati per altri motivi. Da un punto di vista pratico, è sempre consigliabile effettuare una valutazione d'impatto sulla protezione dei dati se la profilazione raggiunge una certa intensità o se a tale scopo vengono collegati dati provenienti da fonti diverse. 37

38 La profilazione ha anche implicazioni per la progettazione e l'attuazione dei processi di governance della protezione dei dati. La profilazione è particolarmente rilevante per l'attuazione dei processi informativi: sia i dati personali ("input") che confluiscono nella profilazione, sia i nuovi dati e i risultati creati con l'aiuto della profilazione ("output") dovrebbero far parte delle informazioni fornite agli interessati in modo adeguato e comprensibile. Le categorie di dati trattati o creati ex novo in relazione alla profilazione e le finalità di trattamento perseguite con la profilazione devono essere descritte nell'informativa sulla privacy. La profilazione in sé, tuttavia, non deve essere menzionata specificamente nell'informativa sulla privacy. Tuttavia, una spiegazione della profilazione può essere consigliabile come misura di rafforzamento della fiducia ai fini della trasparenza. Il trattamento dei dati in relazione alla profilazione deve essere documentato con le informazioni necessarie nell'elenco dei trattamenti ai sensi dell'art. 12 LPD.

39 Infine, è buona prassi fornire agli interessati la possibilità di opporsi alla profilazione. In pratica, tali possibilità di opt-out possono essere implementate, ad esempio, attraverso funzionalità tecniche con cui gli interessati possono disattivare o impedire autonomamente il trattamento dei dati o i servizi connessi alla profilazione - ad esempio, la ricezione di misure di marketing diretto personalizzato. Tali possibilità di opt-out rendono operativo il diritto generale di opposizione di cui all'art. 30 cpv. 2 lett. b LPD e tengono conto anche dell'idea di "privacy by design". Tali opzioni di opt-out soddisfano inoltre sempre più le aspettative dei clienti di poter influenzare il trattamento dei loro dati in modo pertinente.

BIBLIOGRAFIA

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).

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 6 cpv. 3-5 LPD

Un commentario di Caroline Gaul

CITAZIONE SUGGERITA

Caroline Gaul, Commentario all'art. 6 cpv. 3-5 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Gaul, Art. 6 cpv. 3-5 LPD N. XXX.

Art. 6 Principi

[...]

[3] I dati personali possono essere raccolti soltanto per uno scopo determinato e riconoscibile per la persona interessata; possono essere trattati ulteriormente soltanto in modo compatibile con tale scopo.

[4] I dati personali sono distrutti o resi anonimi appena non sono più necessari per lo scopo del trattamento.

[5] Chi tratta dati personali deve accertarsi della loro esattezza. Deve prendere tutte le misure adeguate per rettificare, cancellare o distruggere i dati inesatti o incompleti rispetto allo scopo per il quale sono stati raccolti o trattati. L'adeguatezza delle misure dipende segnatamente dal tipo e dall'entità del trattamento dei dati come pure

dai rischi derivanti dal trattamento per la personalità o i diritti fondamentali della persona interessata.

STRUTTURA

In breve 96
I. Considerazioni generali 96
A. Osservazioni preliminari 96
B. Contesto e scopo della norma 97
C. Destinatario degli obblighi 98
D. Conseguenze giuridiche ed economiche di una violazione 98
E. Storia dell'origine dei singoli principi di trattamento 99
1. Principio della limitazione delle finalità e della trasparenza, art. 6 cpv. 3 LPD . 99
2. Limitazione temporale del trattamento dei dati, art. 6 cpv. 4 LPD 99
3. Principio di esattezza, art. 6 cpv. 5 LPD 100
II. Oggetto delle disposizioni 100
A. Principio della limitazione delle finalità e della trasparenza, art. 6 cpv. 3 LPD .. 100
1. Requisiti 100
2. Esempi 101
3. Raccomandazioni per l'attuazione 105
B. Limitazione temporale del trattamento dei dati, art. 6 cpv. 4 LPD 105
1. Requisiti 105
2. Raccomandazioni per l'attuazione 107
C. Principio di correttezza, art. 6 cpv. 5 LPD 107
1. Correttezza dei dati 107
a. Requisiti 107
b. Esempi 109
2. Obbligo di accertamento, obbligo di rettifica e cancellazione 110
a. Requisiti 110
b. Esempi 111
3. Raccomandazioni per l'attuazione 111
Bibliografia 112
I Materiali 113

IN BREVE

Le disposizioni dell'art. 6 cpv. 3 LPD (**limitazione delle finalità e trasparenza**), dell'art. 6 cpv. 4 LPD (**limitazione temporale del trattamento dei dati**) e dell'art. 6 cpv. 5 LPD (**esattezza**) fanno parte dei cosiddetti **principi di trattamento**, i principi materiali più importanti della legge sulla protezione dei dati. Sono essenziali per la configurazione concreta del trattamento dei dati.

Una violazione dei principi di trattamento costituisce una violazione dei diritti della personalità delle persone interessate. Tuttavia, la violazione della personalità può essere giustificata da un consenso, da un interesse privato o pubblico preponderante o dalla legge nel caso di responsabili del trattamento dei dati privati. Questa differenza sostanziale rispetto al DSGVO dell'UE, in base al quale ogni trattamento dei dati richiede una base giuridica concreta, è stata mantenuta anche nella nuova LPD.

Una violazione dei principi di trattamento qui trattati non è soggetta a sanzioni pecuniarie ai sensi della LPD, a differenza di quanto previsto dal DSGVO dell'UE, ma può avere conseguenze di vasta portata, soprattutto alla luce dei poteri ampliati del Commissario federale per la protezione dei dati (IFPDT) con la nuova LPD. Quest'ultimo può ordinare che il trattamento dei dati sia modificato, interrotto o addirittura interrotto in tutto o in parte e che i dati personali siano distrutti in tutto o in parte. Inoltre, si dovrebbe tener conto delle possibili rivendicazioni legali (di diritto civile) delle persone interessate e, in particolare, delle conseguenze di una **perdita di fiducia** e di un **danno alla reputazione**.

I. CONSIDERAZIONI GENERALI

A. Osservazioni preliminari

1 Le disposizioni dell'art. 6 cpv. 3 LPD (**limitazione delle finalità e trasparenza**), dell'art. 6 cpv. 4 LPD (**limitazione temporale del trattamento dei dati**) e dell'art. 6 cpv. 5 LPD (**esattezza**) fanno parte, insieme all'art. 6 cpv. 1 LPD (liceità), all'art. 6 cpv. 2 (proporzionalità e buona fede) e art. 8 LPD (sicurezza dei dati) sono i cosiddetti **principi di trattamento**, i principi materiali più importanti della protezione dei dati e le

idee guida della legge. Gli articoli 6 cpv. 6 e cpv. 7 LPD (consenso) non sono principi di trattamento, ma spiegano semplicemente i requisiti del consenso.

I principi di trattamento della LPD si applicano sia ai responsabili del trattamento dei dati privati che agli organi federali. Una violazione dei principi di trattamento costituisce una **violazione della personalità**. Tuttavia, nel caso dei responsabili del trattamento dei dati privati, non tutte le violazioni della personalità sono illegali. Piuttosto, possono essere giustificate dal consenso della persona interessata, da un interesse privato o pubblico preponderante o dalla legge (art. 31 cpv. 1 LPD). Questa differenza sostanziale rispetto al DSGVO dell'UE, in base al quale ogni trattamento dei dati richiede una giustificazione (divieto con riserva di autorizzazione), è stata mantenuta nel corso della revisione della LPD. Secondo la legge svizzera sulla protezione dei dati, i responsabili del trattamento dei dati privati continueranno quindi a richiedere una base giuridica solo in caso di violazione della personalità. Per il trattamento dei dati da parte delle autorità federali, a differenza del trattamento da parte di privati, anche secondo la legge svizzera sulla protezione dei dati è necessaria una base giuridica (divieto con riserva di autorizzazione). Anche se e nella misura in cui tale base giuridica esiste, si applicano in linea di principio anche i principi di trattamento. Essi costituiscono norme di comportamento direttamente applicabili, la cui violazione può essere perseguita legalmente dalla persona interessata. Se e in che misura le autorità federali sono esentate in via eccezionale dal rispetto dei principi di trattamento deve essere determinato sulla base della legge. 2

I principi del trattamento dei dati si applicano all'intero ciclo di vita del trattamento dei dati, indipendentemente dai mezzi e dalle procedure utilizzati, e sono quindi **neutrali dal punto di vista tecnologico**, cioè senza riferimento ad applicazioni tecniche o commerciali concrete. 3

B. Contesto e scopo della norma

Il legislatore svizzero ha sempre sottolineato che la legge svizzera sulla protezione dei dati non ha lo scopo di impedire o limitare le possibilità di sviluppo nel campo delle tecnologie dell'informazione. Piuttosto, in Svizzera si dovrebbe sviluppare una politica dei dati coerente e **orientata al futuro**. In questo contesto, l'IFPDT ha espressamente affermato che, anche con la nuova legge sulla protezione dei dati, i rischi potenzialmente elevati di trattamento non costituiscono un argomento decisivo contro i progetti di trasformazione 4

digitale. Tuttavia, devono essere rispettate alcune **linee guida**. Oltre agli altri principi di trattamento, questi includono il principio della limitazione delle finalità (art. 6 cpv. 3 LPD), qui trattato, le disposizioni sulla durata del trattamento dei dati (art. 6 cpv. 4 LPD) e i requisiti di correttezza dei dati (art. 6 cpv. 5 LPD). Proprio alla luce del rapido e dinamico sviluppo della tecnologia dell'informazione, il rispetto di questi principi di elaborazione dovrebbe impedire un trattamento eccessivo, improprio o inesatto dei dati.

C. Destinatario degli obblighi

5 Gli obblighi derivanti dai principi di trattamento riguardano in primo luogo il **responsabile del trattamento** (art. 5 lett. j LPD). L'incaricato del trattamento tratta i dati personali solo su incarico del responsabile (art. 5 lett. k LPD) e può basarsi sugli stessi motivi di giustificazione del responsabile (art. 9 cpv. 4 LPD).

6 Il responsabile del trattamento non è espressamente indicato come destinatario dei principi di trattamento di cui all'art. 6 LPD, a differenza del principio di trattamento (sanzionabile) della sicurezza dei dati (art. 8 LPD, art. 61 lett. c LPD) e di altri obblighi della LPD, ad esempio l'art. 12 cpv. 1 LPD, art. 17 cpv. 2 LPD e nel capitolo 3 della LPD, che esplicitamente attribuiscono responsabilità al responsabile e/o all'incaricato del trattamento.

D. Conseguenze giuridiche ed economiche di una violazione

7 Le disposizioni dell'art. 6 cpv. 3 LPD (limitazione delle finalità e trasparenza), dell'art. 6 cpv. 4 LPD (limitazione temporale del trattamento dei dati) e dell'art. 6 cpv. 5 LPD (esattezza) non sono elencate nel catalogo esaustivo dei reati (art. 60 segg. LPD). Una violazione di questi principi di trattamento non è di per sé punibile ai sensi della LPD, anche se non è giustificata. Nonostante la revisione completa delle disposizioni penali, nel corso della revisione della LPD non è stato modificato nulla. Tuttavia, sussiste il rischio di punibilità in caso di violazione di altri obblighi correlati a questi principi di trattamento, ad esempio l'obbligo di informazione, art. 19, 21 in combinato disposto con l'art. 60 cpv. 1 lett. b LPD. Possono essere presi in considerazione anche reati al di fuori della LPD.

8 Di notevole importanza sono gli ulteriori **poteri dell'IFPDT** derivanti dalla nuova legge sulla protezione dei dati, che in caso di violazione delle norme sulla protezione dei dati possono portare, tra l'altro, a un **divieto di attività**

di trattamento o a un'ordinanza di **distruzione dei dati**. A questo proposito, l'IFPDT ha già annunciato nella sua relazione di attività 2022/2023 che intensificherà la sua attività di vigilanza e aumenterà il numero di indagini.

Inoltre, una violazione può far sorgere diritti legali ai sensi della LPD (in particolare ai sensi degli artt. 32 e 41 LPD) e diritti di natura civile per violazione della personalità (art. 32 cpv. 2 LPD). 9

A prescindere dalle potenziali conseguenze giuridiche di una violazione dei principi di trattamento, nella pratica occorre considerare soprattutto la possibile **perdita di fiducia** e **il danno alla reputazione** che accompagnano una violazione dei principi di trattamento e che possono avere un impatto negativo a lungo termine sullo sviluppo dell'attività. 10

E. Storia dell'origine dei singoli principi di trattamento

1. Principio della limitazione delle finalità e della trasparenza, art. 6 cpv. 3 LPD

L'art. 6 cpv. 3 LPD combina i principi della finalità e della riconoscibilità, che nella aDSG erano contenuti in due paragrafi separati (art. 4 cpv. 3 aDSG e art. 4 cpv. 4 aDSG). La nuova formulazione dovrebbe avvicinarsi maggiormente alla formulazione dell'art. 5 cpv. 4 lett. b della Convenzione 108 plus, in quanto i dati personali possono essere trattati solo per uno scopo "specifico" e "riconoscibile" per le persone interessate. Un'altra novità è la formulazione secondo cui i dati possono essere trattati solo in modo «compatibile» con tale scopo. La disposizione si avvicina quindi terminologicamente all'art. 5 cpv. 1 lett. b DSGVO. Tuttavia, in termini di contenuto, ciò non comporta modifiche sostanziali rispetto all'aDSG. 11

2. Limitazione temporale del trattamento dei dati, art. 6 cpv. 4 LPD

Con l'art. 6 cpv. 4 LPD è stato introdotto esplicitamente l'obbligo di distruggere o anonimizzare i dati personali non appena non sono più necessari per lo scopo del trattamento. Ciò è conforme ai requisiti della Convenzione 108 plus, nonché all'art. 4 cpv. 1 lett. e della Direttiva (UE) 2016/680 e all'art. 5 cpv. 1 lett. e DSGVO («limitazione della conservazione»). Anche questo obbligo non è nuovo. Derivava già in precedenza dal principio generale di proporzionalità (art. 4 cpv. 2 aDSG, art. 6 cpv. 2 LPD). Con l'inserimento esplicito nella legge, il legislatore ha voluto sottolineare la 12

particolare importanza della limitazione temporale del trattamento dei dati personali, che si impone alla luce dello sviluppo tecnologico e delle possibilità di archiviazione quasi illimitate.

3. Principio di esattezza, art. 6 cpv. 5 LPD

13 Mentre finora il principio di esattezza dei dati era evidenziato in un articolo a sé stante (art. 5 aLPD), ora è stato integrato come cpv. 5 nell'art. 6 LPD, al fine di riunire i principi più importanti della protezione dei dati in un unico articolo. Questo schema si ispira all'art. 5 della Convenzione 108 plus, all'art. 4 della direttiva (UE) 2016/680 e all'art. 5 del DSGVO. Il diritto di rettifica, finora contenuto nell'art. 5 cpv. 2 aDSG, è ora disciplinato dall'art. 32 LPD.

II. OGGETTO DELLE DISPOSIZIONI

A. Principio della limitazione delle finalità e della trasparenza, art. 6 cpv. 3 LPD

1. Requisiti

14 Secondo il principio della limitazione delle finalità e della trasparenza, i dati personali possono essere raccolti solo per una finalità determinata e riconoscibile per la persona interessata. Possono essere trattati solo in modo compatibile con tale finalità, art. 6 cpv. 3 LPD.

15 Secondo la nuova formulazione della legge, l'identità dello scopo non è più esplicitamente richiesta. Il trattamento deve solo essere (costantemente) *compatibile con* lo scopo iniziale. L'ulteriore trattamento per altri scopi è consentito solo se non è inaspettato e non può essere considerato inappropriato o discutibile.

16 Il principio della limitazione delle finalità era già stato relativizzato dal Tribunale federale prima dell'entrata in vigore della nuova LPD, con sentenza del 18 marzo 2021, in un caso riguardante la divulgazione di dati personali da parte di un organo federale, e aveva stabilito che non si può richiedere l'identità assoluta delle finalità, poiché altrimenti l'assistenza amministrativa prevista dall'art. 19 cpv. 1 aDSG sarebbe troppo limitata. In ogni caso, lo scopo dell'assistenza amministrativa deve essere almeno *compatibile con* lo scopo della raccolta iniziale dei dati personali. Il Tribunale federale aveva già

ritenuto sufficiente la “compatibilità” del trattamento con lo scopo iniziale ai sensi dell'aDSG.

L'ulteriore condizione di riconoscibilità deve essere soddisfatta sia per quanto riguarda la raccolta dei dati personali che per quanto riguarda lo scopo del loro trattamento. Può essere considerata soddisfatta se la raccolta dei dati e lo scopo del loro trattamento sono chiaramente evidenti dalle circostanze o se il trattamento è previsto dalla legge. Questa possibilità esiste ancora, anche se i termini «evidenti dalle circostanze» e «o previsto dalla legge» dell'art. 4 cpv. 3 aDSG non sono stati ripresi nel testo dell'art. 6 cpv. 3 LPD. 17

I requisiti di riconoscibilità devono essere determinati caso per caso, tenendo conto dei principi di proporzionalità e di buona fede, art. 6 cpv. 2 LPD. Finalità di trattamento vaghe, non definite o imprecise non sono in linea di principio sufficienti, sebbene tale caratteristica debba essere valutata nuovamente in base alle circostanze e si debba trovare un equilibrio tra gli interessi delle persone interessate e quelli del responsabile o dell'incaricato del trattamento e della società. Nel caso di «Google Street View», ad esempio, il Tribunale federale ha stabilito che il principio della finalità e della trasparenza non è soddisfatto se i veicoli di Google, sui quali sono installate le telecamere, sono visibili ai passanti e ai residenti. Lo scopo di questi veicoli, che percorrono e fotografano sistematicamente strade (ecc.) e pubblicano le immagini su Internet senza il consenso delle persone interessate, non è immediatamente riconoscibile, anche se Google Street View gode di un alto grado di notorietà tra la popolazione svizzera. 18

Il requisito della riconoscibilità è strettamente legato all'obbligo di informazione ai sensi dell'art. 19 e segg. LPD. Tuttavia, non deve essere confuso con esso. Mentre il requisito della riconoscibilità è un principio di elaborazione, la cui violazione può eventualmente essere giustificata (art. 31 LPD), non è così per la violazione dell'obbligo di informazione. Piuttosto, la violazione dell'obbligo di informazione è punibile ai sensi dell'art. 60 cpv. 1 lett. b LPD. 19

2. Esempi

Il trattamento successivo di indirizzi per l'**invio di materiale pubblicitario** viola il principio della finalità e della trasparenza se gli indirizzi sono stati originariamente raccolti in un contesto completamente diverso, ad esempio 20

nell'ambito di una campagna politica. È inoltre illegale l'analisi dei dati personali in relazione alle **abitudini di consumo** (per scopi diversi dalla lotta contro la frode) sulla base di pagamenti effettuati con carta di credito o carta cliente senza il consenso della persona interessata. Anche l'invio di pubblicità via e-mail non richiesta a indirizzi sconosciuti e raccolti in modo indiscriminato su Internet o l'acquisizione da parte di un'azienda privata di indirizzi IP di titolari di connessione che offrono copie pirata da scaricare costituisce una violazione del principio di limitazione delle finalità e di trasparenza.

21 È invece consentito dal punto di vista della protezione dei dati l'utilizzo di un indirizzo a fini pubblicitari se la persona interessata ha fornito il proprio indirizzo per ricevere una **carta cliente** o per un ordine (online o meno) nell'ambito di una finalità inizialmente riconoscibile.

22 Inoltre, l'invio di newsletter pubblicitarie deve soddisfare i requisiti della legge contro la concorrenza sleale, in particolare l'art. 3 cpv. 1 lett. o LCSl («**articolo spam**»). La violazione di tali requisiti può comportare sanzioni penali. Inoltre, quando si inviano newsletter all'estero, è necessario rispettare il rispettivo **diritto nazionale** e le consuetudini locali, che possono comportare requisiti ancora più severi.

23 Il trattamento dei dati «**a titolo precauzionale**», cioè senza scopo, viola sia il principio di proporzionalità che il principio di finalità e trasparenza ed è quindi illegale. Tuttavia, in Svizzera è ancora consentita la memorizzazione e la conservazione senza motivo di **dati marginali delle telecomunicazioni**. È consentita, almeno per un certo periodo di tempo, anche la conservazione da parte della polizia delle registrazioni della **sorveglianza di luoghi pubblici**, in cui i dati vengono raccolti ed elaborati per eventuali indagini penali. Il Tribunale federale ha invece considerato in modo diverso la questione dell'uso (eccessivo) dei **contatori dell'acqua radio**. In questo caso mancava uno scopo per la memorizzazione di determinati dati e la necessità della loro trasmissione.

24 Nel caso di **trasmissione di dati a terzi**, occorre considerare in particolare se tale divulgazione rientra ancora nello scopo originario. Ciò vale anche per lo scambio di dati all'interno di **società del gruppo**. In mancanza di un privilegio di gruppo completo, anche le società dello stesso gruppo sono considerate terze parti, a meno che non elaborino i dati solo come

responsabili del trattamento. La distinzione tra responsabile del trattamento e titolare (congiunto) del trattamento è spesso difficile nella pratica. Di conseguenza, è fondamentale impostare la configurazione in modo coerente e renderla trasparente. Ad esempio, nel **settore delle risorse umane**, si raccomanda di chiarire il contesto del gruppo già nel contratto di lavoro. Quando si trasmettono dati a terzi, è inoltre necessario tenere conto del fatto che il principio della limitazione delle finalità deve essere rispettato anche (ma non solo) durante l'ulteriore trattamento dei dati da parte del destinatario.

Le **applicazioni di big data** come il **data warehousing** e il **data mining** 25
presentano sfide particolari in termini di finalità e trasparenza, poiché la natura stessa delle analisi dei big data implica che il loro scopo concreto si manifesti solo quando i dati vengono combinati sulla base delle nuove conoscenze acquisite.

I big data sono anche la base più importante per l'**intelligenza artificiale** 26
(IA), che si trova quindi in una situazione di tensione con il principio di finalità e trasparenza. L'ammissibilità di tali applicazioni deve essere valutata caso per caso. Spesso, quando si sviluppano sistemi di IA e si inseriscono dati di addestramento, lo scopo dell'elaborazione successiva non può ancora essere definito, ad esempio se l'algoritmo può svolgere una varietà di compiti. Inoltre, vengono solitamente utilizzati dati di addestramento che sono stati originariamente raccolti per scopi completamente diversi (ad esempio, se come dati di addestramento vengono utilizzati dati disponibili gratuitamente su Internet). Pertanto, spesso è dubbio se il loro trattamento sia ancora "compatibile" con lo scopo originario. Particolare importanza sarà data a un'analisi differenziata dei diversi trattamenti dei dati nel **ciclo di vita dell'IA** (sviluppo, inserimento di **dati di addestramento**, utilizzo del risultato del sistema di IA "**output**", ecc.) e ai motivi di giustificazione del consenso, dell'adempimento del contratto e dell'interesse legittimo. Secondo la comunicazione dell'IFPDT, i produttori, i fornitori e gli utenti di sistemi di IA devono inoltre rendere trasparenti le finalità, il funzionamento e le fonti di dati dei trattamenti basati sull'IA. L'autorità di controllo francese CNIL fornisce esempi concreti di finalità secondo il DSGVO da parte degli sviluppatori di sistemi di IA:

Esempi di finalità considerate esplicite e specificate:

- Sviluppo di un modello linguistico di grandi dimensioni (LLM) in grado di rispondere a domande, generare testo in base al contesto (e-mail, lettere, relazioni, compreso il codice informatico), eseguire traduzioni, sintesi e correzioni di testo, eseguire la classificazione del testo, l'analisi dei sentimenti, ecc.;
- Sviluppo di un modello di riconoscimento vocale in grado di identificare un parlante, la sua lingua, età, sesso, ecc.;
- Sviluppo di un modello di visione artificiale in grado di rilevare diversi oggetti come veicoli (auto, camion, scooter, ecc.), pedoni, arredo urbano (cassonetti, panchine pubbliche, pensiline per biciclette, ecc.), segnali stradali, semafori tricolore, segnali stradali, ecc.
- Al contrario, lo scopo non sarebbe considerato sufficientemente specificato se si riferisse solo al tipo di sistema di IA, senza menzionare le funzionalità e le capacità tecnicamente realizzabili.

Esempi di finalità che non sono considerate esplicite e specificate:

- Sviluppo di un modello di IA generativo (le possibili capacità non sono definite);
- Sviluppo e miglioramento di un sistema di IA (non sono definiti né il tipo di modello né le possibili capacità);
- Sviluppo di un modello per identificare l'età di una persona (il tipo non è definito).

Per motivi di trasparenza, la CNIL raccomanda inoltre che in questo caso il responsabile del trattamento sia in grado di determinare in anticipo le capacità prevedibili del sistema di IA che presentano i rischi maggiori, che lo scopo si riferisca alle funzionalità che sono escluse a priori e che lo scopo stabilisca il più possibile le condizioni per l'utilizzo del sistema di IA.

Anche per quanto riguarda i requisiti di trasparenza, occorre inoltre tenere conto della legge europea sull'IA, che può essere applicabile anche alle imprese svizzere.

27 Il potenziale del riutilizzo dei dati per **scopi di utilizzo secondario** è stato riconosciuto anche dal legislatore svizzero. Il 12 giugno 2023, il Consiglio nazionale ha approvato, in qualità di seconda Camera, una mozione per la

creazione di una **legge quadro per l'utilizzo secondario** dei dati. In questo modo il Consiglio federale è incaricato di elaborare una legge che risolva il conflitto tra protezione dei dati e utilizzo dei dati e crei spazi di dati affidabili.

A livello europeo, inoltre, devono essere presi in considerazione in particolare 28
il Data Governance Act, il Data Act, la regolamentazione relativa allo European Health Data Space e, come già accennato, l'AI Act. Questi possono essere applicati anche alle aziende svizzere.

3. Raccomandazioni per l'attuazione

Le finalità del trattamento dei dati devono essere definite, rispettate in modo 29
permanente e rese trasparenti. In pratica, quest'ultimo aspetto può essere raggiunto, a seconda dei casi, almeno in parte attraverso le condizioni generali di contratto o attraverso comunicazioni/avvertenze individuali, nell'ambito della dichiarazione sulla protezione dei dati che è comunque necessaria. È importante notare che finalità di trattamento vaghe, non definite o imprecise non sono sufficienti. Il grado di precisione richiesto deve essere determinato caso per caso, tenendo conto dei principi di proporzionalità e di buona fede. In caso di trasmissione a terzi, si raccomanda spesso di stipulare un accordo contrattuale che preveda il trattamento dei dati solo per scopi specifici e legittimi, compreso l'obbligo di indennizzo. Almeno, tuttavia, dovrebbe essere fatto riferimento alla limitazione delle finalità.

B. Limitazione temporale del trattamento dei dati, art. 6 cpv. 4 LPD

1. Requisiti

Secondo il principio della limitazione temporale del trattamento dei dati, i 30
dati personali devono essere **distrutti o resi anonimi** non appena non sono più necessari ai fini del trattamento.

Tuttavia, un ulteriore trattamento dei dati può essere giustificato, art. 31 cpv. 1 31
LPD. Ciò avviene in particolare quando devono essere soddisfatti **obblighi di conservazione**, ad esempio l'obbligo di conservazione per dieci anni di libri contabili, documenti contabili, relazioni commerciali e di revisione o obblighi di conservazione ai sensi del diritto tributario. Un interesse legittimo alla

conservazione può anche derivare da potenziali controversie legali future e da norme sulla prescrizione.

32 **Distruggere** significa, in senso stretto, distruggere o rimuovere i dati in modo irreversibile. Per i dati cartacei, questi devono essere distrutti o bruciati e bisogna assicurarsi che terzi non abbiano accesso alle "reliquie". Per i dati elettronici, non è rilevante solo il modo in cui sono memorizzati, ma anche come sono stati ottenuti. Se sono stati trasmessi tramite chiavetta USB, la chiavetta USB deve essere resa inutilizzabile e tutte le copie devono essere trattate in modo tale che i dati non possano più essere resi leggibili. Se sono stati trasmessi via e-mail, anche eventuali copie temporanee di questa e-mail devono essere distrutte. Inoltre, la distruzione è soggetta a requisiti elevati. Secondo il messaggio relativo alla LPD, i normali comandi di cancellazione o la semplice riformattazione non costituiscono una distruzione ai sensi della legge sulla protezione dei dati.

33 **La distruzione** richiede quindi più della **cancellazione**. Tuttavia, nella letteratura si ritiene che l'art. 6 cpv. 4 LPD sia un errore editoriale e che il principio della limitazione temporale possa essere soddisfatto anche con la cancellazione. Ciò è giustificato da un'imprudente ripresa del termine "distruzione" dalla precedente disposizione dell'art. 5 aDSG. Inoltre, i termini "distruzione" e "cancellazione" sono usati come sinonimi nella LPD. Secondo il nostro parere, ciò è certamente accettabile se il termine di cancellazione, che peraltro non è definito né nella LPD né nella DSGVO, è inteso nel senso che non è più possibile stabilire un riferimento personale, perché allora la LPD non è (più) applicabile per definizione in mancanza di dati personali, art. 5 lett. a. LPD. Secondo l'approccio basato sul rischio della LPD, ciò si verifica già quando il riferimento alla persona può essere stabilito solo con un dispendio elevato che nessun interessato sarebbe disposto a sostenere. Se ciò possa essere affermato anche nel contesto dell'**archiviazione dei dati**, ad esempio, deve essere verificato caso per caso. Anche misure organizzative come i blocchi di accesso e il principio del doppio controllo possono essere considerate misure sufficienti.

34 Il principio della limitazione temporale può essere soddisfatto anche attraverso l'**anonimizzazione**. Per anonimizzazione si intende qualsiasi misura che abbia l'effetto di rendere impossibile o estremamente difficile l'identificazione delle persone interessate. L'anonimizzazione non deve essere confusa con la **pseudonimizzazione**. La pseudonimizzazione consiste nello

scambiare il nome e altri elementi identificativi con un altro segno distintivo, ad esempio un segnaposto, allo scopo di escludere o rendere difficile l'identificazione della persona interessata. In altre parole, la pseudonimizzazione consente di ripristinare il riferimento personale con la chiave corrispondente. Questo vale però solo per chi possiede la chiave. Questo **approccio relativo** fa sì che anche per chi non possiede la chiave e per chi è praticamente impossibile ottenerla non siano disponibili dati personali. Questo approccio relativo ha un impatto significativo sulla pratica, perché esclude dal campo di applicazione della legge sulla protezione dei dati chi non possiede una chiave.

2. Raccomandazioni per l'attuazione

L'obbligo di distruggere o rendere anonimi i dati può rappresentare una grande sfida per i responsabili. In una prima fase, si raccomanda di ottenere una panoramica dei consueti trattamenti dei dati nei rispettivi settori di attività. Successivamente, dovrebbero essere stabiliti i rispettivi periodi di conservazione e cancellazione. In pratica, ciò avviene in elenchi chiari, che fungono anche da linee guida interne ("linee guida sulla conservazione"/"data retention policy"). 35

Per l'implementazione è utile se il software utilizzato per l'elaborazione dei dati offre già le funzionalità appropriate per la cancellazione automatica, prestando attenzione, da un lato, che queste soddisfino i requisiti di legge in materia di protezione dei dati dal punto di vista tecnico e, dall'altro, che l'obbligo di cancellazione sia sufficientemente coperto contrattualmente nell'ambito dei contratti di elaborazione dei dati dell'ordine con il fornitore IT/fornitore di cloud. 36

C. Principio di correttezza, art. 6 cpv. 5 LPD

1. Correttezza dei dati

a. Requisiti

I dati personali sono corretti se riflettono in modo adeguato le circostanze e i fatti relativi alla persona interessata. Devono essere corretti nel loro contesto generale, tenendo conto delle finalità e delle modalità del trattamento. Ne consegue che il concetto di correttezza nel diritto della protezione dei dati 37

non deve essere inteso in senso assoluto, ma che il caso concreto di applicazione assume un'importanza significativa.

38 Anche i dati personali corretti possono essere inesatti nel contesto generale e tenendo conto dello scopo del trattamento ai sensi della legge sulla protezione dei dati, ad esempio se una persona è registrata come «perseguita» in una raccolta di dati sulla solvibilità, anche se ha pagato le sue fatture correttamente e in tempo per anni e c'è stata una sola esecuzione perché la fattura è stata consegnata a un indirizzo sbagliato. D'altro canto, le dichiarazioni false non devono necessariamente essere inesatte ai sensi della legge sulla protezione dei dati. Secondo la sentenza del Tribunale federale, ad esempio, alcune informazioni non possono essere considerate false se l'insieme delle informazioni riflette correttamente la situazione reale. Inoltre, le informazioni possono essere state del tutto corrette in termini di "istantanee", anche se successivamente diventano inesatte, ad esempio se in una sentenza viene ancora riportato un nome che nel frattempo è stato modificato. In questo caso, è fondamentale lo scopo per cui i dati vengono ancora utilizzati. In questo contesto, il principio di accuratezza deve essere considerato in modo differenziato, in particolare per quanto riguarda le attività di archivi, musei, biblioteche e altre istituzioni della memoria. Poiché il compito di tali istituzioni è quello di raccogliere, catalogare, conservare e trasmettere documenti di ogni tipo, questi non devono essere modificati, perché ciò sarebbe contrario allo scopo dell'archiviazione. Gli archivi consentono, con l'aiuto dei documenti, di ottenere un'istantanea del passato, la cui «correttezza» si riferisce esclusivamente al fatto che i documenti in questione sono riprodotti fedelmente, indipendentemente dal fatto che ciò sia ancora considerato accurato da una prospettiva attuale. Allo stesso modo, la pretesa di correttezza nei controlli di polizia non si riferisce alle informazioni oggettivamente verificabili sulle persone interessate, ma all'autenticità del verbale. Ciò che conta è se i dati disponibili riflettono l'osservazione soggettiva della persona autorizzata al momento della valutazione.

39 La correttezza dei dati può in linea di principio riferirsi solo a **fatti concreti** che possono essere accertati oggettivamente. **I giudizi di valore** sono soggettivi e difficilmente classificabili come corretti o errati. È difficile distinguere quando i giudizi di valore e i fatti concreti sono mescolati. Ciò ha acquisito un'importanza attuale soprattutto in relazione alle "fake news". Ad esempio, può essere corretta o errata l'indicazione che un giudizio di valore è

stato espresso da una determinata persona o documentato in un fascicolo. Può essere altrettanto corretta o errata anche l'indicazione di chi è oggetto del giudizio di valore. Anche l'ulteriore utilizzo del fatto del giudizio di valore è soggetto ai principi generali di elaborazione.

Il rispetto del principio di correttezza dei dati pone sfide particolari per quanto riguarda i **sistemi di IA**. Soprattutto nel caso dei sistemi di IA in cui i **dati di addestramento** provengono da fonti accessibili al pubblico, in particolare da Internet, spesso non è possibile verificare efficacemente la correttezza dei dati. Anche i risultati dell'elaborazione dei dati da parte dei sistemi di IA («**output**») possono essere inesatti. Da un lato, non si può presumere che la «correttezza statistica» sia sempre sufficiente per l'elaborazione dei dati in relazione ai sistemi di IA. D'altro canto, tuttavia, non si possono imporre requisiti più elevati per il trattamento dei dati in relazione ai sistemi di IA rispetto ad altri trattamenti di dati, poiché la LPD è fondamentalmente neutrale dal punto di vista tecnologico. Ciò significa che la questione dell'esattezza dei dati deve essere valutata anche nel caso di trattamenti di dati nell'ambito di sistemi di IA caso per caso e tenendo conto del contesto generale. Particolarmente rilevanti sono lo scopo del trattamento dei dati e l'importanza dell'output, nonché le aspettative degli utenti. In questo caso, nella pratica, sarà fondamentale informare adeguatamente gli utenti. Il requisito associato alla verifica dell'output dovrebbe riflettersi anche nelle «**AI Guidelines**» delle aziende. 40

In generale, il trattamento di dati inesatti non costituisce di per sé una violazione della personalità. Solo se le informazioni inesatte danno luogo a una violazione della personalità a causa del loro trattamento, devono essere corrette o distrutte. Anche il principio di correttezza non è assoluto. Una violazione può essere giustificata per i responsabili del trattamento dei dati privati ai sensi dell'art. 31 LPD. Per gli organi federali, il diritto alla cancellazione può essere limitato (cfr. art. 41 cpv. 3-5 LPD). 41

b. Esempi

In caso di trattamento di **informazioni sospette** relative alla commissione di possibili reati, l'art. 6 cpv. 5 LPD non si oppone a tale trattamento fintanto che la rilevanza dell'informazione corrispondente è nota e il sospetto non appare come una conoscenza certa. **Le e-mail archiviate** che, in base alle conoscenze attuali, contengono informazioni errate, sono comunque corrette 42

ai sensi della legge sulla protezione dei dati, a meno che non vengano elaborate partendo dal presupposto che siano ancora attuali. Allo stesso modo, la conservazione della **corrispondenza commerciale** è consentita nell'ambito dell'obbligo di conservazione, anche se contiene informazioni errate. Se in un database di indirizzi di un'associazione viene registrato un numero civico errato, ma il database di indirizzi non serve per la spedizione postale, ma solo per il controllo dell'effettivo dei membri, l'informazione non deve essere corretta. In ogni caso, anche in caso di tale trattamento dei dati, è necessario verificare il rispetto degli altri principi generali di trattamento, in particolare i principi di proporzionalità e di limitazione delle finalità.

2. Obbligo di accertamento, obbligo di rettifica e cancellazione

a. Requisiti

43 Secondo il principio di correttezza, chiunque tratti dati personali deve accertarne la correttezza (art. 6 cpv. 5 LPD). L'art. 6 cpv. 5 LPD stabilisce inoltre esplicitamente che devono essere adottate tutte le misure adeguate per correggere, cancellare o distruggere i dati inesatti. Questo obbligo completa l'obbligo di verifica, che altrimenti non avrebbe senso. La portata dell'obbligo di verifica dipende dal singolo caso. In particolare, occorre considerare lo scopo e la portata del trattamento, nonché il tipo di dati trattati, la misura in cui i dati vengono comunicati e la loro sensibilità. In questo contesto deve essere esercitato anche l'obbligo di verifica da parte del responsabile del trattamento dei dati. Maggiore è il rischio di violazione della personalità, maggiori sono i requisiti da porre all'obbligo di verifica. L'obbligo di verifica può quindi anche portare a un **obbligo di aggiornamento**. Tuttavia, non comporta un obbligo generale di controllo regolare senza motivo.

44 L'attuazione delle misure di verifica può anche essere **delegata a** terzi, ad esempio alla fonte dei dati o a un incaricato del trattamento. In caso di violazione dell'obbligo di verifica, sussiste per legge una violazione dei principi di trattamento e quindi una violazione della personalità, art. 30 cpv. 2 lett. a LPD. Secondo il senso e lo scopo della legge, una tale violazione dei doveri può tuttavia dare luogo a richieste di rettifica e di risarcimento danni solo se i dati sono effettivamente inesatti. Le misure da adottare dipendono, tra l'altro, dal tipo, dalla portata e dallo scopo del trattamento dei dati, dalla sensibilità dei dati e dal rischio per i diritti della personalità della persona

interessata. Anche questo deve essere determinato caso per caso. Inoltre, gli obblighi di legge possono ostacolare le misure di rettifica, cancellazione o aggiornamento.

b. Esempi

Se il trattamento dei dati a fini di marketing si basa su **informazioni fornite dalla persona interessata**, il responsabile non deve accertarne l'esattezza. Allo stesso modo, non vi è alcun obbligo generale di controllare costantemente gli indirizzi obsoleti in una scheda clienti a fini di marketing. Tuttavia, se un assicurato comunica all'assicuratore un cambiamento di indirizzo, da cui si evince anche il cambiamento dello stato civile, l'assicuratore deve aggiornare lo stato civile, se questo ha un impatto sull'erogazione della prestazione assicurativa. D'altro canto, le informazioni fornite una volta in una polizza assicurativa non devono essere ulteriormente verificate, a meno che non abbiano un impatto sul premio o sulla prestazione assicurativa. Per quanto riguarda le agenzie di informazioni commerciali, l'entità dei dati, la presenza di profili di personalità e consensi e il numero di query effettuate devono essere presi in considerazione in particolare per quanto riguarda la verifica dei set di dati. Se un'assicurazione desidera utilizzare l'**intelligenza artificiale** (**IA**) per creare un profilo dei clienti che stipulano un'assicurazione e utilizzare questo profilo come base per le sue decisioni nel calcolo del rischio assicurativo, non solo i dati dei clienti esistenti provenienti da fonti di dati con informazioni corrette e aggiornate dovrebbero essere utilizzati come dati di addestramento, ma anche un pool di clienti rappresentativo della popolazione dovrebbe essere utilizzato per evitare distorsioni. 45

3. Raccomandazioni per l'attuazione

I requisiti per le misure richieste ai sensi dell'art. 6 cpv. 5 LPD dovrebbero essere proporzionati ai rischi e alle conseguenze dell'uso concreto. Esempi di misure da adottare, che rappresentano anche aspetti centrali nell'ambito della progettazione tecnica secondo i principi di **Privacy by Design** e **Privacy by Default**, possono essere: 46

- verifica dell'affidabilità della fonte dei dati
- determinazione del grado di accuratezza in base alle circostanze generali del singolo caso

- eventuali nuove verifiche dei dati in base alle circostanze generali e alle diverse fasi del trattamento dei dati
- riduzione dei falsi positivi / falsi negativi, ad esempio per ridurre gli errori nel processo decisionale automatizzato e nell'uso dell'intelligenza artificiale
- aggiornamento dei dati, se necessario per lo scopo del trattamento
- Implementazione di soluzioni self-service, in cui le persone interessate possono verificare e, se necessario, correggere i propri dati
- Introduzione di controlli di plausibilità e di qualità
- Implementazione di controlli automatici dell'inserimento dei dati, ad esempio per evitare l'inserimento errato dei codici postali
- Menu a tendina invece di inserimento di testo libero

47 Dal punto di vista dei responsabili, si raccomanda inoltre di imporre contrattualmente alle persone interessate l'obbligo di fornire dati corretti e aggiornati e di escludere, per quanto possibile, qualsiasi responsabilità in merito. In linea di principio, per le fonti di dati esterne dovrebbe essere preso in considerazione anche un obbligo di indennizzo. A seconda del caso, ciò può essere preso in considerazione nell'ambito di un concetto globale che comprenda l'assegnazione di dati e responsabilità, nonché altri diritti e doveri correlati.

BIBLIOGRAFIA

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).

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 6 cpv. 6 e 7 LPD

Un commentario di Gaspare T. Loderer

CITAZIONE SUGGERITA

Gaspare Loderer, Commentario all'art. 6 LPD cpv. 6 e 7, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Loderer, art. 6 LPD N. XXX.

Art. 6 Principi

[...]

6 Laddove sia una condizione necessaria per il trattamento, il consenso della persona interessata è valido soltanto se, dopo debita informazione, è dato in modo libero in riferimento a uno o più trattamenti specifici.

7 È necessario l'espresso consenso per:

a. il trattamento di dati personali degni di particolare protezione;

b. la profilazione a rischio elevato da parte di privati;

c. la profilazione da parte di un organo federale.

STRUTTURA

IN BREVE 117
I. Informazioni generali 117
A. Storia dell'origine 117
B. Sistema e delimitazione 118
C. Ambito di applicazione 119
D. Confronto con il DSGVO 119
II. Requisiti per il consenso (art. 6 cpv. 6 LPD) 120
A. Informazioni generali 120
B. Capacità di giudizio 120
D. Uno o più trattamenti specifici 121
E. Informazioni adeguate 122
F. Volontarietà 124
G. Inequivocabilità 126
H. Forma 127
III. Consenso esplicito (art. 6 cpv. 7 LPD) 128
IV. Revoca 130
V. Conseguenze legali del consenso mancante, non valido o revocato 130
VI. Consigli pratici 131
VII. Critiche alla norma 131
Bibliografia 132
I materiali 135

IN BREVE

Gli artt. 6 cpv. 6 e 7 LPD stabiliscono i requisiti di validità del consenso ai sensi della legge sulla protezione dei dati. I casi in cui è necessario il consenso sono tuttavia disciplinati in altre disposizioni. Il contenuto delle nuove disposizioni sul consenso è sostanzialmente identico a quello dell'art. 4 cpv. 5 aDSG. È stato solo specificato che il consenso deve essere dato per una o più operazioni di trattamento specifiche, già applicate in precedenza. Nel caso di consenso esplicito, la nuova profilazione introdotta ha sostituito il vecchio profilo di personalità giuridica. Per il resto, tuttavia, la situazione giuridica non dovrebbe cambiare. Se il consenso è richiesto, deve essere comunque prestato volontariamente per uno o più trattamenti specifici, dopo aver fornito informazioni adeguate. Se il consenso è richiesto per il trattamento di dati personali particolarmente sensibili, per la profilazione ad alto rischio da parte di un privato o per la profilazione da parte di un organismo federale, anche questo deve essere esplicito. Tuttavia, anche in questi casi, non esiste un obbligo generale di consenso, sebbene alcuni sostengano il contrario. Nell'ambito di applicazione del DSGVO, il consenso è utilizzato più frequentemente come base giuridica per il trattamento a causa del diverso concetto (principio di divieto con riserva di autorizzazione) e i requisiti per un consenso valido sono generalmente più elevati rispetto alla LPD.

I. INFORMAZIONI GENERALI

A. Storia dell'origine

L'art. 6 cpv. 6 e il cpv. 7 LPD corrispondono essenzialmente al contenuto dell'art. 4 cpv. 5 aDSG, sebbene siano state apportate alcune modifiche redazionali nell'ambito della revisione totale. Il consenso esplicito è stato separato dal consenso "ordinario" e disciplinato in un paragrafo separato. È stato inoltre chiarito che il consenso deve riguardare una o più operazioni di trattamento specifiche. Questo chiarimento è stato fatto al fine di armonizzare con la Convenzione ETS 108 rivista, ma non comporta alcuna modifica della situazione giuridica. Poiché nell'ambito della revisione totale anche il termine "profilo della personalità" è stato sostituito da "profilazione", il consenso per la profilazione ad alto rischio da parte di privati e per la 1

profilazione da parte di organismi federali deve ora essere dato esplicitamente.

2 Il nuovo criterio del consenso inequivocabile introdotto nella bozza è stato abbandonato durante le deliberazioni parlamentari. Anche questo criterio era stato originariamente aggiunto al fine di armonizzarlo con la Convenzione ETS 108 riveduta.

B. Sistema e delimitazione

3 La legge svizzera sulla protezione dei dati si basa sul principio dell'autorizzazione con riserva di divieto. Di conseguenza, il trattamento è generalmente consentito a condizione che siano rispettati i principi di trattamento di cui all'art. 6 e la sicurezza dei dati ai sensi dell'art. 8 LPD, che i dati personali non siano trattati senza il consenso esplicito della persona interessata o che i dati personali che richiedono una protezione speciale siano comunicati a terzi (art. 30 cpv. 2 LPD). In caso contrario, si verifica una violazione dei diritti della personalità, che può essere giustificata, tra l'altro, dal consenso della persona interessata (art. 31 cpv. 1 LPD).

4 Gli artt. 6 cpv. 6 e 7 LPD non stabiliscono quindi un requisito generale per il consenso, ma definiscono solo le condizioni in cui il consenso è valido. Se e per quali casi è necessario il consenso, tuttavia, è disciplinato altrove. Di conseguenza, il consenso non è richiesto di per sé per i casi di cui all'art. 6 cpv. 7 LPD (trattamento di dati personali particolarmente sensibili, profilazione ad alto rischio da parte di un privato e profilazione da parte di un organo federale), anche se alcuni sostengono il contrario.

5 Nonostante la posizione sistematica delle disposizioni sul consenso di cui all'art. 6 LPD con il titolo "Principi", i requisiti di validità del consenso non sono un principio di trattamento ai sensi della legge sulla protezione dei dati. In particolare, non vi è alcuna violazione dei diritti della personalità se i requisiti per il consenso non sono soddisfatti, sebbene l'art. 30 cpv. 2 lett. a LPD faccia riferimento ai "principi" dell'art. 6 LPD. Per questo motivo, sarebbe stato meglio spostare le disposizioni sul consenso nelle definizioni dell'art. 5 LPD.

C. Ambito di applicazione

Per i privati, il consenso può in particolare giustificare una violazione dei diritti della personalità (art. 31 cpv. 1 LPD). Inoltre, il consenso può essere rilevante per i privati nei seguenti casi: Per la divulgazione di dati personali all'estero in deroga all'art. 16 cpv. 1 e 2 LPD (art. 17 cpv. 1 lett. a LPD); per le decisioni individuali automatizzate senza dover rispettare i requisiti dell'art. 21 cpv. 1 e 2 LPD (art. 21 cpv. 3 lett. b LPD); nell'ambito del diritto all'informazione per la comunicazione di dati sulla salute da parte di un operatore sanitario (art. 25 cpv. 3 LPD). 6

Per gli organi federali, il consenso può sostituire il requisito generale di una base giuridica in singoli casi (art. 34 cpv. 4 lett. b LPD), anche per la divulgazione di dati personali all'estero (art. 36 cpv. 2 lett. b LPD). 7

Inoltre, il consenso è menzionato anche in altre parti della LPD e può essere previsto anche da leggi speciali. Se e in che misura i requisiti della LPD si applichino in questo caso non è stato chiarito completamente, in particolare nell'intersezione con il divieto di spam ai sensi dell'art. 3 cpv. 1 lett. o LCSl. Tuttavia, ciò si presume almeno implicitamente. 8

D. Confronto con il DSGVO

Il concetto svizzero si differenzia fondamentalmente dal concetto inverso del DSGVO. In Svizzera vige il principio del divieto con riserva di autorizzazione, secondo il quale qualsiasi trattamento di dati personali è vietato a meno che non vi sia una base giuridica per il trattamento (art. 6 DSGVO). Una di queste possibili basi giuridiche è il consenso (art. 6 cpv. 1 lett. a DSGVO). I suoi requisiti sono generalmente descritti in modo più dettagliato nell'art. 4 n. 11 e nell'art. 7 DSGVO, per quanto riguarda il consenso dei minori nell'art. 8 DSGVO e per il trattamento di categorie speciali di dati personali, il consenso deve essere dato espressamente (art. 9 cpv. 2 lett. a DSGVO). 9

I requisiti per un consenso valido ai sensi del DSGVO sono più severi di quelli previsti dalla LPD. Il consenso valido ai sensi del DSGVO soddisfa quindi generalmente i requisiti del DSGVO, mentre il consenso valido ai sensi dell'LPD non soddisfa necessariamente i requisiti più severi del DSGVO. 10

II. REQUISITI PER IL CONSENSO (ART. 6 CPV. 6 LPD)

A. Informazioni generali

11 Il consenso è soggetto ai "limiti" generali dei diritti della persona, che comprendono le disposizioni degli artt. 16 e segg. CC (capacità di giudizio) e art. 27 CC (eccesso di obbligo). Il consenso deve essere qualificato come un negozio giuridico unilaterale, motivo per cui il CO si applica in particolare all'interpretazione del consenso (principio di fiducia), alle limitazioni di cui agli artt. 19 e 20 CO e ai vizi della volontà (art. 23 e segg. CO).

B. Capacità di giudizio

12 Il rilascio del consenso ai sensi della legge sulla protezione dei dati costituisce l'esercizio di un diritto personalissimo e può quindi essere esercitato autonomamente da persone prive di capacità (art. 19c cpv. 1 CC). Tuttavia, le persone prive di capacità sono generalmente rappresentate dal loro rappresentante legale (art. 19c cpv. 2 CC). Nell'ambito della loro rappresentanza legale e nei limiti delle cure parentali a cui hanno diritto, i genitori possono dare il consenso ai minori privi di capacità (art. 304 CC).

13 Una persona è capace di giudizio se non manca della capacità di agire razionalmente a causa di determinate condizioni (infanzia, disabilità mentale, disturbo mentale, intossicazione o simili) (art. 16 CC). Come regola generale, si presume che la capacità di giudizio esista nei minori a partire dai 13 anni. Data la natura relativa della capacità di giudizio, i requisiti devono essere più elevati, ad esempio nel caso di trattamenti complessi, dati personali sensibili e interventi gravi sulla personalità.

C. Tempistica

14 In genere il consenso deve essere dato prima del trattamento dei dati, che può essere precedente alla raccolta o alla divulgazione dei dati (cfr. art. 5 lett. d LPD). Se il consenso è necessario e non è stato dato, il relativo trattamento dei dati è illegale.

15 È escluso il consenso successivo in senso stretto. Tuttavia, può essere presa in considerazione un'autorizzazione successiva, che deve essere interpretata come una rinuncia a far valere i propri diritti. Tuttavia, il trattamento dei dati è illegale fino al momento dell'autorizzazione successiva. Inoltre,

l'autorizzazione successiva si estende solo ai trattamenti di dati sui quali sono state fornite informazioni adeguate inizialmente o successivamente.

D. Uno o più trattamenti specifici

Con la revisione totale è stato aggiunto il criterio secondo cui il consenso deve riguardare uno o più trattamenti specifici. In questo modo la formulazione si allinea all'art. 5 cpv. 2 della Convenzione ETS 108 riveduta, ma senza modificare la situazione giuridica. 16

Come nella vecchia legge, è necessario che il trattamento sia sufficientemente definito, in particolare in termini di ambito e finalità. L'interessato deve essere in grado di capire per quale trattamento sta dando il proprio consenso. La portata specifica del consenso è determinata dalla dichiarazione di consenso e dalle informazioni appropriate. Senza ulteriori informazioni, descrizioni generiche di finalità quali "migliorare l'esperienza dell'utente", "finalità pubblicitarie", "finalità di sicurezza informatica" o "ricerche future" sono inadeguate. Il trattamento può essere limitato o illimitato nel tempo. In alcuni casi, tuttavia, il consenso è richiesto caso per caso. 17

Il consenso a più trattamenti non richiede che tutti abbiano la stessa finalità; il consenso può essere dato anche per trattamenti diversi. Inoltre, una finalità di trattamento come il trattamento medico da parte di un medico può richiedere diverse operazioni di trattamento, ad esempio lo scambio di dati personali particolarmente sensibili con altri specialisti o compagnie assicurative e il trattamento a fini di fatturazione. 18

La misura in cui il consenso generale è ammissibile è controversa. In ogni caso, i limiti del consenso devono essere chiari e, in base al principio di proporzionalità, quanto più sensibili sono la natura e la portata del trattamento, tanto più chiari devono essere. Non sono pertanto consentite dichiarazioni di consenso illimitate per qualsiasi finalità, per qualsiasi trattamento o per tutte le categorie di dati personali da parte di responsabili del trattamento illimitati. D'altro canto, è consentito, ad esempio, autorizzare il precedente datore di lavoro a fornire in generale informazioni a potenziali datori di lavoro, il che richiede un consenso esplicito nel caso di divulgazione di dati personali particolarmente sensibili (come le informazioni sulle assenze per malattia). 19

E. Informazioni adeguate

20 Il consenso ai sensi della legge sulla protezione dei dati si basa sul "consenso informato del paziente", il che significa che tutte le informazioni devono essere fornite nel caso specifico in modo che la persona interessata possa prendere una decisione libera. In altre parole, è importante che l'interessato abbia ben chiaro a cosa sta acconsentendo, cioè che conosca la portata del suo consenso. Le informazioni specifiche da fornire non erano già valutate in modo uniforme con la vecchia legge, né lo saranno con la nuova legge.

21 Secondo l'opinione espressa in questa sede, i requisiti per un'informazione adeguata possono essere modellati sull'obbligo di fornire informazioni ai sensi dell'art. 19 LPD. Questo perché le informazioni adeguate richieste per il consenso possono portare a un'esenzione dall'obbligo di informazione ai sensi dell'art. 19 LPD, in quanto la persona interessata dispone già delle informazioni pertinenti (art. 20 cpv. 1 lett. a LPD).

22 Tuttavia, ciò non significa che tutte le informazioni di cui all'art. 19 LPD debbano sempre essere fornite come base per le informazioni appropriate di cui all'art. 6 par. 6 LPD, anche se tale approccio integrativo può essere richiesto nella pratica. Secondo il parere espresso in questa sede, per un'informativa adeguata nel contesto del consenso sono necessarie almeno le seguenti informazioni:

- Identità del responsabile del trattamento;
- Scopo del trattamento;
- (categorie di) dati personali trattati.

23 Quali di queste informazioni siano necessarie e con quale livello di dettaglio, e se siano necessarie informazioni aggiuntive, dipende dalle circostanze del singolo caso. In applicazione del principio di proporzionalità, quanto più sensibili sono i dati personali in questione, tanto più chiare devono essere le informazioni appropriate. Ad esempio, l'art. 16 cpv. 2 dell'HRA specifica che per il consenso a progetti di ricerca, tra le altre cose, devono essere fornite informazioni sui rischi e gli oneri prevedibili e sulle misure di protezione dei dati personali raccolti. Ai sensi dell'art. 8 cpv. 1 dell'HRO, devono essere fornite informazioni anche sul diritto di rifiuto o di revoca e sulle conseguenze della revoca, nonché, in generale, su altri contenuti necessari per la decisione.

A differenza dell'art. 7 cpv. 3 DSGVO, tuttavia, la LPD non richiede in generale informazioni sul diritto di revocare il consenso e sul fatto che la revoca non pregiudica la liceità del trattamento basato sul consenso prima della sua revoca. La mancanza di informazioni al riguardo non invalida quindi il consenso prestato. 24

Il DSGVO richiede inoltre che il consenso possa essere revocato con la stessa facilità con cui è stato dato. L'IFPDT lo ha richiesto anche per l'aDSG sulla base del principio di buona fede. Tuttavia, la legge non fornisce alcun supporto a questa generalizzazione, che va pertanto respinta. D'altra parte, il carattere volontario del consenso può essere discutibile se non può essere revocato in modo ragionevole. 25

In linea con le spiegazioni contenute nel Dispaccio del 2003, alcuni ritengono che debbano essere fornite informazioni sulle conseguenze negative o sugli svantaggi del rifiuto del consenso. Secondo l'opinione espressa in questa sede, questa non è una parte necessaria dell'informazione appropriata, ma a seconda delle conseguenze negative, può mettere in discussione la validità del consenso a causa della mancanza di volontarietà. D'altra parte, devono essere fornite informazioni su eventuali rischi esistenti nel trattamento dei dati. 26

Il responsabile del trattamento deve sempre fornire informazioni adeguate. Tuttavia, è possibile ottenere il consenso per il trattamento da parte di terzi. Ciò richiede regolarmente che il terzo sia nominato, a meno che questa informazione non sia sufficientemente chiara dalle circostanze, come può accadere, ad esempio, nel caso di società del gruppo. 27

Le informazioni fornite devono essere interpretate secondo il principio di fiducia, ossia come la persona interessata avrebbe potuto e dovuto intenderle. Ciò deve basarsi sull'ipotesi di una persona media del gruppo di destinatari. La dottrina che vorrebbe invece concentrarsi sulle capacità del singolo interessato deve quindi essere respinta. 28

Le informazioni appropriate devono essere precise, trasparenti e comprensibili. Deve essere redatta nella lingua in cui il responsabile del trattamento fornisce i servizi su cui si basa il trattamento. Le informazioni possono essere fornite oralmente o per iscritto; tuttavia, per motivi di prova, è consigliabile fornire prove in forma di testo. Se le informazioni sul trattamento per il quale è stato prestato il consenso devono essere 29

frammentate e raccolte da più parti in un unico documento, ciò può essere un argomento a sfavore dell'esistenza di informazioni adeguate.

30 Deve essere possibile prendere nota delle informazioni prima di dare il consenso. Un periodo di riflessione può essere appropriato a seconda della sensibilità del trattamento. Ad esempio, l'art. 16 cpv. 3 dell'HRA richiede che sia concesso un ragionevole periodo di riflessione prima che la persona interessata acconsenta a un progetto di ricerca.

31 Il fatto che le informazioni vengano effettivamente prese in considerazione è irrilevante. L'unico fattore decisivo è se vi sia stata una ragionevole opportunità di prendere nota dell'informazione. Nel caso di un'accettazione globale, vale a dire la concessione del consenso senza prendere atto dell'informazione (ad esempio perché si trova solo in termini e condizioni generali collegati o in un'informativa sulla privacy), le clausole inusuali non si applicano (regola dell'inusualità). Può quindi essere opportuno sottolineare separatamente gli aspetti inusuali.

F. Volontarietà

32 Il consenso deve essere prestato volontariamente, ossia deve essere espressione della libera volontà dell'interessato. Esiste un'interazione con la necessità di informazioni adeguate. Se non vengono fornite le informazioni adeguate, non si può ritenere che il consenso sia volontario. Il consenso non è volontario nemmeno se è stato ottenuto con l'inganno, le minacce o la coercizione.

33 La LPD non riconosce un divieto di abbinamento basato sull'art. 7 cpv. 4 del DSGVO, sebbene la sua esistenza e la sua portata ai sensi del DSGVO siano controverse. Tuttavia, anche la legge svizzera prevede forme di legatura non autorizzata del consenso, sebbene gli ostacoli siano più elevati rispetto al DSGVO. In particolare, il consenso non dovrebbe essere volontario se il rifiuto del consenso comporta uno svantaggio non correlato alla finalità del trattamento o sproporzionato rispetto ad essa. Tuttavia, qualsiasi altro svantaggio derivante dal rifiuto del consenso non pregiudica la validità del consenso stesso.

34 Esempi: Il consenso alla verifica del merito creditizio per l'ottenimento di una carta di credito è dato volontariamente ed è lecito, in quanto senza il consenso lo svantaggio di non ricevere la carta di credito è proporzionato.

L'impossibilità di partecipare a un programma assicurativo è direttamente correlata al trattamento dei dati per il quale si ottiene il consenso; e il fatto che vengano pubblicizzati benefici monetari e bonus in denaro per un massimo di 75,00 franchi all'anno solo per le persone con un'assicurazione di base non mette in discussione la natura volontaria del consenso. Tuttavia, la minaccia di licenziamento in caso di mancato consenso al trattamento dei dati non previsto dal contratto di lavoro è considerata involontaria perché sproporzionata.

In alcuni casi, il consenso volontario si presume solo se esiste una ragionevole alternativa. Secondo il parere espresso in questa sede, a parte situazioni eccezionali (in particolare posizione dominante sul mercato, dipendenze sociali o di fatto), non è richiesta alcuna alternativa per affermare la volontarietà. Pertanto, se il consenso non viene dato, alla persona interessata può essere generalmente negato l'uso di un servizio. 35

La questione della volontarietà del consenso è controversa, soprattutto nel rapporto di lavoro. Alcuni sostengono che in questo contesto manchi la necessaria volontarietà o che qualsiasi trattamento dei dati che vada oltre l'art. 328b CO sia inammissibile. Altri autori si limitano a considerare l'ambito della volontarietà più ristretto, ad esempio nel senso che il dipendente deve avere a disposizione un'alternativa ragionevole. La dottrina prevalente e l'IFPDT ritengono che il trattamento dei dati che va oltre l'art. 328b cpv. 1 CO sia ammissibile solo se è vantaggioso per i dipendenti o nel loro interesse (art. 362 CO). Altri autori ritengono che il consenso che si discosta dall'art. 328b CO a scapito dei dipendenti sia valido in determinate circostanze. Secondo il Tribunale federale, sebbene il trattamento dei dati contrario all'art. 328b CO sia illegale, può essere basato su una giustificazione ai sensi dell'art. 13 aDSG. Secondo questa opinione, l'art. 328b CO è quindi un principio di trattamento e non una disposizione di divieto. Tuttavia, le brevi spiegazioni in merito sono state criticate dalla dottrina. Il Tribunale federale ha successivamente confermato la sua opinione, ma senza fare riferimento alla sua precedente decisione. 36

Secondo l'opinione espressa in questa sede, il consenso nel rapporto di lavoro non è escluso di per sé e può essere dato anche a un trattamento che va oltre l'art. 328b cpv. 1 CO. Il fattore decisivo in questo caso è se siano state fornite o meno informazioni adeguate e se si possa presumere che il consenso sia effettivamente volontario sotto forma di opzione di rifiuto senza conseguenze 37

negative. Ad esempio, è possibile dare il consenso alla pubblicazione di foto dei dipendenti senza contatto con i clienti su Internet o anche a fini pubblicitari, a condizione che siano state fornite informazioni sul relativo trattamento e che il dipendente abbia un'effettiva libertà di scelta. La posizione del dipendente e il suo ciclo di vita (candidatura, rapporto di lavoro in corso, cessazione) possono essere determinanti per questa valutazione. D'altro canto, nell'ultimo esempio citato al n. 34 si dovrebbe ipotizzare una mancanza di volontarietà.

38 Nel contesto europeo, la questione dei cosiddetti "dark patterns" o "nudging" deve essere presa in considerazione per la questione della volontarietà, soprattutto nell'ambito dei cookie banner. Secondo la giurisprudenza e l'opinione delle autorità di vigilanza, invogliare gli utenti a dare il proprio consenso, ad esempio attraverso un design di colore e dimensioni diseguali dei pulsanti "Accetta" e "Rifiuta" o uno sforzo aggiuntivo per rifiutare (ad esempio, offrendo un pulsante "Rifiuta tutto" solo al secondo livello di visualizzazione, dopo aver cliccato su "Continua"), mette in discussione la volontarietà. È discutibile se questo sviluppo acquisterà importanza anche in Svizzera. Il diritto svizzero, infatti, non richiede generalmente il consenso per i cookie. L'art. 45c lit. b TCA richiede solo che gli utenti "siano informati del trattamento e delle sue finalità e che possano rifiutare il trattamento". Tuttavia, sarà necessario monitorare gli ulteriori sviluppi in questo senso, poiché l'IFPDT e altri ritengono generalmente che il tracciamento costituisca una violazione giustificabile della privacy.

39 Il DSGVO prevede che si possa dare un consenso granulare per diverse operazioni di trattamento. Questo è uno dei motivi per cui i banner di cookie conformi alla legge europea spesso offrono la possibilità di acconsentire a ogni singolo cookie separatamente. Naturalmente, l'utilità di tale granularità per i cookie è discutibile. Dopo tutto, è piuttosto improbabile che una persona voglia dare il proprio consenso a certi singoli cookie e non ad altri. Poiché tale requisito di granularità non può essere dedotto dalla LPD, può essere richiesto solo in casi eccezionali.

G. Inequivocabilità

40 La bozza della LPD prevedeva ancora che il consenso dovesse essere dato "in modo non ambiguo". A questo proposito, il dispaccio afferma che la dichiarazione della persona interessata deve indicare inequivocabilmente la

sua volontà, che dipende dalle circostanze del singolo caso, e che quanto più sensibili sono i dati personali in questione, tanto più chiaro deve essere il consenso sulla base del principio di proporzionalità.

Tuttavia, il requisito dell'inequivocabilità è stato abbandonato dal Parlamento e quindi non è stato incluso nella formulazione dell'art. 6 cpv. 6 LPD. Tuttavia, il fatto che il messaggio faccia riferimento a questo criterio ha apparentemente creato confusione tra gli studiosi. 41

Il messaggio del 2003 affermava già che, in base al principio di proporzionalità, quanto più sensibili sono i dati personali in questione, tanto più chiaro deve essere il consenso. Ciò riguarda la chiarezza della dichiarazione d'intenti, il che significa che vi sono paralleli con il criterio dell'"atto affermativo non ambiguo" presente nel DSGVO. In alternativa alla "dichiarazione", questo rappresenta il secondo caso d'uso di "espressione inequivocabile di volontà" ai sensi dell'art. 4 n. 11 del DSGVO. Tuttavia, in assenza di un criterio corrispondente nella LPD, a differenza del DSGVO, non se ne può dedurre che il consenso sia inammissibile, ad esempio barrando una casella. Ciò non contraddice necessariamente il requisito della "privacy by default" ai sensi dell'art. 7 cpv. 3 LPD. 42

Tuttavia, un'interpretazione del criterio dell'univocità in conformità con l'ETS 108 rivisto richiederebbe che il consenso sia dato "senza ambiguità". Questo requisito può riguardare sia la forma che il contenuto della dichiarazione. Il messaggio suggerisce che l'elemento si riferisce alla forma. Se è così, il legislatore ha tenuto conto di questo requisito formale affermando che il consenso mediante silenzio non è generalmente sufficiente. Nella misura in cui il contenuto deve essere influenzato, si applica in ogni caso il principio secondo cui i requisiti variano in base al principio di proporzionalità. Pertanto, secondo il diritto svizzero, il criterio dell'univocità non avrebbe alcun significato autonomo. 43

H. Forma

Il consenso può essere dato senza forma. A parte le eccezioni legali, è quindi possibile anche il consenso verbale. Tuttavia, poiché l'onere della prova del consenso ricade sull'incaricato del trattamento, il consenso documentabile è la scelta più ovvia. Ciò relativizza, almeno de facto, la libertà fondamentale di forma. 44

45 In linea di principio, il consenso può essere ottenuto anche nell'ambito di termini e condizioni generali. Tuttavia, se in questo caso si fa un'ipotesi globale, si applica la regola dell'inusualità, secondo la quale i consensi inusuali sono inefficaci a scapito dell'interessato. Inoltre, entra in gioco la regola dell'ambiguità, secondo la quale le formulazioni poco chiare sono a carico dell'autore in caso di dubbio.

46 Tranne che nel caso dell'espressività richiesta dall'art. 6 cpv. 7 LPD, il consenso può essere dato anche implicitamente. In questo caso, la dichiarazione di volontà non risulta dalla dichiarazione stessa, ma da un comportamento che può essere inteso come una chiara espressione di volontà in base alle circostanze. È il caso, ad esempio, di chi rende accessibili i propri dati.

47 Il consenso implicito è spesso usato come sinonimo di consenso tacito, ma questo dovrebbe essere evitato. Il silenzio o l'inattività non comportano in genere un consenso valido (cfr. art. 6 CO), a meno che le parti non abbiano concordato il silenzio come consenso.

48 In casi eccezionali di urgenza, è possibile ipotizzare un consenso presunto, ad esempio nel caso di pazienti incoscienti. Tuttavia, l'importanza di tale consenso è trascurabile, poiché in questi casi probabilmente si applicherebbe comunque una giustificazione basata sul prevalente interesse della persona interessata. A volte viene fatta una distinzione tra consenso presunto e consenso ipotetico. Secondo questa distinzione, il consenso dovrebbe essere valido nonostante la mancanza di informazioni adeguate, in quanto l'interessato avrebbe acconsentito anche se fosse stato pienamente informato. Tuttavia, non c'è quasi spazio per questo, a meno che l'interessato non lo autorizzi successivamente sotto forma di rinuncia a far valere i propri diritti.

III. CONSENSO ESPLICITO (ART. 6 CPV. 7 LPD)

49 Se è necessario il consenso per il trattamento di dati personali particolarmente sensibili, per la profilazione ad alto rischio da parte di un privato o per la profilazione da parte di un organismo federale, questo deve essere dato espressamente. Ciò significa che il consenso non è generalmente richiesto nemmeno per questi trattamenti. Sebbene le dichiarazioni nel dibattito parlamentare abbiano talvolta suggerito il contrario, la formulazione dell'art. 6 cpv. 7 LPD non lo prevede nell'introduzione, a differenza di quella

dell'art. 6 cpv. 6 LPD, e l'IFPDT e la dottrina sostengono talvolta il contrario, ciò deriva dal chiarimento nel dibattito parlamentare e dal fatto che non deve essere apportata alcuna modifica alla situazione giuridica.

Oltre ai requisiti dell'art. 6 cpv. 6 LPD, va osservato il criterio dell'espressività. 50
Ciò era meglio espresso nell'art. 4 cpv. 5 LPD e nella bozza preliminare della LPD, in quanto il consenso "normale" e quello esplicito erano disciplinati nello stesso paragrafo e l'aggiunta "in aggiunta" lo chiariva.

È controverso se l'elemento più rigoroso dell'esplicitezza riguardi solo la 51
forma o anche il contenuto del consenso. Per quanto riguarda la forma, l'espresso è inteso come il contrario dell'implicito. Tuttavia, il consenso scritto non è richiesto. In base all'art. 1 CO, la questione dell'espressività è determinata dal fatto che la volontà espressa risulti direttamente dalla dichiarazione di intenti sotto forma di parole scritte o parlate o di un segno. In altre parole, il modo in cui viene espressa la volontà deve già fornire chiarezza sull'intenzione. Esempi di segni espliciti sono la spunta attiva di una casella, la selezione attiva di determinati parametri tecnici per i servizi informatici, l'annuire con la testa in segno di assenso durante un trattamento medico o l'aprire la bocca per rimuovere la mucosa dalla guancia dopo essere stati informati in tal senso. Per motivi di onere della prova, tuttavia, è nuovamente richiesto un consenso documentabile.

Secondo alcuni studiosi e l'IFPDT, l'espressività si riferisce anche al 52
contenuto. Nel caso del consenso espresso, il comportamento affermativo deve riguardare il trattamento dei dati in questione e non solo l'azione che porta a tale trattamento. Il consenso a ricevere pubblicità personalizzata non includerebbe quindi il consenso esplicito alla profilazione ad alto rischio su cui si basa la pubblicità.

Secondo l'opinione espressa in questa sede, il requisito dell'esplicitezza 53
riguarda la forma del consenso e non il suo contenuto. Il Dispaccio del 2003 afferma: "Il consenso non è vincolato a una forma specifica e può essere dato tacitamente o implicitamente, purché non riguardi il trattamento di dati particolarmente sensibili o di profili della personalità". In conformità al principio di proporzionalità, si presume già che quanto più sensibili sono i dati personali in questione, tanto più chiaro deve essere il consenso". Per la seconda frase, il dispaccio rimanda a un riferimento bibliografico che intende espressamente il consenso come il contrario del consenso implicito.

L'elemento dell'interpretazione storica conferma questa constatazione, soprattutto perché il dispaccio del 2017 afferma che non ci si deve discostare dalla situazione giuridica attuale.

IV. REVOCA

54 Il consenso può essere revocato in qualsiasi momento e senza alcuna giustificazione. Tuttavia, la revoca in un momento inopportuno può far scattare la responsabilità per danni. La revoca ha effetto solo per il futuro, il che significa che la legalità del trattamento già avvenuto non è influenzata dalla revoca. Tuttavia, un trattamento precedente può essere contestato per mancanza di consenso. I dati trattati sulla base del consenso possono essere cancellati se non vi sono altre giustificazioni per un ulteriore trattamento sotto forma di conservazione.

55 Secondo la Corte Suprema Federale, i dati personali che non fanno parte dell'area centrale dell'esistenza umana, come il nome, la voce o l'immagine, possono essere organizzati irrevocabilmente se l'obbligo contrattuale è basato su interessi economici. Tuttavia, la misura in cui queste considerazioni sul diritto alla propria immagine possono essere generalizzate non è del tutto chiara. Nel caso in esame, uno dei fattori decisivi è stato il fatto che la cancellazione fosse possibile dietro il pagamento di una moderata tassa di cancellazione sotto forma di penale contrattuale.

V. CONSEGUENZE LEGALI DEL CONSENSO MANCANTE, NON VALIDO O REVOCATO

56 Se un determinato trattamento richiede il consenso e questo non viene dato (in tempo utile) o non soddisfa i requisiti di validità, il trattamento corrispondente è illegale o costituisce una violazione dei diritti della personalità. Anche la prosecuzione del trattamento nonostante la revoca del consenso costituisce una violazione dei diritti della personalità (art. 30 cpv. 2 lett. b LPD).

57 In questi casi, il responsabile del trattamento può invocare altre giustificazioni (art. 31 LPD) come giustificazione secondaria. Tuttavia, se non si applica nessun'altra giustificazione, si può ricorrere contro i responsabili del trattamento privati (art. 32 cpv. 2 LPD) o gli organi federali (art. 41 LPD) e, se

necessario, l'IFPDT adotta misure investigative e amministrative (art. 49 e segg. LPD).

La violazione degli artt. 6 cpv. 6 e 7 LPD non è direttamente punibile. 58
Tuttavia, è possibile una sanzione indiretta, in particolare nel caso di divulgazione di dati personali all'estero sulla base di un consenso non valido o revocato, a condizione che la divulgazione sia proseguita sulla base di tale consenso (art. 61 lett. a in combinato disposto con l'art. 17 cpv. 1 lett. a LPD). Inoltre, in particolare nel settore della pubblicità elettronica di massa, la mancanza di consenso ai sensi dell'art. 3 cpv. 1 lett. o LCSl può comportare sanzioni ai sensi dell'art. 23 LCSl.

VI. CONSIGLI PRATICI

Nella pratica, a volte si ottiene il consenso per trattamenti che non lo 59
richiedono. Talvolta si sostiene che l'obbligo di trasparenza o il principio di buona fede vietino di ottenere un consenso non necessario. Tale rigore non è generalmente appropriato perché la questione della necessità del consenso è spesso associata all'incertezza giuridica. Tuttavia, poiché il consenso può essere revocato in qualsiasi momento, è necessario esaminare prima le giustificazioni alternative.

Su Internet si trovano spesso formulazioni come "Accetto l'informativa sulla 60
privacy", "Accetto l'informativa sulla privacy" o simili. Tuttavia, un'informativa sulla privacy dovrebbe fornire solo informazioni unilaterali e non costituire un contratto bilaterale. Nel caso di un trasferimento globale, anche la regola dell'inusualità ha un effetto restrittivo. L'informativa sulla privacy dovrebbe quindi essere solo collegata e il consenso dovrebbe essere ottenuto separatamente e con cautela.

VII. CRITICHE ALLA NORMA

Secondo il dispaccio sulla nuova legge sulla protezione dei dati, uno dei 61
principi guida della revisione era il rafforzamento dei diritti degli interessati, che doveva essere supportato anche da una definizione più precisa dei requisiti per un consenso valido da parte dell'interessato. Non si può presumere che questo obiettivo venga raggiunto grazie al chiarimento dei requisiti per il consenso. Da un lato, la situazione giuridica non è cambiata. D'altro canto, le dichiarazioni di consenso, proprio come le dichiarazioni di

protezione dei dati, non vengono quasi mai lette. Questo può portare a un "sovraccarico di informazioni" e alla stanchezza da clic, soprattutto se, oltre alla dichiarazione di consenso ai sensi della legge sulla protezione dei dati, si ottiene il consenso ai termini e alle condizioni generali e si porta all'attenzione dell'utente la dichiarazione sulla protezione dei dati.

BIBLIOGRAFIA

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).

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 7 LPD

Un commentario di Samuel Klaus

CITAZIONE SUGGERITA

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

Breve citazione: OK-Klaus, N. XXX zu Art. 7 DSG.

Art. 7 Protezione dei dati personali sin dalla progettazione e per impostazione predefinita

[1] Il titolare del trattamento è tenuto ad adottare i provvedimenti tecnici e organizzativi necessari affinché il trattamento dei dati personali sia conforme alle disposizioni sulla protezione dei dati, in particolare ai principi di cui all'articolo 6. Li adotta sin dalla progettazione.

[2] I provvedimenti tecnici e organizzativi devono essere adeguati in particolare allo stato della tecnica, al tipo e all'entità del trattamento dei dati personali come pure ai rischi derivanti dal trattamento per la personalità o i diritti fondamentali delle persone interessate.

[3] Il titolare del trattamento è tenuto a garantire, mediante appropriate impostazioni predefinite, che il trattamento di dati personali sia

circoscritto al minimo indispensabile per lo scopo perseguito, salvo che la persona interessata disponga altrimenti.

STRUTTURA

In breve 140
I. Aspetti generali 140
A. Osservazioni preliminari e contesto 140
B. Destinatari 141
II. Protezione dei dati attraverso la tecnologia / privacy by design (cpv. 1-2) 142
A. Concetto e contesto 142
B. Contenuto e ambito di applicazione (cpv. 1) 144
C. Adeguatezza (cpv. 2) 144
D. Attuazione nella pratica 145
1. Standard internazionali 146
2. Guide e ausili per l'orientamento 148
3. Esempi di misure possibili 150
III. Impostazioni predefinite favorevoli alla protezione dei dati / privacy by default (cpv. 3) 153
A. Termine 153
B. Contenuto e ambito di applicazione 153
C. Attuazione nella pratica 154
IV. Conseguenze della violazione degli obblighi 156
V. Disposizioni transitorie 157
Bibliografia 158
I Materiali 159

IN BREVE

Privacy by Design e Privacy by Default sono i principi guida per l'attuazione della protezione dei dati. Secondo il principio della privacy by design, è necessario adottare misure appropriate in anticipo, già nella fase di pianificazione del trattamento dei dati, al fine di garantire una protezione sistemica dei dati. Se gli interessati o gli utenti hanno a disposizione diverse opzioni di impostazione/scelta, il principio della privacy by default dovrebbe garantire che l'impostazione predefinita rifletta la combinazione di opzioni più rispettosa della protezione dei dati.

I. ASPETTI GENERALI

A. Osservazioni preliminari e contesto

1 La premessa che i requisiti di protezione dei dati devono essere attuati mediante misure tecniche appropriate era già applicata nella legge precedente, poiché i requisiti dell'art. 4 aDSG (principi) e dell'art. 7 aDSG (sicurezza dei dati) non potevano essere raggiunti in altro modo. La nuova legge sulla protezione dei dati esprime esplicitamente questo concetto nell'art. 7 LPD con i due principi "Privacy by Design" (protezione dei dati attraverso la tecnologia, art. 7 cpv. 1-2 LPD) e "Privacy by Default" (impostazioni predefinite favorevoli alla protezione dei dati, art. 7 cpv. 3 LPD). Dal punto di vista del contenuto, l'art. 7 LPD va letto insieme all'art. 6 LPD (principi) e all'art. 8 LPD (sicurezza dei dati): Le misure tecniche e organizzative utilizzate da Privacy by Design ("LPD") devono in particolare consentire l'attuazione dei principi di cui all'art. 6 della FADP, e la garanzia della sicurezza dei dati (art. 8 della FADP) rappresenta - tra gli altri - uno dei punti focali rilevanti. Un importante aspetto secondario della LPD è inoltre specificamente menzionato nell'art. 7, cpv. 3, della LPD con il principio della "Privacy by Default" ("PbDefault").

2 Lo scopo normativo dell'art. 7 LPD è fortemente programmatico e quindi difficile da cogliere nell'attuazione concreta: L'intento della PbDesign è quello di creare le condizioni sistemiche per l'adempimento e la garanzia (permanente) della protezione dei dati. Resta da vedere se ciò sia utile alla luce della ristretta cerchia di destinatari (cfr. sezione B).

In termini di dogma giuridico, l'introduzione di PbDesign e PbDefault risale all'art. 10 cpv. 2-4 dell'ER-Conv 108+, che sarà ratificato con l'entrata in vigore della LPD rivista. Per gli organi federali, PbDesign e PbDefault sono già prescritti nell'ambito della FADP dal 1° marzo 2019 (art. 5 FADP). L'SDSG sarà abrogato con l'entrata in vigore della revisione della LPD e l'obbligo di PbDesign e PbDefault sarà quindi disciplinato per tutti i destinatari nella LPD. L'art. 7 DPA attua i requisiti dell'art. 10 cpv. 2-4 dell'ER-Conv 108+ (cfr. art. 4 cpv. 1 dell'ER-Conv 108+), in modo simile ma non identico all'art. 25 DPA per gli Stati membri dell'UE. 3

L'art. 25 del DSGVO (protezione dei dati per concezione e per impostazione predefinita) attua quindi gli stessi requisiti generali, utilizzando gli stessi termini e con la stessa spinta - ma sullo sfondo leggermente diverso del sistema del DSGVO. Per l'applicazione, l'interpretazione e l'attuazione dell'art. 7 DPA, la letteratura e la giurisprudenza sull'art. 25 DPA possono quindi essere utili, anche se occorre tenere conto di alcune differenze: In particolare, nell'applicazione analoga delle linee guida sviluppate per l'attuazione dell'art. 25 LPD si deve tenere conto del diverso punto di partenza per quanto riguarda il trattamento dei dati (principio del divieto con riserva di autorizzazione ai sensi del DSGVO rispetto al trattamento dei dati fondamentalmente consentito con restrizioni e possibilità di giustificazione ai sensi della LPD). Resta da vedere se l'attuazione dei principi di LPD e di LPD di default comporterà differenze significative rispetto a quelli previsti dal DSGVO. Da un punto di vista pragmatico, ciò dovrebbe essere evitato a favore di un'applicazione il più possibile uniforme di questi principi fondamentali. 4

B. Destinatari

I destinatari delle disposizioni dell'art. 7 LPD sono i responsabili del trattamento dei dati, per cui si rivolgono sia i privati che gli enti federali. L'idea di base e lo scopo del PbDesign dovrebbero riguardare in particolare anche i progettisti, i produttori e i distributori di sistemi, applicazioni e altri strumenti utilizzati per il trattamento dei dati. Tuttavia, questi non rientrano nell'ambito di applicazione dell'art. 7 LPD, o vi rientrano solo indirettamente attraverso l'obbligo dei responsabili del trattamento. 5

Mentre i responsabili del trattamento dei dati sono quindi direttamente obbligati ad attuare i requisiti dell'art. 7 LPD, l'idea di base della "protezione sistemica dei dati" viene attuata solo indirettamente nei confronti degli attori a 6

monte della catena del valore: Ai sensi dell'art. 7 LPD, i responsabili del trattamento dei dati sono tenuti ad adottare misure adeguate per garantire che i servizi e i prodotti a monte siano progettati in modo tale che essi (i responsabili del trattamento dei dati) possano adempiere ai loro obblighi di PbDesign e PbDefault ai sensi dell'art. 7 LPD. Le parti responsabili devono tenerne conto, ad esempio attraverso requisiti contrattuali nei confronti dei fornitori di servizi o dei fornitori, una corrispondente progettazione dei requisiti di approvvigionamento, ecc.

II. PROTEZIONE DEI DATI ATTRAVERSO LA TECNOLOGIA / PRIVACY BY DESIGN (CPV. 1-2)

A. Concetto e contesto

7 Il concetto di PbDesign si basa sull'idea che i mezzi tecnici non dovrebbero ostacolare, ma piuttosto consentire e persino promuovere l'attuazione dei requisiti di protezione dei dati. Originariamente discusso nell'ambito di specifiche tecnologie di miglioramento della privacy (PET), il PbDesign si è evoluto nel tempo in un concetto più ampio. Non esiste una definizione generalmente vincolante, ma il termine viene utilizzato a seconda del contesto.

8 Il concetto di PbDesign è stato plasmato in modo significativo da Ann Cavoukian (Privacy Commissioner dell'Ontario, Canada, dal 1997 al 2014), con un concetto di PbDesign basato su 7 principi (principi in corsivo, enfasi in grassetto secondo l'implementazione della Cavoukian):

1. *Proactive* not *Reactive*; **Preventative** not *Remedial*: il PbDesign deve essere inteso come un concetto proattivo e anticipatorio e mira a prevenire le violazioni della protezione dei dati (e non a rimediare a violazioni già avvenute).

2. *Privacy as the Default Setting*:: anche se l'interessato non intraprende alcuna azione specifica, la protezione dei dati deve essere garantita nel modo più completo possibile, cfr. infra III - Impostazioni predefinite amichevoli per la protezione dei dati / Privacy per impostazione predefinita (cpv. 3).

3. *Privacy Embedded into Design*: la protezione dei dati deve essere considerata in modo integrale già nella progettazione e nell'implementazione di sistemi e processi.

4. *Full Functionality - Positive Sum, not Zero-Sum*: la protezione dei dati non deve impedire o portare a restrizioni funzionali, ma creare valore aggiunto attraverso la sua considerazione integrale.

5. *End-to-End Security - Full Lifecycle Protection*: la sicurezza dei dati deve essere garantita durante l'intero ciclo di vita dei dati stessi.

6. *Visibility and Transparency - Keep it Open*: devono essere garantite trasparenza e verificabilità.

7. *Respect for User Privacy - Keep it User-Centric*:: gli interessi degli interessati devono essere presi in considerazione.

9 Questi principi di base possono servire come linee guida e aiuti alla comprensione. A causa del loro orientamento piuttosto programmatico, sono difficilmente adatti come ausili concreti per l'attuazione. Nel testo della legge, si possono trovare almeno riferimenti al Principio 1 - Proattivo/Preventivo (nell'art. 7 cpv. 1 LPD con l'approccio preventivo e il riferimento alla considerazione fin dalla fase di pianificazione), al Principio 2 - Impostazione predefinita (nell'art. 7 cpv. 3 LPD per quanto riguarda le impostazioni predefinite rispettose della protezione dei dati) e al Principio 3 - Incorporato (nell'art. 7 cpv. 1 LPD con l'obbligo di progettare il trattamento dei dati tenendo conto dei requisiti di protezione dei dati e della considerazione fin dalla fase di pianificazione). Il principio 5 - Protezione dell'intero ciclo di vita è poi trattato nell'art. 8 cpv. 2 LPD e il principio 1 - Proattivo/Preventivo nell'art. 8 cpv. 1 LPD.

10 Per l'attuazione pratica, possono essere utili le linee guida esistenti di carattere generale (come le linee guida EDSA 4/2019 sull'articolo 25 del DSGVO o lo standard ISO 31700 sulla privacy by design) e le linee guida specifiche per settore o applicazione (si veda la sezione D - Attuazione nella pratica). Nell'implementazione di tali linee guida, occorre tenere conto delle differenze derivanti dal fatto che molte di esse sono orientate al DSGVO.

B. Contenuto e ambito di applicazione (cpv. 1)

11 Il PbDesign mira a eliminare o almeno a ridurre il rischio di violazione delle disposizioni in materia di protezione dei dati attraverso precauzioni tecniche, ma senza puntare a una tecnologia specifica. Piuttosto, nella progettazione dei sistemi, delle applicazioni e dei processi utilizzati dovrebbero essere implementate misure tecniche e organizzative adeguate ("TOM"). Nel fare ciò, non si deve considerare solo uno specifico sistema, una singola applicazione o uno specifico aspetto tecnico, ma nel senso di un "approccio olistico" all'intero trattamento dei dati, con particolare attenzione all'attuazione dei principi di cui all'art. 6 LPD.

12 Da un punto di vista temporale, la PbDesign deve essere presa in considerazione già al momento della pianificazione del trattamento dei dati (art. 7 cpv. 1 frase 2 LPD). Se deve essere effettuata una valutazione d'impatto sulla protezione dei dati ("DIA") ai sensi dell'art. 22 LPD, i TOM previsti per l'implementazione della PbDesign possono essere inclusi nel processo DIA ed elencati come misure ai sensi dell'art. 22 cpv. 3 LPD. Tuttavia, l'obbligo di effettuare la PbDesign e l'obbligo di effettuare una DIA sono indipendenti l'uno dall'altro, vale a dire che l'obbligo di effettuare la PbDesign esiste anche se non esiste un "rischio elevato" ai sensi dell'obbligo di effettuare una DIA ai sensi dell'Art. 22 (1) LPD.

C. Adeguatezza (cpv. 2)

13 I modelli di gestione del rischio da implementare nell'ambito della PbDesign devono essere "adeguati", il che esprime l'approccio basato sul rischio di questa disposizione. Come criteri rilevanti per valutare l'adeguatezza, l'art. 7(2) LPD cita "in particolare" (a) lo stato dell'arte, (b) il tipo e la portata del trattamento dei dati e (cpv.) il rischio per la personalità o i diritti fondamentali delle persone interessate. L'elenco non è esaustivo; è decisiva la visione d'insieme, tenendo conto delle circostanze specifiche.

14 Lo stato dell'arte si riferisce a un livello avanzato di sviluppo tecnico che si è dimostrato nell'applicazione pratica o si è affermato sul mercato. Ciò include anche la fattibilità economica da un punto di vista generale e oggettivo (non quello della rispettiva persona responsabile). Poiché lo stato dell'arte è in continua evoluzione, soprattutto in campo digitale, l'implementazione del PbDesign comporta anche l'obbligo di verificare regolarmente se il TOM

implementato corrisponde ancora all'attuale stato dell'arte o se deve essere adattato, se necessario: L'art. 7 cpv. 1 LPD stabilisce a questo proposito che la LPD deve essere presa in considerazione "fin" (e non solo "durante") la fase di pianificazione.

Il tipo e l'ambito del trattamento dei dati si riferiscono alle componenti contenutistiche e quantitative del trattamento: dal punto di vista contenutistico, è particolarmente importante quali dati (categorie) vengono trattati in che modo e per quale scopo. Dal punto di vista quantitativo, si deve tenere conto sia dell'ambito dei soggetti interessati (ossia il numero di soggetti) sia dell'ambito delle categorie di dati trattati (ossia il numero di record di dati). 15

Il rischio per le persone interessate è il parametro generale per valutare l'adeguatezza della TOM. Quanto più alto è il rischio, cioè quanto maggiore è la probabilità che si verifichi e le potenziali conseguenze, tanto più alti sono i requisiti perché le disposizioni tecniche siano considerate adeguate. Strumenti chiaramente strutturati e matematico-probabilistici possono essere un aiuto nella valutazione del rischio. Tuttavia, dovrebbero servire solo come punto di partenza, poiché la valutazione del rischio deve essere effettuata da una prospettiva olistica e contenutistica e deve prendere in considerazione tutti gli aspetti (non solo quelli probabilistici). 16

Nel valutare l'adeguatezza, in genere si dovrebbe applicare uno standard basato sul rischio piuttosto che assoluto. In questo modo, il rischio associato a un trattamento deve essere messo in relazione con le possibilità tecniche di ridurlo. Il principio della PbDesign mira a creare un equilibrio appropriato per il conflitto di obiettivi tra trattamento e protezione dei dati. Nel senso del Principio 4 - Somma positiva, non somma zero, formulato da Cavoukian (cfr. n. 8 sopra), il trattamento dei dati non dovrebbe essere impedito, ma piuttosto reso possibile con il dovuto riguardo per i requisiti di protezione dei dati, al fine di creare un valore aggiunto per i responsabili del trattamento e gli interessati. 17

D. Attuazione nella pratica

Non esiste una ricetta semplice per il successo su come implementare la PbDesign in modo universale. La PbDesign deve essere intesa come un processo specifico per ogni progetto. Di conseguenza, non esiste una 18

procedura universale che possa coprire tutti i casi d'uso. Piuttosto, il TOM da implementare deve essere orientato (1.) alle specificità del rispettivo trattamento dei dati, (2.) all'ambiente settoriale in cui si svolge e (3.) ai sistemi e ai processi esistenti in cui è incorporato (e anche questi devono essere adattati, se necessario). Il successo dell'implementazione della PbDesign richiede quindi che i rischi e i requisiti specifici del progetto o del processo siano registrati e affrontati con misure concrete su misura. Le misure per l'attuazione della sicurezza dei dati (art. 8 LPD, artt. 1-6 LPD) riguardano solo una sottoarea (anche se molto rilevante) (cfr. n. 30).

19 Si raccomanda una procedura chiaramente strutturata basata sulle linee guida pertinenti al caso di applicazione, integrata da ulteriori chiarimenti e specifiche proprie in base alle caratteristiche specifiche del progetto. Questa procedura dovrebbe essere sufficientemente documentata per consentire una revisione e un aggiornamento successivi (ad esempio, a causa di modifiche tecniche, di ulteriori sviluppi dello stato dell'arte, di adeguamenti del business case, ecc.)

20 Si possono consultare diversi strumenti di orientamento, come gli standard internazionali, le best practice delle associazioni di settore, le linee guida delle autorità di protezione dei dati, ecc. È importante notare che tali indicazioni possono essere utili come punto di partenza, ma devono sempre essere integrate con i requisiti del caso d'uso specifico e con lo stato attuale dell'arte. Occorre inoltre tenere presente che molte di queste linee guida sono state formulate tenendo conto dell'articolo 25 del DSGVO. Nell'utilizzarle, occorre quindi tenere conto di eventuali differenze nell'ambito della LPD, come in particolare la diversa posizione di partenza rispetto al trattamento dei dati (principio del divieto con riserva di autorizzazione ai sensi del DSGVO rispetto al trattamento dei dati fondamentalmente consentito con restrizioni e possibilità di giustificazione ai sensi della LPD).

1. Standard internazionali

21 L'Organizzazione internazionale per la standardizzazione (ISO) ha pubblicato lo standard ISO 31700 sulla privacy by design nel febbraio 2023. Questo è diviso in due parti: ISO 31700-1:2023 (https://www.iso.org/standard/84977.html) e ISO/TR 31700-2:2023 (https://www.iso.org/standard/84978.html).

Ad esempio, la sezione 4.4 - Progettazione dell'interfaccia uomo-computer (HCI) per la privacy, la sezione 7.2 - Integrazione della progettazione e del funzionamento dei controlli sulla privacy nel ciclo di vita dello sviluppo e della gestione del prodotto, o la sezione 8.2 - Progettazione dei controlli sulla privacy per il ritiro e la fine dell'utilizzo). Poiché la norma ISO non si basa su un fondamento specifico della legge sulla protezione dei dati, essa contiene, oltre a questi requisiti specifici per la progettazione, anche specifiche su aspetti fortemente influenzati dalla legge sulla protezione dei dati applicabile (a livello locale) (come la sezione 5.2 - Fornitura di informazioni sulla privacy, la sezione 5.4 - Risposta alle richieste e ai reclami dei consumatori o la sezione 6.2 - Conduzione di una valutazione del rischio per la privacy). Tali requisiti devono pertanto essere sempre letti in combinazione con le disposizioni di legge pertinenti, come ad esempio gli artt. 19 e segg. LPD per quanto riguarda l'obbligo di informazione, l'Art. 22 f. LPD per quanto riguarda la valutazione dell'impatto sulla protezione dei dati, ecc. Tuttavia, possono anche servire come base per una procedura strutturata a questo proposito. 22

La seconda parte (ISO/TR 31700-2:2023 - Protezione dei consumatori - Privacy by design per beni e servizi di consumo - Parte 2: Casi d'uso) contiene tre casi d'uso illustrativi che dimostrano l'implementazione dei requisiti della prima parte: (1) Vendita al dettaglio on line (negozio on line di commercio elettronico); (2) Azienda di fitness (centro fitness con dispositivi collegati tramite sensori a un'app di fitness dell'utente); e (3) Serrature intelligenti (linea di prodotti di serrature elettroniche IoT per porte con connessione on line e relativa app di controllo). I casi d'uso coprono molti aspetti pratici. L'implementazione chiaramente strutturata delle specifiche della prima parte nei casi d'uso può quindi servire non solo per familiarizzare con l'argomento, ma anche direttamente come lista di controllo per l'implementazione di singoli aspetti rilevanti. 23

In conclusione, si può affermare che gli standard ISO 31700-1/2 sono mantenuti a un alto livello di astrazione a causa del loro orientamento generalmente valido. Ciononostante, possono servire come buona base grazie alla loro chiara strutturazione. I casi d'uso orientati alla pratica possono essere utili anche come liste di controllo per gli aspetti comparabili nei diversi casi d'uso. 24

2. Guide e ausili per l'orientamento

25 Esistono molte guide generali e sussidi di orientamento. Il seguente elenco può servire come punto di partenza per le vostre ricerche. Per una panoramica concettuale, la linea guida EDSA 4/2910 sull'articolo 25 [DSGVO] dell'Autorità europea di vigilanza sulla protezione dei dati (EDSA) è adatta, mentre i Privacy Patterns possono servire come introduzione più pragmatica:

- **EDSA Guideline 4/2019 on Article 25 - Privacy by Design and by Default** (EDPB - European Data Protection Board / EDSA - European Data Protection Board, version 2.0 of 20.10.2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_de, visited on 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/, visited 5/20/2023).
- **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/, visited 5/21/2023).
- **Data Protection by Technology Design and by Data Protection-Friendly Default Settings (Art. 25 DS-GVO)** (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, visited on 5/21/2023).
- **OIPC (Office of the Information and Privacy Commissioner) - Privacy by Design Resources (IAPP - International Association of Privacy Professionals)**, https://iapp.org/resources/article/oipc-privacy-by-design-resources/, visited on 5/21/2023).

- **Manage a privacy program - 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/, visited on 5/21/2023).
- **Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices** (Ann Cavoukian, 2012, https://collections.ola.org/mon/26012/320221.pdf, visited on 5/21/2023).
- **Privacy and Data Protection by Design - from policy to engineering** (ENISA - European Union Agency for Networks and Information Security, 2014, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design, visited on 5/21/2023).

Soprattutto nell'ambito dello sviluppo di software e applicazioni, sorgono diverse domande sull'attuazione di PbDesign e PbDefault. Le autorità preposte alla protezione dei dati e le linee guida specifiche del settore possono fornire indicazioni in merito, come ad esempio: 26

- **Privacy by Design and Privacy by Default - A Guide for Developers** (Catalan Data Protection Authority, 2023, https://apdcat.gencat.cat/web/.content/03-documentacio/documents/guiaDesenvolupadors/GUIA-PDDD_EN.pdf, visited 5/20/2023).
- **Guide: Developing privacy-compliant apps** (Data Protection Commissioner of the Canton of Zurich, 2022, https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_entwicklung_datenschutzkonformer_apps.pdf, visited on 5/20/2023).
- **eHealth Suisse - Leitfaden für App-Entwickler, Hersteller und Inverkehrbringer** (eHealth Suisse - Kompetenz- und Koordinationsstelle von Bund und Kantonen, 2022, https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/D/Leitfaden_e-Health_Suisse_fuer_App_Entwickler.pdf, visited on 5/21/2023).
- **Mobile Apps in Healthcare: Requirements from Data Protection** (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, visited on 5/21/2023).

- **American Medical Association (AMA) - Privacy is Good Business - A case for privacy by design in app development** (2021), https://www.ama-assn.org/system/files/privacy-principles-by-design.pdf, visited on 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, visited 5/21/2023).
- **Privacy Design Guidelines for Mobile Application Developmen**t (GSMA - Global System for Mobile Communications, 2018, https://www.gsma.com/publicpolicy/wp-content/uploads/2018/02/GSMA-Privacy-Design-Guidelines-for-Mobile-Application-Development.pdf, accessed 5/21/2023).
- **Guidelines on Software development with Data Protection by Design and Default** (Norwegian Data Protection Authority Datatilsynet, 2017, https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/data-protection-by-design-and-by-default/, visited on 5/21/2023).
- **Privacy by Design in Big Dat**a (ENISA - European Union Agency for Networks and Information Security, 2015, https://www.enisa.europa.eu/publications/big-data-protection, visited 5/21/2023).

3. Esempi di misure possibili

27 Le misure concrete devono essere determinate di volta in volta in base al caso d'uso specifico e al profilo di rischio associato. Il seguente elenco può servire come panoramica esemplare delle possibili misure e mostrare i punti di partenza. Può anche essere utile orientarsi su casi d'uso concreti, cfr. ad esempio Tamò-Larrieux, pag. 203 e segg. e i casi d'uso in ISO/TR 31700-2:2023 (cfr. n. 23).

28 Le possibili misure possono essere raggruppate in aspetti sistemici, aspetti più tecnici e aspetti di natura organizzativa. Gli aspetti sistemici si riferiscono (come i principi di trattamento ai sensi dell'art. 6 cpv. 1-5 LPD) in una visione olistica all'intero caso aziendale. Gli aspetti tecnici e organizzativi si intersecano con i requisiti di sicurezza dei dati (art. 8 LPD). Gli aspetti sistemici, tecnici e organizzativi si sovrappongono in molte aree e

difficilmente possono essere chiaramente distinti l'uno dall'altro. Tuttavia, utilizzando gli aspetti sistemici per far sì che alcuni argomenti di livello superiore siano per così dire "davanti alla staffa" dell'implementazione tecnico-organizzativa, si può facilitare un approccio strutturato, in particolare consentendo che gli aspetti generali di livello superiore confluiscano in tutte le considerazioni fin dalle prime fasi e siano presi in considerazione in tutte le fasi del progetto.

Da una prospettiva generale e sistemica, dovrebbero essere esaminati, ad esempio, i seguenti aspetti: 29

- **Minimizzazione dei dati (LPD 6 cpv. 2)**: I dati personali raccolti dovrebbero essere limitati in termini di contenuto (quali dati (categorie)) e di portata (quanti dati, ad esempio in termini di tempo) a quanto necessario per l'elaborazione del rispettivo caso aziendale; non dovrebbe esserci una "raccolta di dati per lo stock".
- **Segregazione dei dati**: limitare il collegamento o la messa in comune dei dati, la centralizzazione dell'archiviazione dei dati e l'aggregazione dei set di dati, ecc.
- **Pseudonimizzazione**: la pseudonimizzazione può creare una protezione aggiuntiva (nel senso di separare le informazioni di identificazione da altre categorie di dati), soprattutto se il collegamento di alcuni dati con una persona specifica è necessario solo per alcune fasi del trattamento.
- **Dichiarazione dei dati**: etichettatura dei record di dati (ad esempio tramite metadati o descrittori), ad esempio per quanto riguarda l'origine, il livello di protezione, il periodo di conservazione ("data di scadenza"), ecc.
- **Anonimizzazione e/o cancellazione (art. 6 cpv. 4 LPD)**: per attuare il principio della minimizzazione dei dati (ad es. mediante "date di scadenza" per determinati set di dati, cicli regolari di anonimizzazione/cancellazione, ecc.)

Da un punto di vista tecnico, si può fare riferimento innanzitutto alle misure tecniche necessarie per implementare la sicurezza dei dati (cfr. art. 8 LPD e le spiegazioni al riguardo negli artt. 1-6 LPD). Tuttavia, sono ipotizzabili anche altre misure tecniche che non servono (solo) alla sicurezza dei dati, ma agli obiettivi generali di protezione dei dati in generale. Ad esempio, possono essere particolarmente rilevanti le misure tecniche per l'attuazione dei 30

principi generali di trattamento (art. 6 cpv. 1-5 LPD) e del principio di minimizzazione dei dati (art. 6 cpv. 2 LPD). Si pensi, ad esempio, all'implementazione tecnica dei concetti di cancellazione (vedi sopra) o alla pixelatura automatica dei volti/degli elementi identificativi nel caso di immagini/video non personali, ecc.

31 Da un punto di vista organizzativo, è necessario creare le condizioni interne per implementare i requisiti sistemici e tecnici. Ciò può includere, ad esempio, i seguenti aspetti:

- **Cultura aziendale e visione olistica**: la cultura aziendale deve intendere la protezione dei dati come parte dell'azione aziendale (e non, come spesso accade, come una restrizione imposta dall'esterno). È quindi necessaria una "mentalità favorevole alla protezione dei dati". Inoltre, la protezione dei dati deve essere vista in modo olistico, cioè non solo in modo selettivo rispetto al proprio trattamento, ma anche, ad esempio, come parte della gestione dei contratti e dei fornitori.
- **Processi, responsabilità e documentazione**: l'implementazione di procedure e processi rilevanti per la protezione dei dati deve essere definita e sufficientemente documentata. Particolarmente importanti sono le responsabilità chiare e la documentazione sufficiente. Anche se non esiste un principio generale di responsabilità ai sensi della LPD, e potrebbe non esserci l'obbligo legale di creare un documento specifico (ad esempio un repertorio dei trattamenti, cfr. art. 12 in combinato disposto con l'art. 24 LPD), la sua creazione (almeno in forma semplificata) può comunque essere necessaria o almeno utile per poter attuare i principi della PbDesign, verificarli nel tempo e adattarli se necessario.
- **Formazione e sensibilizzazione**: per garantire che le TOM pianificate siano effettivamente messe in pratica, i dipendenti devono essere formati di conseguenza e sensibilizzati alle questioni relative alla protezione dei dati, ad esempio attraverso corsi di formazione sulla protezione dei dati, direttive e regolamenti interni, ecc.
- **Attuazione tecnica**: le misure tecniche (N. 30) devono essere integrate da corrispondenti misure organizzative per garantirne l'attuazione. Ad esempio, un'efficace restrizione dell'accesso richiede anche un processo per la concessione delle autorizzazioni di accesso, il controllo regolare del loro aggiornamento e la garanzia della loro cancellazione (ad esempio,

quando i dipendenti cambiano lavoro o mansione). Allo stesso modo, l'indicazione di una limitazione del periodo di conservazione di alcuni dati richiede un processo associato per effettuare regolarmente un controllo corrispondente e l'eventuale cancellazione.

III. IMPOSTAZIONI PREDEFINITE FAVOREVOLI ALLA PROTEZIONE DEI DATI / PRIVACY BY DEFAULT (CPV. 3)

A. Termine

PbDefault è un contenuto parziale di PbDesign (cfr. n. 8, par. 2) ed è stato formulato nell'art. 7 cpv. 3 LPD. La formulazione è fuorviante, in quanto non vi è alcun obbligo di creare opzioni di impostazione speciali (cfr. n. 35). L'obbligo di cui all'art. 7 cpv. 3 LPD si riferisce solo al fatto che, se esistono diverse opzioni di impostazione, le impostazioni predefinite devono essere impostate in modo da attuare il trattamento dei dati più "minimamente invasivo" ai sensi della legge sulla protezione dei dati. 32

Il Dispaccio descrive le impostazioni predefinite come "le impostazioni, in particolare del software, che vengono applicate per impostazione predefinita, ossia se l'utente non apporta alcuna modifica". Ciò significa l'impostazione di base, l'impostazione standard o la "configurazione predefinita" che viene applicata se l'utente non seleziona attivamente un'impostazione diversa. 33

B. Contenuto e ambito di applicazione

Anche se il messaggio cita specificamente il software come caso di applicazione, l'ambito di applicazione non è limitato alle impostazioni del software o del sistema, ma riguarda tutta l'elaborazione dei dati. Pertanto, tutte le opzioni di impostazione che esistono nell'elaborazione dei dati e in particolare nella raccolta dei dati sono generalmente coperte. Quando esistono diverse opzioni o scelte di impostazione, la combinazione di impostazioni più rispettosa della protezione dei dati deve essere fornita come impostazione di base. 34

Le impostazioni predefinite rispettose della protezione dei dati possono essere effettuate solo se sono previste diverse opzioni di impostazione. Se queste debbano essere previste deve essere esaminato l'aspetto della PbDesign (N. 7 e segg.). Le disposizioni sulla PbDefault (art. 7 cpv. 3 LPD) non 35

prevedono comunque un obbligo specifico di prevedere in ogni caso determinate opzioni di impostazione per la classificazione dell'intensità dell'intrusione ai sensi della legge sulla protezione dei dati.

36 In termini di contenuto, l'attenzione qualitativa deve essere rivolta all'entità dell'interferenza con i diritti personali o fondamentali delle persone interessate, non solo (quantitativamente) al numero e alla portata dei dati trattati. Il riferimento al principio di minimizzazione dei dati contenuto nell'invio deve essere inteso come un riferimento al principio guida del PbDefault, e non come un'indicazione che la sua attuazione debba essere affrontata in modo puramente quantitativo-tecnico.

37 La finalità del trattamento funge da parametro di riferimento (cfr. la formulazione relativa alla limitazione "al minimo necessario ai fini dell'utilizzo"). Nel determinare tale finalità, il responsabile del trattamento rimane libero, vale a dire che non vi è alcun obbligo di offrire determinati servizi anche senza la raccolta o il trattamento dei dati. Se, ad esempio, un servizio online è finanziato da pubblicità personalizzata, non vi è alcun obbligo di offrire una versione di tale servizio priva di pubblicità. Tuttavia, nell'implementazione del servizio online e del relativo trattamento dei dati per la pubblicità personalizzata, devono essere rispettati i principi di PbDesign e PbDefault.

38 Partendo dall'impostazione predefinita più rispettosa della protezione dei dati, gli interessati possono effettuare una scelta diversa e quindi consentire un trattamento dei dati più esteso. Non vi è alcun obbligo di prevedere tali ulteriori opzioni. Tuttavia, è probabile che il responsabile del trattamento lo preveda come regola nel proprio interesse, per dare agli interessati la possibilità di acconsentire a un trattamento più esteso dei dati che non sarebbe strettamente necessario per la realizzazione della finalità d'uso strettamente definita.

C. Attuazione nella pratica

39 Il punto di partenza è la finalità d'uso e il trattamento dei dati "minimamente invasivo" necessario per attuarla o raggiungerla. L'eventuale disponibilità di diverse varianti di implementazione o opzioni di impostazione/scelta deve essere decisa dalla persona responsabile sulla base del caso aziendale o d'uso e applicando i principi della PbDesign (N. 7 e segg.). In tal caso, la

combinazione di impostazioni/scelte più rispettosa della protezione dei dati deve essere fornita come impostazione predefinita o di base, ossia l'impostazione predefinita con il minore impatto sui diritti personali e fondamentali degli interessati.

Se agli interessati viene data la possibilità di discostarsi da queste impostazioni più rispettose della protezione dei dati e di consentire un ulteriore trattamento, occorre verificare se per tale ulteriore trattamento è necessario il consenso ai sensi dell'art. 6 cpv. 6 LPD e quindi devono essere rispettati i requisiti ivi previsti (ed eventualmente anche quelli dell'art. 6 cpv. 7 LPD). 40

Mentre (secondo il diritto svizzero, a differenza di quanto previsto dal DSGVO), sotto l'aspetto del consenso, anche le caselle di controllo pre-attivate ("caselle spuntate") possono essere considerate un consenso (esplicito), a seconda delle circostanze, ciò sembra essere discutibile sotto l'aspetto del PbDefault: lo scopo del PbDefault e la sua formulazione nell'Art. 6 Paragrafo 7 RPD. Lo scopo del PbDefault e la sua formulazione nell'art. 7 (3) LPD è proprio quello di consentire agli interessati di fare affidamento sul fatto che tutte le opzioni di impostazione/scelta implementino la variante più rispettosa della protezione dei dati nell'impostazione di base. 41

Ciò va osservato sotto le parole chiave del principio di fiducia e della regola dell'inusualità, in analogia con le regole di interpretazione sviluppate per le adozioni globali delle CG. Lo scopo della LPD, ai sensi dell'art. 7 cpv. 3, è proprio quello di evitare che gli interessati debbano studiare singolarmente ogni opzione di impostazione, verificarne la compatibilità con la protezione dei dati e quindi attivarla o disattivarla, selezionarla o deselezionarla individualmente. Piuttosto, dovrebbero poter contare sul fatto che la combinazione di opzioni di impostazione/scelta presentata loro al primo utilizzo rappresenti la combinazione di opzioni di impostazione più rispettosa della protezione dei dati e quindi "minimamente invasiva". 42

A seconda della formulazione concreta delle singole opzioni di impostazione, ciò può ovviamente comportare che alcuni campi di selezione debbano essere già attivati in anticipo: Se un'opzione di selezione consiste, ad esempio, in un'opzione come "Non desidero ricevere informazioni sui prodotti", tale campo di selezione dovrebbe essere attivato per impostazione predefinita secondo il principio della PbDefault (anche se l'invio di informazioni sui 43

prodotti sarebbe consentito ai sensi dell'art. 3 cpv. 1 lett. o LCSl a causa di un rapporto preesistente con il cliente).

44 A seconda della formulazione specifica delle singole opzioni di impostazione/scelta, può quindi accadere che sotto l'aspetto del PbDefault alcune opzioni debbano essere attivate, mentre altre debbano essere disattivate. Il fattore decisivo è che, con la combinazione di opzioni attivate/disattivate, venga attuata la combinazione di impostazioni/scelte più rispettosa della protezione dei dati nel singolo caso. Gli interessati dovrebbero poter contare sul fatto che, se non apportano modifiche a queste impostazioni predefinite, godranno sempre dell'impostazione più rispettosa della protezione dei dati.

45 Secondo il parere qui espresso, ciò deve valere anche per l'impostazione predefinita nel contesto dell'ottenimento del consenso. I requisiti per il PbDefault non si limitano a parametri puramente tecnici, ma, ai sensi dell'art. 7 cpv. 3 LPD, riguardano "il trattamento dei dati personali" in generale. In una visione olistica, come presuppongono i concetti di PbDesign e PbDefault, deve essere compreso anche l'eventuale consenso ottenuto. In questo caso va applicata la regola dell'insolito: se gli utenti confermano le CG nel contesto di un'accettazione globale, sono protetti da conseguenze inaspettate dalla regola dell'insolito. Lo stesso dovrebbe valere per la regolazione delle impostazioni e l'ottenimento del consenso: Il principio del PbDefault crea un'aspettativa legittima tra gli interessati di poter beneficiare in ogni momento dell'impostazione più favorevole alla protezione dei dati senza dover apportare modifiche personali. Ciò non dovrebbe essere compromesso consentendo campi di selezione pre-attivati per ulteriori elaborazioni che non corrispondono all'impostazione di base più favorevole alla protezione dei dati. Piuttosto, gli interessati dovrebbero essere protetti nella loro fiducia nell'attuazione completa del principio del PbDefault. Le circostanze concrete del rispettivo caso di applicazione sono decisive per la valutazione.

IV. CONSEGUENZE DELLA VIOLAZIONE DEGLI OBBLIGHI

46 La violazione degli obblighi di cui all'art. 7 LPD non ha conseguenze sanzionatorie dirette (cfr. art. 60 e segg. LPD). La violazione dell'obbligo di implementazione di PbDesign e PbDefault non costituisce di per sé (ancora) una violazione della personalità: L'art. 30 cpv. 2 lett. a LPD si riferisce esplicitamente solo agli artt. "6 e 8" (e non "da 6 a 8"): "Una violazione dei

diritti della personalità sussiste in particolare se: (a) i dati personali sono trattati in violazione dei principi di cui agli articoli 6 e 8".

D'altro canto, una violazione degli obblighi di cui all'art. 7 LPD può avere conseguenze sanzionatorie indirette se i sistemi, le applicazioni e i processi alla base di un trattamento rendono impossibile o limitano il rispetto dei requisiti di protezione dei dati a causa di una pianificazione e/o implementazione inadeguata. Se, ad esempio, non è possibile accedere ai dati personali memorizzati (e, se necessario, elaborarli, correggerli o cancellarli) su base personale, e il titolare del trattamento ne è (o deve essere) consapevole, è solo un piccolo passo verso la fornitura (eventualmente) intenzionale di informazioni false o incomplete ai sensi dell'art. 60 cpv. 1 lett. a LPD. 47

L'attuazione inadeguata dei principi PbDesign e PbDefault può anche portare a una violazione generale delle norme sulla protezione dei dati, in particolare dei principi dell'articolo 6 LPD. Se vi sono sufficienti indizi di tali violazioni, l'IFPD può avviare un'indagine d'ufficio o su segnalazione (art. 49 cpv. 1 LPD) ed emettere ordini appropriati (art. 51 LPD), tra cui l'ordine di attuare i principi di PbDesign e PbDefault (art. 51 cpv. 3 lett. b LPD). Se un ordine della LPD non viene rispettato, esiste la minaccia di una sanzione ai sensi dell'art. 63 LPD (inosservanza degli ordini). 48

V. DISPOSIZIONI TRANSITORIE

In linea di principio, la LPD è direttamente applicabile a tutti i trattamenti di dati a partire dalla sua entrata in vigore, a meno che gli artt. 69 segg. LPD non prevedano disposizioni transitorie speciali. Ai sensi dell'art. 69 LPD (disposizioni transitorie relative ai trattamenti in corso), le disposizioni dell'art. 7 LPD non si applicano ai trattamenti di dati esistenti che proseguono senza modifiche: "Gli articoli 7, 22 e 23 non si applicano ai trattamenti di dati iniziati prima dell'entrata in vigore della presente legge se lo scopo del trattamento rimane invariato e non vengono acquisiti nuovi dati". 49

La disposizione di esenzione dell'art. 69 LPD si riferisce quindi solo a trattamenti di dati con archivi di dati puramente statici e con uno scopo di trattamento costante e solo a trattamenti di dati già esistenti, non ai sistemi, alle applicazioni, ai processi o ad altri aspetti del trattamento di dati in quanto tali utilizzati a questo scopo: Non appena vengono elaborati nuovi dati con un sistema, un'applicazione o un processo esistente, o per nuovi scopi, questo 50

sistema, applicazione o processo (o altro aspetto dell'elaborazione dei dati) deve essere misurato rispetto alle nuove specifiche applicabili di PbDesign e PbDefault. Mentre, ad esempio, i sistemi legacy che continuano a funzionare in modo invariato (come un'applicazione di archivio puramente statica senza nuovi afflussi di dati) rientrano nelle disposizioni transitorie, i sistemi, le applicazioni e i processi operativi esistenti devono essere progettati in conformità ai principi di PbDesign e PbDefault e adattati costantemente al corrispondente stato dell'arte.

BIBLIOGRAFIA

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.

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 10 LPD

Un commentario di Michèle Balthasar

CITAZIONE SUGGERITA

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

Breve citazione: OK-Balthasar, N. XXX zu Art. 10 DSG.

Art. 10 Consulente per la protezione dei dati

[1] I titolari privati del trattamento possono nominare un consulente per la protezione dei dati.

[2] Il consulente funge da interlocutore per le persone interessate come pure per le autorità competenti in Svizzera per la protezione dei dati. Ha segnatamente i compiti seguenti:

a. fornire formazione e consulenza al titolare privato del trattamento in questioni concernenti la protezione dei dati;

b. partecipare all'applicazione delle disposizioni sulla protezione dei dati.

[3] I titolari privati del trattamento possono avvalersi dell'eccezione di cui all'articolo 23 capoverso 4 se:

a. il consulente esercita la sua funzione in modo indipendente dal titolare del trattamento e senza ricevere da questi istruzioni;

b. il consulente non esercita attività inconciliabili con i suoi compiti di consulente;

c. il consulente dispone delle conoscenze tecniche necessarie; e

d. il titolare del trattamento pubblica i dati di contatto del consulente e li comunica all'IFPDT.

[4] Il Consiglio federale disciplina la nomina dei consulenti da parte degli organi federali.

STRUTTURA

In breve 165
I. Aspetti generali 165
A. Introduzione 165
B. Diritto comparato 166
1. Obbligo di nominare un responsabile della protezione dei dati ai sensi del DSGVO 166
2. Obbligo di nominare un responsabile della protezione dei dati in base alle normative specifiche del paese. 167
C. Terminologia 167
II. Consulente per la protezione dei dati presso il responsabile del trattamento 168
A. Nomina del consulente per la protezione dei dati (art. 10 cpv. 1 LPD) 168
1. Natura volontaria della nomina del consulente per la protezione dei dati personali 168
2. Nomina di un consulente interno o esterno per la protezione dei dati 169
3. Nomina di un consulente comune per la protezione dei dati per un gruppo di società 170
B. Compiti del consulente per la protezione dei dati (art. 10 cpv. 2) 170
1. Punto di contatto per l'IFPDT e le altre autorità responsabili della protezione dei dati in Svizzera, nonché per le persone interessate. 170
2. Formazione e consulenza del responsabile del trattamento privato in materia di protezione dei dati (cpv. 2 lett. a) 171
3. Partecipazione all'applicazione delle norme sulla protezione dei dati (cpv. 2 lett. b) 171
4. Excursus: Nessuna responsabilità del consulente per la protezione dei dati ... 173
C. Requisiti del consulente per la protezione dei dati (cpv. 3) 174
1. Professionalmente indipendente e non vincolato da istruzioni (lett. a) 174
2. Nessuna incompatibilità con altri incarichi (lett. b) 174
3. Competenze richieste (lett. c) 175
4. Pubblicazione dei dati di contatto (lett. d) 176
D. Obblighi del responsabile del trattamento privato (art. 23 DPA) 176
1. Messa a disposizione dei mezzi necessari (lett. a) 176
2. Garantire l'accesso a tutte le informazioni, i documenti, gli elenchi delle attività di trattamento e i dati personali (lett. b) 177
3. Garantire il diritto di informare la direzione o l'organo amministrativo più alto in casi importanti (lett. c) 177
III. Consulente per la protezione dei dati presso gli organi federali (art. 10 cpv. 4 LPD) 178
A. Nomina (art. 25 LPD) 178
B. Requisiti e compiti (art. 26 LPD) 178
C. Compiti dell'organo federale (art. 27 LDP) 179

D. Punto di contatto dell'IFPDT (art. 28 IFPDT) 180
Bibliografia 180
I Materiali 180

IN BREVE

L'art. 10 LPD disciplina la nomina e i compiti del consulente per la protezione dei dati, nonché i requisiti per l'utilizzo della deroga di cui all'art. 23 cpv. 4 LPD. L'istituzione del consulente per la protezione dei dati consente alle aziende private di autoregolamentarsi. La nomina di un consulente per la protezione dei dati è volontaria per il responsabile del trattamento privato, tuttavia, in caso di nomina, può beneficiare dell'esenzione che consente di rinunciare alla consultazione dell'IFPDT in caso di valutazione d'impatto sulla protezione dei dati (DIA) a determinate condizioni.

I. ASPETTI GENERALI

A. Introduzione

L'art. 10 LPD disciplina la nomina e i compiti del consulente per la protezione dei dati, nonché le condizioni per avvalersi della deroga di cui all'art. 23 cpv. 4 LPD. L'art. 23 RGPD specifica i requisiti per un responsabile del trattamento dei dati privati che nomina un consulente per la protezione dei dati. L'istituzione del consulente per la protezione dei dati consente anche alle aziende private di autoregolamentarsi o di nominare una persona che gestisca la protezione dei dati in azienda. 1

Con l'introduzione della nuova disposizione sul consulente per la protezione dei dati nell'art. 10 LPD, la consultazione dell'IFPDT - obbligatoria a determinate condizioni - nell'ambito di una LPD è ora facilitata. Ad esempio, un progetto di trattamento dei dati da parte di responsabili privati che presenta ancora un "rischio elevato" nonostante una LPD non deve più essere sottoposto all'IFPDT se il consulente per la protezione dei dati è già stato consultato (art. 23 cpv. 4 LPD). Un'azienda che ha nominato un consulente per la protezione dei dati può quindi affidarsi esclusivamente alla consulenza interna in materia di protezione dei dati senza dover consultare l'IFPDT. 2

La nomina di un consulente per la protezione dei dati è facoltativa per il responsabile del trattamento privato. In base alla legge precedente, la nomina di un "incaricato della protezione dei dati" (paragonabile nella sua struttura) significava che le aziende non erano più obbligate a notificare all'IFPDT le loro raccolte di dati, che altrimenti avrebbero dovuto essere registrate. Con la 3

revisione, l'obbligo di registrazione per i privati viene generalmente abbandonato.

4 La nomina di un consulente per la protezione dei dati è facoltativa per i responsabili del trattamento dei dati privati, ma è obbligatoria per gli organi federali (art. 10 cpv. 4 LPD in combinato disposto con l'art. 25 e segg. LPD). Il Consiglio federale disciplina la nomina nell'art. 25 LPD e i requisiti e i compiti del consulente per la protezione dei dati degli organi federali nell'art. 26 LPD. L'art. 27 LDP definisce gli obblighi degli organi federali nei confronti del consulente per la protezione dei dati e l'art. 28 LDP definisce il consulente per la protezione dei dati come punto di contatto nei confronti dell'IFPDT.

B. Diritto comparato

1. Obbligo di nominare un responsabile della protezione dei dati ai sensi del DSGVO

5 Con l'entrata in vigore del DSGVO, l'Unione europea ha introdotto l'obbligo di nominare un cosiddetto responsabile della protezione dei dati in determinati casi. L'art. 37(1) del DSGVO elenca tre gruppi di casi in cui è necessario nominare un responsabile della protezione dei dati.

6 In primo luogo, ai sensi dell'art. 37 cpv. 1 let. a DSGVO, tale obbligo sussiste per le autorità pubbliche e gli enti pubblici, ad eccezione dei tribunali, se agiscono nel corso delle loro attività giudiziarie. Si tratta, ad esempio, di autorità edilizie, fornitori di acqua e di energia o aziende di trasporto.

7 Inoltre, l'art. 37 cpv. 1 DSGVO alla lettera b impone l'obbligo di designazione se l'attività principale del responsabile del trattamento o dell'incaricato del trattamento consiste nell'effettuare operazioni di trattamento che, per la loro natura, il loro ambito di applicazione e/o le loro finalità, richiedono un ampio monitoraggio regolare e sistematico delle persone. Il considerando 97 del DSGVO spiega che l'attività principale di un responsabile del trattamento si riferisce alle "sue attività principali e non al trattamento dei dati personali come attività accessoria". Il Gruppo di lavoro Articolo 29 della Commissione europea ha pubblicato delle linee guida su questo argomento con il WP 243 in relazione ai responsabili della protezione dei dati ("DPO"). Le "attività principali" sono quindi i principali processi lavorativi necessari per raggiungere gli obiettivi del responsabile del trattamento o dell'incaricato del

trattamento. Il monitoraggio è "regolare" se è continuo o periodico, e "sistematico" se segue un approccio metodico o organizzato o fa parte di una strategia più ampia. Tra gli esempi vi sono le società di sicurezza private che monitorano centri commerciali e luoghi pubblici, o le app la cui funzionalità principale richiede l'analisi dei dati di localizzazione (ad esempio, le app sportive o di navigazione).

Infine, ai sensi dell'art. 37 cpv. 1 DSGVO, vi è l'obbligo di nominare un responsabile della protezione dei dati nei casi in cui l'attività principale del responsabile del trattamento o dell'incaricato del trattamento consista in un trattamento esteso di categorie particolari di dati personali ai sensi dell'art. 9 DSGVO o di dati personali relativi a condanne penali e reati ai sensi dell'art. 10 DSGVO. Il fatto che un trattamento sia esteso ai sensi di questa disposizione deve essere chiarito caso per caso, ad esempio tenendo conto della quantità di dati trattati o del numero di interessati. Esempi sono il trattamento dei dati dei pazienti nell'ambito dell'ordinaria attività di un ospedale o il trattamento dei dati dei clienti nell'ambito dell'ordinaria attività di una compagnia di assicurazioni. 8

2. Obbligo di nominare un responsabile della protezione dei dati in base alle normative specifiche del paese.

Le normative nazionali possono prevedere disposizioni più ampie in base alle quali deve essere nominato un responsabile della protezione dei dati. Ad esempio, la legge federale tedesca sulla protezione dei dati (BDSG) prevede l'obbligo di nominare un responsabile della protezione dei dati se almeno 20 dipendenti sono coinvolti in modo permanente nel trattamento automatizzato dei dati personali (sezione 38 (1) frase 1 BDSG). Inoltre, il BDSG menziona due ulteriori scenari nella sezione 38 (1) frase 2 in cui le aziende devono nominare un responsabile della protezione dei dati indipendentemente dal numero di persone coinvolte nel trattamento: Da un lato, nei casi in cui è richiesto un responsabile della protezione dei dati ai sensi dell'art. 35 DSGVO e, dall'altro, nelle costellazioni in cui trattano i dati personali su base commerciale a scopo di trasmissione anonima o per ricerche di mercato o di opinione. 9

C. Terminologia

La precedente LPD utilizzava il termine "responsabile della protezione dei dati" in tedesco e "responsabile per la protezione dei dati" in italiano, mentre 10

la versione francese recita "conseiller à la protection des données", ossia "consulente per la protezione dei dati" (art. 11a cpv. 5 lett. e aDSG). Per evitare confusione con il "responsabile" ai sensi dell'art. 5 lett. i LPD o con il "responsabile", la revisione della LPD ha introdotto il termine "consulente per la protezione dei dati" in tedesco o "consulente per la protezione dei dati" in italiano. Ciò ha uniformato la terminologia dell'art. 10 LPD in tutte e tre le lingue.

11 Allo stesso tempo, è stato anche chiarito che la responsabilità del trattamento dei dati personali in conformità con la legge sulla protezione dei dati non spetta al consulente per la protezione dei dati, ma all'azienda responsabile, il "responsabile del trattamento".

II. CONSULENTE PER LA PROTEZIONE DEI DATI PRESSO IL RESPONSABILE DEL TRATTAMENTO

A. Nomina del consulente per la protezione dei dati (art. 10 cpv. 1 LPD)

1. Natura volontaria della nomina del consulente per la protezione dei dati personali

12 L'art. 10 cpv. 1 LPD stabilisce che la nomina di un consulente per la protezione dei dati è volontaria per i responsabili del trattamento privati. Secondo la LPD, spetta quindi al titolare del trattamento privato nominare o meno un consulente per la protezione dei dati. Tuttavia, un'azienda che ha nominato un consulente per la protezione dei dati ai sensi dell'art. 10 cpv. 3 LPD può, anche se il rischio rimane elevato, affidarsi esclusivamente alla consulenza interna in materia di protezione dei dati dopo aver effettuato una DIA senza dover consultare l'IFPDT (art. 23 cpv. 4 LPDT).

13 Tuttavia, le aziende che operano a livello internazionale devono rispettare le disposizioni del DSGVO e sono quindi spesso obbligate a nominare un responsabile della protezione dei dati ai sensi dell'art. 37 del DSGVO.

14 Inoltre, è nell'interesse di ogni azienda garantire una protezione dei dati efficiente ed efficace all'interno della propria organizzazione in termini di conformità adeguata. Pertanto, è spesso consigliabile nominare almeno un responsabile della protezione dei dati internamente e affidargli compiti di

protezione dei dati. Questa persona non è tenuta a soddisfare i requisiti di cui all'art. 10 cpv. 3 LPD. Tuttavia, se non soddisfa i requisiti di cui all'art. 10 cpv. 3, l'azienda non può beneficiare delle agevolazioni di cui all'art. 24 cpv. 3 LDP.

Nel caso della designazione di una persona o di un organismo di questo tipo, occorre evitare ambiguità in merito alla qualifica, allo status, alla posizione e al campo di attività. Pertanto, già dalla qualifica all'interno dell'azienda e nei confronti dell'IFPDT e delle persone interessate dovrebbe essere chiaro che non si tratta di un consulente per la protezione dei dati ai sensi dell'art. 10 cpv. 3 LPD. È consigliabile scegliere un'altra denominazione per questa funzione, come unità di protezione dei dati, persona di contatto per la protezione dei dati, coordinatore della protezione dei dati o responsabile della privacy. L'azienda responsabile è libera di assegnare i compiti come ritiene più opportuno. Tuttavia, i compiti devono essere chiaramente definiti in un capitolato. 2. 15

2. Nomina di un consulente interno o esterno per la protezione dei dati

L'azienda responsabile può nominare una persona interna o una persona o un organismo esterno come consulente per la protezione dei dati. 16

Il consulente interno per la protezione dei dati è un dipendente o un dipartimento di un'azienda che si occupa specificamente della protezione dei dati nella rispettiva azienda. Nelle aziende più grandi, essi sono regolarmente affiancati, a un livello gerarchico inferiore, dai cosiddetti responsabili della protezione dei dati o titolari dei dati, che sono responsabili della protezione dei dati nel loro rispettivo settore, come la creazione e la manutenzione del registro delle attività di trattamento (art. 12 LPD). 17

I consulenti esterni per la protezione dei dati, invece, sono persone fisiche o giuridiche che offrono servizi di protezione dei dati (data protection as a service) e agiscono sulla base di un rapporto contrattuale. Di norma, tuttavia, anche in questi casi dovrà essere nominata una persona di riferimento all'interno dell'azienda, che funga da punto di contatto sia per lui che per i dipendenti sulle questioni relative alla protezione dei dati all'interno dell'azienda. 18

Il vantaggio di un consulente interno per la protezione dei dati è che è integrato nell'azienda stessa e ha quindi una migliore visione d'insieme dei processi interni. Inoltre, può controllare e influenzare direttamente che la 19

protezione dei dati sia "vissuta" nella cultura aziendale e non esista solo sulla carta. D'altra parte, può essere svantaggioso essere troppo vicini all'azienda e ai dipendenti, il che può portare a conflitti di interesse. Spesso mancano anche le risorse e il relativo know-how o ci sono conflitti di interesse per garantire che la protezione dei dati sia adeguatamente salvaguardata in azienda. In queste situazioni, è opportuno esternalizzare il mandato del consulente per la protezione dei dati.

3. Nomina di un consulente comune per la protezione dei dati per un gruppo di società

20 È possibile nominare un consulente comune per la protezione dei dati per un gruppo di società. Tuttavia, il consulente comune deve essere facilmente accessibile agli interessati e all'IFPDT come persona di contatto interno attraverso canali di comunicazione adeguati. Deve essere in grado di comunicare efficacemente con gli interessati e di collaborare efficacemente con le autorità di controllo competenti. Tuttavia, non vi è alcun obbligo di risiedere in Svizzera, purché il consulente per la protezione dei dati sia in grado di svolgere efficacemente i propri compiti. Tuttavia, è probabile che sia richiesta la conoscenza di una lingua nazionale.

B. Compiti del consulente per la protezione dei dati (art. 10 cpv. 2)

1. Punto di contatto per l'IFPDT e le altre autorità responsabili della protezione dei dati in Svizzera, nonché per le persone interessate.

21 Il consulente per la protezione dei dati è un importante punto di contatto in relazione alle attività di trattamento dei dati svolte dal titolare del trattamento. È coinvolto nei processi di conformità dell'azienda in materia di protezione dei dati. In questo modo è possibile identificare direttamente una persona di contatto professionale, il che facilita l'esercizio dei diritti da parte dell'IFPDT o degli interessati.

22 Per le questioni relative al trattamento dei dati personali nell'azienda, la persona di contatto funge da punto di contatto per l'IFPDT e per le altre autorità responsabili della protezione dei dati in Svizzera (come la FINMA o le autorità cantonali per la protezione dei dati). Inoltre, funge da punto di

contatto per gli interessati, ad esempio in caso di richiesta di informazioni ai sensi degli artt. 25 e segg. LPD.

2. Formazione e consulenza del responsabile del trattamento privato in materia di protezione dei dati (cpv. 2 lett. a)

Per garantire un'efficace protezione dei dati nella rispettiva azienda, il consulente per la protezione dei dati deve formare, educare e sensibilizzare il titolare del trattamento privato e i suoi dipendenti. Come minimo, tutti i dipendenti che entrano in contatto con i dati personali dovrebbero essere coinvolti. L'attenzione deve essere rivolta ai principi della legge sulla protezione dei dati (art. 6 LPD). Altri argomenti di formazione sono i requisiti per la divulgazione all'estero e il trattamento di dati personali particolarmente sensibili in azienda. Inoltre, i dipendenti devono essere formati anche sui requisiti di sicurezza dei dati (art. 8 LPD). 23

La formazione dei dipendenti in materia di protezione e sicurezza dei dati da parte del consulente per la protezione dei dati deve essere ripetuta a intervalli regolari, preferibilmente ogni anno. Una regolare sensibilizzazione mantiene il tema della protezione dei dati nella mente dei dipendenti. Inoltre, le innovazioni attuali, ad esempio per quanto riguarda il panorama informatico dell'azienda, possono essere trasmesse ai dipendenti in modo tempestivo. 24

Nel suo ruolo di consulente, il consulente per la protezione dei dati ha il compito di consigliare l'osservanza delle norme sulla protezione dei dati nel trattamento dei dati, identificando i fatti rilevanti della questione della protezione dei dati in ogni caso e indicando decisioni alternative sulla base di questi. 3. Partecipazione all'applicazione della protezione dei dati 25

3. Partecipazione all'applicazione delle norme sulla protezione dei dati (cpv. 2 lett. b)

Un ulteriore compito del consulente per la protezione dei dati è la sua partecipazione all'applicazione delle norme sulla protezione dei dati. Ciò comprende, in particolare, l'assistenza all'emanazione delle condizioni di utilizzo e delle norme sulla protezione dei dati. Inoltre, deve controllare il trattamento dei dati personali e raccomandare misure correttive in caso di violazione delle disposizioni sulla protezione dei dati. Inoltre, deve assistere il responsabile del trattamento privato nella stesura dei DSFA e verificarne 26

l'esecuzione. Inoltre, è importante che il consulente per la protezione dei dati sia percepito come un interlocutore all'interno dell'istituzione e che sia membro dei gruppi di lavoro pertinenti che si occupano delle attività di trattamento dei dati all'interno dell'azienda. Tuttavia, i compiti del consulente per la protezione dei dati del responsabile del trattamento privato non comprendono la segnalazione delle violazioni della sicurezza dei dati all'IFPDT o agli interessati. Anche se spesso può essere opportuno coinvolgere il consulente per la protezione dei dati in caso di violazioni della sicurezza dei dati, ciò non è richiesto dalla legge.

27 Il consulente per la protezione dei dati deve essere inteso come un organo di supporto, ma non come un organo di controllo. Per quanto riguarda la revisione del trattamento dei dati e la raccomandazione di misure correttive, non si tratta quindi di introdurre un obbligo attivo di revisione o di prescrivere controlli sistematici di tutto il trattamento dei dati. Piuttosto, è sufficiente che il responsabile del trattamento dei dati si attivi se, ad esempio, richiede una revisione del trattamento dei dati o se riceve indicazioni di violazione delle norme sulla protezione dei dati. Naturalmente, il titolare del trattamento è libero di chiedere che il consulente per la protezione dei dati verifichi in modo proattivo il trattamento dei dati. Nella pratica è ipotizzabile e comune che il consulente effettui un audit sulla protezione dei dati una volta all'anno.

28 Altri compiti del consulente per la protezione dei dati possono essere:

- Sviluppare e verificare l'attuazione delle misure di sicurezza dei dati (art. 8 LPD);
- l'esame del trattamento da parte dell'incaricato del trattamento (art. 9 LPD);
- elaborazione e verifica degli elenchi delle attività di trattamento (art. 12 LPD);
- Esame della divulgazione dei dati all'estero (art. 16 e segg. LPD);
- Assistenza nell'adempimento degli obblighi di informazione (art. 19 e segg. LPD);
- Sviluppo e implementazione di processi per la gestione delle richieste degli interessati (art. 25 LPD);

- Sviluppo di processi appropriati per la salvaguardia dei diritti degli interessati e il rispetto delle norme sulla protezione dei dati (art. 25 e segg. LPD);
- condurre valutazioni del rischio (ad esempio, rischio di divulgazione, cancellazione o trattamento non intenzionale/non autorizzato dei dati, perdita di dati o errore tecnico, ecc;
- preparare relazioni annuali sulle attività all'attenzione del titolare del trattamento.

4. Excursus: Nessuna responsabilità del consulente per la protezione dei dati

Spesso si ritiene che il consulente per la protezione dei dati sia responsabile della protezione dei dati e della loro conformità all'interno dell'azienda. Tuttavia, il consulente per la protezione dei dati non ha alcuna autorità per agire al di là delle sue funzioni di formazione, consulenza e partecipazione, che derivano dalla LPD stessa. L'unico potere decisionale - e quindi anche l'unica responsabilità per il trattamento dei dati personali in conformità alla legge sulla protezione dei dati - spetta all'azienda responsabile. Il consulente per la protezione dei dati deve riferire al livello dirigenziale più alto dell'azienda interessata. La situazione sarebbe diversa solo se il consulente per la protezione dei dati agisse come un organo di fatto e quindi avesse un'influenza decisiva sul processo decisionale del responsabile del trattamento, decidendo i mezzi e le finalità del trattamento. Tuttavia, ciò non sarebbe ammissibile a causa dell'indipendenza professionale e della libertà da istruzioni richieste dall'art. 10 cpv. 3 LPD. Se un consulente per la protezione dei dati decide comunque le finalità e i mezzi del trattamento, è possibile che si configuri una responsabilità (di natura obbligatoria e/o penale). 29

Se il consulente per la protezione dei dati formula raccomandazioni, l'azienda deve assicurarsi che tali raccomandazioni vengano attuate. Se non lo fa e la raccomandazione era giustificata, questo può portare - se l'incidente diventa pubblico - a un notevole danno di immagine per l'azienda. Può anche portare a sanzioni nei confronti di un singolo dipendente. Tuttavia, se la raccomandazione era sbagliata o non corretta, il consulente per la protezione dei dati è responsabile nell'ambito del suo rapporto di lavoro o contrattuale. 30

C. Requisiti del consulente per la protezione dei dati (cpv. 3)

31 Affinché un'azienda possa essere esonerata dal consultare l'IFPDT se, nonostante l'esecuzione di una DIA, sussiste ancora un rischio elevato (art. 23 cpv. 4 LPD), il consulente per la protezione dei dati deve soddisfare i requisiti di cui all'art. 10 cpv. 3 LPD.

1. Professionalmente indipendente e non vincolato da istruzioni (lett. a)

32 Il consulente per la protezione dei dati deve essere indipendente nelle sue attività nella misura in cui i compiti possono essere svolti indipendentemente dalle istruzioni e non possono essere sanzionati dall'azienda sulla base delle sue attività. Ciò significa che il consulente per la protezione dei dati non può ricevere istruzioni su come procedere in una determinata situazione, ad esempio su quale risultato si debba ottenere, su come si debba dare seguito a un reclamo o se si debba o meno consultare l'IFPDT. Inoltre, non deve essere istruito ad assumere una posizione particolare su una questione di protezione dei dati (ad esempio, in merito all'interpretazione di una legge).

33 Occorre inoltre garantire che il consulente per la protezione dei dati possa esprimere liberamente le proprie raccomandazioni - anche se talvolta impopolari - senza timore di essere penalizzato. Questa indipendenza implica anche che il consulente per la protezione dei dati possa sottoporre questioni importanti ai vertici aziendali (ad esempio, il consiglio di amministrazione di una società per azioni) (art. 23 lett. c LADP). In linea di principio, il consulente per la protezione dei dati dovrebbe quindi riferire anche direttamente alla direzione o addirittura al consiglio di amministrazione del responsabile del trattamento. 2. Incompatibilità con altri incarichi (art. 23 lett. c LADP).

2. Nessuna incompatibilità con altri incarichi (lett. b)

34 Affinché il consulente per la protezione dei dati possa svolgere i propri compiti all'interno dell'azienda, non deve svolgere altre attività che siano incompatibili con i suoi doveri. La consulenza in materia di protezione dei dati deve essere fornita separatamente dai compiti dell'azienda. Deve essere evitato un conflitto di interessi. Ciò potrebbe verificarsi, ad esempio, se il consulente per la protezione dei dati è un membro della direzione, un capo della divisione operativa o un capo del dipartimento IT, o se svolge funzioni nell'ambito della gestione del personale o del sistema informativo (come il

responsabile IT). Il consulente per la protezione dei dati non può ricoprire allo stesso tempo una posizione in cui decide lui stesso i mezzi e le finalità delle attività di trattamento dei dati del responsabile del trattamento o ha un interesse in esse. È inoltre consigliabile non mescolare la consulenza in materia di protezione dei dati con altre consulenze e rappresentanze legali.

Un possibile conflitto di interessi deve quindi essere evitato in anticipo 35
attraverso la posizione organizzativa del consulente per la protezione dei dati. In linea di principio, occorre assicurarsi che la posizione di consulente per la protezione dei dati non sia associata ad alcuna responsabilità di linea. È quindi consigliabile che un'azienda stabilisca la funzione del consulente per la protezione dei dati come una posizione di staff, ad esempio. È importante che ciò non comporti una funzione esecutiva in un'area aziendale. Un'altra possibilità sarebbe quella di combinare il compito del consulente per la protezione dei dati con quello del responsabile della sicurezza delle informazioni.

Poiché nella pratica i conflitti di interesse sono difficilmente evitabili, il 36
consulente per la protezione dei dati - tranne nel caso di aziende più grandi che dispongono di un proprio dipartimento per la protezione dei dati - sarà di norma un fornitore di servizi esterno.

3. Competenze richieste (lett. c)

Per poter svolgere i propri compiti in modo indipendente, il consulente per la 37
protezione dei dati deve possedere le necessarie qualifiche professionali. Deve avere conoscenze sufficienti in tutti i settori per poter valutare le raccomandazioni e le misure proposte e valutarle nel quadro della strategia di protezione dei dati dell'azienda.

I requisiti comprendono non solo le conoscenze nel campo della protezione e 38
della sicurezza dei dati, ma anche le competenze specifiche dell'azienda. Se dovesse avere conoscenze meno sviluppate in determinate aree, deve almeno avere la possibilità di accedere a tali conoscenze. È richiesta una conoscenza interdisciplinare, soprattutto nei settori dell'informatica e del diritto. I sistemi di gestione devono essere compresi.

4. Pubblicazione dei dati di contatto (lett. d)

39 È responsabilità del titolare del trattamento pubblicare i dati di contatto del consulente per la protezione dei dati e notificarli all'IFPDT. A tal fine, l'IFPDT ha creato un portale di segnalazione. Come per il responsabile del trattamento privato, non è necessario che l'azienda pubblichi il nome del consulente per la protezione dei dati. È sufficiente indicare, ad esempio, l'indirizzo e-mail dell'organo tecnicamente competente. L'organo competente può anche essere un intero team o un'azienda. Il consulente per la protezione dei dati è una persona di contatto importante per quanto riguarda il trattamento dei dati effettuato dall'azienda in questione. La pubblicazione dei dati di contatto garantisce che gli interessati o l'IFPDT possano contattare direttamente il consulente per la protezione dei dati.

40 Non è necessario che l'azienda pubblichi il nome del consulente per la protezione dei dati. È sufficiente indicare, ad esempio, l'indirizzo e-mail dell'ufficio tecnicamente competente.

D. Obblighi del responsabile del trattamento privato (art. 23 DPA)

41 Affinché un'azienda possa essere esonerata dal consultare l'IFPDT se, nonostante l'esecuzione della LPD, sussiste ancora un rischio elevato (art. 23 cpv. 4 LPD), il responsabile del trattamento privato deve anche adempiere a determinati obblighi. Il contenuto di questi obblighi corrisponde alle precedenti disposizioni della legge sulla protezione dei dati; essi sono stati adattati alla nuova LPD solo dal punto di vista terminologico.

1. Messa a disposizione dei mezzi necessari (lett. a)

42 Ai sensi dell'art. 23 lett. a RGPD, il responsabile del trattamento privato deve mettere a disposizione del consulente per la protezione dei dati le risorse necessarie - di solito sotto forma di tempo di lavoro - per consentirgli di svolgere i suoi compiti. Sebbene i requisiti varino a seconda delle dimensioni dell'azienda, il consulente deve sempre disporre di risorse sufficienti per poter svolgere adeguatamente la funzione. Ciò significa che più complesse e/o sensibili sono le operazioni di trattamento dei dati, più risorse devono essere messe a disposizione del consulente per la protezione dei dati.

2. Garantire l'accesso a tutte le informazioni, i documenti, gli elenchi delle attività di trattamento e i dati personali (lett. b)

Per poter svolgere la propria funzione, il consulente per la protezione dei dati deve poter accedere, su richiesta, a tutte le informazioni, i documenti, i registri delle attività di trattamento e i dati personali di cui ha bisogno per svolgere i propri compiti. Oltre all'accesso, ciò include anche la conoscenza di tutte le attività di trattamento dei dati svolte all'interno dell'azienda. Ciò richiede un diritto completo di ispezione dei documenti, il diritto di vedere i sistemi di elaborazione dei dati e il diritto di informazione nei confronti di tutte le persone responsabili dell'elaborazione dei dati. Sarebbe consigliabile introdurre un obbligo di segnalazione all'interno dell'azienda, il che significa che tutti i trattamenti dei dati devono essere comunicati al consulente per la protezione dei dati. 43

Tuttavia, l'accesso alle informazioni è limitato in quanto si applica solo ai documenti di cui il consulente per la protezione dei dati ha effettivamente bisogno per svolgere i propri compiti. Ad esempio, se il consulente per la protezione dei dati sta conducendo una revisione generale delle norme interne sulla protezione dei dati o dei processi di trattamento dei dati, di norma non avrà bisogno di accedere ai dati personali. 44

3. Garantire il diritto di informare la direzione o l'organo amministrativo più alto in casi importanti (lett. c)

L'art. 23 lett. c LPD introduce la possibilità per i consulenti per la protezione dei dati di informare la direzione o l'organo amministrativo più alto in casi importanti, ossia l'organo che è anche responsabile del rispetto delle norme sulla protezione dei dati nell'azienda. Questo perché il consulente per la protezione dei dati non ha un potere decisionale proprio, ma è subordinato al livello dirigenziale più alto dell'azienda interessata. 45

La disposizione stabilisce un diritto di escalation per il consulente per la protezione dei dati. Ciò consente al consulente per la protezione dei dati non solo di basarsi sui documenti a sua disposizione durante le verifiche interne della conformità alle disposizioni in materia di protezione dei dati, ma anche di imporre l'acquisizione di ulteriori informazioni e documenti. Inoltre, ciò garantisce che il consulente per la protezione dei dati possa riferire ai massimi organi del responsabile del trattamento o dell'incaricato del trattamento in 46

caso di circostanze complesse e di violazioni particolarmente gravi e prendere una decisione. In pratica, le informazioni ai massimi organi di gestione o amministrativi possono essere fornite anche attraverso relazioni trimestrali e annuali sulle attività del consulente per la protezione dei dati.

III. CONSULENTE PER LA PROTEZIONE DEI DATI PRESSO GLI ORGANI FEDERALI (ART. 10 CPV. 4 LPD)

A. Nomina (art. 25 LPD)

47 Gli organi federali sono tenuti a nominare un consulente per la protezione dei dati nello spazio Schengen sulla base dell'articolo 32 della direttiva (UE) 2016/680. Le regole per la nomina del consulente per la protezione dei dati da parte degli organi federali non si trovano tuttavia nella LPD, ma sono state lasciate al Consiglio federale (art. 10 cpv. 4 LPD).

48 Ai sensi dell'art. 25 della LPD, più organi federali possono nominare congiuntamente un consulente per la protezione dei dati. Questa norma ha lo scopo principale di dare agli organi federali più piccoli o ai dipartimenti con una struttura organizzativa centralizzata la possibilità di sfruttare sinergie sensate e di risparmiare risorse. Gli uffici federali più grandi, invece, dovrebbero nominare autonomamente un consulente per la protezione dei dati. Gli organi federali possono anche nominare più consulenti per la protezione dei dati.

B. Requisiti e compiti (art. 26 LPD)

49 L'art. 26 cpv. 1 LPD contiene i requisiti del consulente per la protezione dei dati: deve disporre delle necessarie conoscenze specialistiche ed esercitare la sua funzione nei confronti dell'organo federale in modo professionalmente indipendente e vincolato da istruzioni. Questo regolamento è analogo a quello previsto dall'art. 10 cpv. 3 LPD per i responsabili del trattamento dei dati privati, motivo per cui si può fare riferimento ad esso.

50 Il ruolo del consulente per la protezione dei dati negli organi federali, che di solito sono gerarchici, è stato rafforzato e istituzionalizzato con la revisione, in modo che possa svolgere efficacemente i suoi compiti. L'indipendenza è espressa dal fatto che il consulente per la protezione dei dati può rivolgersi ai vertici dell'organo federale in casi importanti, come previsto per i privati

dall'art. 23 lett. c LADP. L'indipendenza del consulente per la protezione dei dati deve essere garantita soprattutto attraverso misure organizzative: ad esempio, è importante evitare che l'attività di consulente per la protezione dei dati abbia un impatto negativo sul colloquio con i dipendenti.

L'art. 26 cpv. 2 LPD contiene i compiti del consulente per la protezione dei dati di un organo federale. Essi sono stati coordinati terminologicamente con la disposizione relativa ai responsabili privati del trattamento dei dati (art. 10 cpv. 2 LPD), motivo per cui si può fare riferimento anche alle dichiarazioni ivi contenute. Partecipa all'applicazione delle norme sulla protezione dei dati, in particolare controllando il trattamento dei dati personali e raccomandando misure correttive (lett. a). Se viene individuata una violazione delle norme sulla protezione dei dati, consiglia il responsabile e ne verifica l'attuazione (lett. b). Inoltre, forma e consiglia i collaboratori dell'organismo federale sulle questioni relative alla protezione dei dati (lett. c). Infine, funge da punto di contatto per le persone interessate (lett. d). 51

C. Compiti dell'organo federale (art. 27 LDP)

L'organo federale concede al consulente per la protezione dei dati l'accesso a tutte le informazioni, i documenti, gli elenchi delle attività di trattamento e i dati personali di cui ha bisogno per adempiere ai suoi compiti (art. 27 cpv. 1 lett. a RPD) e provvede a informarlo di qualsiasi violazione della sicurezza dei dati (art. 27 cpv. 1 lett. b RPD). 52

L'art. 27 cpv. 1 lett. a LADP è quindi identico al regolamento per i responsabili del trattamento privati di cui all'art. 23 lett. b LADP. Si può fare riferimento, mutatis mutandis, alle spiegazioni ivi contenute. Inoltre, tale obbligo si applica a tutte le violazioni della sicurezza dei dati, non solo a quelle che devono essere segnalate all'IFPDT ai sensi dell'art. 24 LPD. L'informazione sulle violazioni della sicurezza dei dati ai sensi dell'art. 27 cpv. 1 lett. b LADP può essere garantita, ad esempio, dall'organo federale che obbliga i collaboratori, mediante istruzioni, a informare il consulente per la protezione dei dati in caso di violazione della sicurezza dei dati. Il consulente per la protezione dei dati consiglia il titolare del trattamento sulla questione se la violazione è soggetta all'obbligo di segnalazione ai sensi dell'art. 24 della LADP. L'organo federale si assicura che venga informato della violazione dei dati. Tuttavia, la notifica stessa è di competenza dell'organo federale. L'organo federale decide se e quali violazioni vengono segnalate all'IFPDT. 53

54 Infine, l'organo federale pubblica su Internet i dati di contatto del consulente per la protezione dei dati e informa l'IFPDT (art. 27 cpv. 2 LDP). Come per il responsabile del trattamento privato, non è necessario che l'azienda pubblichi il nome del consulente per la protezione dei dati. È sufficiente indicare, ad esempio, l'indirizzo e-mail dell'organo tecnicamente competente. L'organo competente può anche essere un intero team o un'azienda.

D. Punto di contatto dell'IFPDT (art. 28 IFPDT)

55 Il consulente per la protezione dei dati funge da punto di contatto dell'IFPDT per le questioni relative al trattamento dei dati personali da parte dell'organo federale interessato. Poiché dispone delle competenze e delle conoscenze interne necessarie, è quindi il referente tecnico diretto dell'IFPDT.

BIBLIOGRAFIA

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).

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 11 LPD

Un commentario di Ursula Sury / Jael Inauen

CITAZIONE SUGGERITA

Ursula Sury/Jael Inauen, Kommentierung zu Art. 11 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Sury/Inauen, N. XXX zu Art. 11 DSG.

Art. 11 Codice di condotta

[1] Le associazioni professionali, di settore ed economiche autorizzate dai loro statuti a difendere gli interessi economici dei loro membri come pure gli organi federali possono sottoporre all'IFPDT codici di condotta.

[2] L'IFPDT esprime un parere riguardo a ogni codice di condotta; pubblica tali pareri.

STRUTTURA

In breve 183
I. Aspetti generali 184
A. Storia 184
1. I codici di condotta in azienda 184
2. Le migliori pratiche 184
B. Scopo della norma 185
1. Promuovere la conformità alla protezione dei dati 185
2. Autoregolamentazione regolamentata 186
II. Contenuto 187
A. Codice di condotta 187
1. Un codice di condotta in generale 187
2. Codici di condotta per la protezione dei dati 188
3. Concretizzazione e autoregolamentazione 189
B. Distinzione dalla certificazione 189
III. Parere dell'IFPDT 190
A. Portata giuridica di una presentazione 191
B. Conseguenze del parere 192
IV. Autoregolamentazione ai sensi dell'art. 40 del GDPR 193
Bibliografia 194
I materiali 195

IN BREVE

I codici di condotta sono norme di comportamento emanate da associazioni professionali, industriali e imprenditoriali. Si sono affermati nell'economia come parte della "good corporate governance" come codice di condotta e ora vengono estesi alla protezione dei dati. I requisiti e le disposizioni in materia di protezione dei dati sono concretizzati in codici di condotta specifici per ogni settore. Gli organi federali e le associazioni private sono liberi di redigere i propri codici di condotta.

I codici di condotta possono essere sottoposti all'IFPDT. La DFP verifica la compatibilità dei codici con la FADP. La presentazione è obbligatoria solo se il codice deve essere utilizzato come giustificazione per un'esportazione di dati ai sensi dell'art. 12 LPD. Tuttavia, è generalmente raccomandata per ragioni di diligenza e di responsabilità.

L'art. 11 può essere paragonato all'art. 40 DPA, dove i requisiti e le conseguenze legali dei codici di condotta o "regole di condotta" (art. 40 DPA) sono simili. I codici redatti ai sensi dell'art. 40 GDPR costituiscono quindi un buon punto di riferimento per un'eventuale implementazione in Svizzera. Se si desidera l'approvazione del codice per l'Unione Europea, i suoi requisiti sono autorevoli.

Inoltre, la creazione di codici di condotta promuove l'internazionalizzazione delle aziende e la standardizzazione della protezione dei dati all'interno dei singoli settori. I codici di condotta sono stati introdotti da tempo a livello economico internazionale e sostengono una governance aziendale transnazionale, uniforme ed efficiente. Attraverso un codice di condotta, un'azienda può quindi essere in grado di soddisfare anche i requisiti internazionali, legali e specifici del settore.

I. ASPETTI GENERALI

A. Storia

1. I codici di condotta in azienda

1 Uno degli obiettivi principali della revisione totale della FADP è stato quello di ampliare e promuovere gli aspetti di autoregolamentazione. Mentre l'art. 11 dell'aDSG prevedeva solo una procedura di certificazione (n. 22 s.), nella nDSG questa viene integrata dallo strumento dei codici di condotta. Questi hanno lo scopo di consentire alle associazioni di concretizzare autonomamente la legislazione sulla protezione dei dati in base alle loro esigenze. Il codice di condotta introduce un concetto economico e aziendale ("codice di condotta") nella legge sulla protezione dei dati. Come parte della cultura della compliance e della "corporate governance", i codici di condotta sono diffusi da tempo nelle aziende. Ora sono previsti e definiti dalla legge per sostenere, concretizzare e guidare i sistemi di gestione della protezione dei dati.

2. Le migliori pratiche

2 Per l'attuazione della protezione dei dati, il BBl 2017 cita le cosiddette "best practice" per l'attuazione della protezione dei dati all'interno dell'azienda. "Le best practice sono da tempo diffuse nel campo della corporate governance e descrivono vari modelli o metodi per ottimizzare sistematicamente procedure, processi o pratiche all'interno dell'azienda stessa. Una procedura viene standardizzata per ottenere un processo aziendale ottimale. Il concetto di "buona prassi" è anche esplicitamente menzionato nell'art. 58 cpv. 1 lett. g LADP, secondo il quale la stessa DFP deve sviluppare strumenti di lavoro per garantire la conformità.

3 Le buone prassi sono rappresentate anche a livello internazionale; nell'art. 4 cpv. 3 dell'ordinanza sulla certificazione della protezione dei dati (RGPD), si fa riferimento agli standard internazionali esistenti, che costituiscono un punto di riferimento per i sistemi di gestione della protezione dei dati funzionanti. Indirettamente, si fa riferimento anche alle buone prassi e ai codici di condotta. Anche la Nuova Zelanda e l'Argentina fanno riferimento ai codici di condotta come buone pratiche.

Anche in Svizzera, nel corso della consultazione, si è discusso se l'IFPDT debba emanare esso stesso delle best practice in materia di protezione dei dati, dal momento che l'IFPDT ha il compito di fornire consulenza agli organi federali e ai privati e, in questo contesto, di fornire loro anche linee guida e strumenti di lavoro. Queste linee guida nel senso di best practice avrebbero quindi influenzato anche i codici di condotta. L'art. 58 cpv. 1 lett. g LADP può essere inteso anche come una competenza a redigere linee guida simili a codici di condotta. 4

Nel corso della consultazione, la comunità imprenditoriale ha criticato in particolare il fatto che la DFP avrebbe oltrepassato i suoi poteri esecutivi, poiché tali linee guida hanno indirettamente un effetto simile a quello di una legge. Per questo motivo, alla fine si è deciso di non concedere all'IFPDT questi poteri aggiuntivi. Si ricorrerà invece alle misure di autoregolamentazione e individualizzate dei codici di condotta, che hanno riscosso un ampio consenso in sede di consultazione. Le "migliori pratiche" potranno poi essere registrate nel codice di condotta stesso. 5

B. Scopo della norma

Lo scopo della norma e l'obiettivo del legislatore è quello di creare un quadro di orientamento e di certezza giuridica per gli stakeholder e le associazioni imprenditoriali. Attraverso una misura di autoregolamentazione, un'associazione può concretizzare i requisiti di protezione dei dati e adattarli in modo flessibile ai nuovi sviluppi della protezione dei dati. 6

1. Promuovere la conformità alla protezione dei dati

I codici di condotta mirano a promuovere la conformità alla protezione dei dati a due livelli: al primo livello, forniscono un quadro di certezza giuridica per vari gruppi e associazioni di categoria. Le misure di protezione dei dati possono ora essere regolamentate in modo uniforme. La concretizzazione autonoma offre anche la possibilità di adeguamenti specifici per la professione e di flessibilità di fronte agli sviluppi della protezione dei dati. Quest'ultimo aspetto si rivelerà particolarmente importante con l'avanzare del progresso tecnologico. Naturalmente, a fronte di queste libertà, i requisiti della LPD devono essere sempre osservati e rispettati. In questo modo, la nuova legge sulla protezione dei dati può essere attuata meglio a lungo termine. I destinatari devono essere incoraggiati a comportarsi secondo la legge. 7

8 In secondo luogo, la legge solleverà l'IFPDT da una parte del suo carico di lavoro. È evidente che l'adozione di codici da parte dei responsabili del trattamento dei dati porterà a una standardizzazione delle linee guida sulla protezione dei dati nei singoli settori. L'IFPDT può basare qualsiasi verifica di un responsabile del trattamento sul codice già approvato e deve solo controllare che sia rispettato. La ricerca e la compilazione delle norme sulla protezione dei dati sparse in regolamenti e statuti, potenzialmente dispendiose in termini di tempo, non sono più necessarie. I controlli sull'ammissibilità della conformità alla protezione dei dati non sono più selettivi e caso per caso, ma si basano su un insieme uniforme di regole stabilite da un codice di condotta.

2. Autoregolamentazione regolamentata

9 Nel contesto della digitalizzazione e della rete globale, i fornitori di servizi intermedi e gli operatori di rete stanno acquisendo un'influenza sempre maggiore sulla raccolta e sul trattamento dei dati personali. Inoltre, di solito il legislatore può reagire a una determinata tecnologia solo dopo che questa è diventata socialmente e giuridicamente rilevante.

10 L'"autoregolamentazione regolamentata" costituisce oggi un ponte tra le norme giuridiche statali (la cosiddetta "hard law") e le linee guida settoriali di diritto privato. I codici di condotta ne sono un esempio lampante. Da un lato, i codici di condotta sono previsti dalla legge e la loro presentazione ha determinate conseguenze legali (n. 30 s.), dall'altro, il legislatore lascia alle associazioni un notevole margine di manovra nel redigerli in base al proprio ambiente. L'esempio del codice di protezione dei dati dell'Associazione tedesca delle assicurazioni, che si basa sull'analogo regolamento del GDPR, illustra come questo sia stato specificamente concepito nella pratica. Esso stabilisce le regole per il trattamento dei dati personali nelle tipiche attività assicurative, come le statistiche, il calcolo delle tariffe e il calcolo dei premi. Vengono inoltre definite in modo più dettagliato le regole per la trasmissione dei dati a varie categorie di persone specifiche del settore, come riassicuratori, intermediari, concorrenti, ecc. Per l'elaborazione dei dati sulla solvibilità, invece, si fa riferimento alla legge senza emanare ulteriori regolamenti.

11 Nel quadro fornito dalla legge, le associazioni e gli organi federali possono orientarsi e regolamentare su base settoriale. La conoscenza e la

consapevolezza della protezione dei dati sta crescendo all'interno della società. Codici di condotta contestualizzati e precisi portano a una maggiore certezza giuridica. Anche gli standard specificati dovrebbero incontrare una maggiore comprensione e approvazione nel rispettivo settore. Offrire alle aziende queste misure orientate alla pratica è essenziale per una legge sulla protezione dei dati contemporanea, dinamica e, soprattutto, conforme.

II. CONTENUTO

A. Codice di condotta

1. Un codice di condotta in generale

Un codice di condotta è un documento formale che contiene una serie di norme. Ha lo scopo di definire in termini concreti il comportamento auspicabile in azienda. È ben rispettato nella cultura aziendale ed è considerato un importante pilastro della buona governance aziendale ed è diventato una parte indispensabile della cultura aziendale. 12

Tuttavia, un codice di condotta non fa parte di un ordinamento giuridico obbligatorio. Le aziende decidono autonomamente se aderire o meno a un codice di condotta. Si tratta di un impegno personale. Una volta che l'azienda si è impegnata, il codice è in linea di principio vincolante. Spetta all'associazione decidere come e se far rispettare il codice. Lo scopo di un codice di questo tipo è quello di guidare il comportamento dei dipendenti e dei dirigenti, sia all'interno dell'azienda che nei confronti di terzi esterni. Ciò si ottiene standardizzando e sistematizzando le azioni quotidiane e le norme di comportamento all'interno e all'esterno dell'azienda. 13

In questo modo, un codice di condotta protegge l'azienda sia internamente che esternamente. All'esterno, i dipendenti sono tutelati nelle loro decisioni e l'azienda può proteggersi meglio dagli attacchi esterni essendo in grado di dimostrare la conformità legale, la conformità e la diligenza attraverso il codice di condotta. All'interno, un codice di condotta contribuisce a creare una cultura aziendale sana e solidale, stabilendo degli standard, ad esempio nell'area della comunicazione, a cui i dipendenti devono attenersi. Ciò rafforza la fiducia tra i dipendenti. 14

15 Per la creazione di un codice di condotta in generale, è utile farsi guidare da domande guida. In particolare, è necessario chiarire i seguenti punti:

- Come mi devo comportare?
- Cosa mi è permesso fare e cosa è vietato?
- Quando devo intervenire sul comportamento di un terzo?
- Chi è la mia persona di riferimento in caso di domande, dubbi o incertezze?
- Cosa succede in caso di violazione del Codice di Condotta?

16 I punti regolamentati rappresentano un'importante informazione per i dipendenti stessi sul comportamento da tenere. È quindi importante formulare un codice di condotta in modo chiaro e comprensibile e adattarlo all'azienda. I requisiti comportamentali corrispondenti si concentrano anche sui rischi specifici dell'azienda o del settore. Un codice di condotta valido viene regolarmente aggiornato e confermato dalla direzione.

2. Codici di condotta per la protezione dei dati

17 I codici di condotta per la protezione dei dati fanno riferimento alle norme della FADP, le ampliano e le adattano specificamente al settore interessato. Tra questi vi sono, ad esempio, modelli esemplificativi di dichiarazioni sulla protezione dei dati, trattamento dei dati ad alto rischio in azienda o istruzioni sulla corretta anonimizzazione dei dati. Di seguito è riportato un elenco di domande guida sulle possibili aree di regolamentazione. Queste domande non sono né conclusive né obbligatorie. Tuttavia, forniscono una panoramica di ciò che dovrebbe essere incluso in un codice di condotta specifico per la protezione dei dati.

- I dati che sto trattando sono accurati?
- Chi è coinvolto nel trattamento dei dati?
- Quali dati personali vengono raccolti?
- Quali dati sono particolarmente rischiosi?
- È possibile garantire adeguatamente la crittografia dei dati?
- Gli interessati hanno il diritto di essere informati?

- L'azienda dispone di misure tecniche e organizzative per la protezione dei dati?
- Presupposti per il trasferimento di dati personali all'estero e per la garanzia delle garanzie della legge svizzera sulla protezione dei dati
- Modalità procedurali in caso di conflitto tra interessati e responsabili del trattamento.

Queste domande guida possono servire come punto di partenza per le associazioni. Tuttavia, per soddisfare le esigenze individuali di un determinato settore, sono necessarie spiegazioni più dettagliate e un'attenta documentazione e riflessione sui dati raccolti quotidianamente in quel settore. Si deve tenere conto delle esigenze delle aziende che fanno parte dell'associazione, cioè dei dipendenti, degli azionisti, dei clienti, ecc. 18

3. Concretizzazione e autoregolamentazione

Il codice di condotta di cui all'art. 11 della FADP applica quindi le norme della legge sulla protezione dei dati a una situazione specifica. Le formulazioni generali vengono concretizzate, rese più precise e anche comprensibili ai dipendenti. 19

Deve essere almeno altrettanto rigoroso della FADP, con al massimo requisiti più severi e specifici per il settore. È l'associazione stessa a redigere le specifiche. L'obiettivo è promuovere l'autoregolamentazione e la responsabilità personale. L'intervento dello Stato dovrebbe essere ridotto al minimo. Inoltre, l'autonomia di autoregolamentazione promuove il senso di responsabilità dei responsabili. 20

Lo Stato non dovrebbe intervenire attivamente nelle attività dei singoli settori o di altre associazioni, ma lasciare che siano loro a definire le clausole generali del DPA in base alle loro esigenze. Questo porta alla chiarezza della situazione legale e a formulazioni precise. 21

B. Distinzione dalla certificazione

L'art. 13 della FADP introduce le certificazioni di protezione dei dati che dimostrano la conformità dei sistemi, dei prodotti e dei servizi di un'azienda alla protezione dei dati. Gli organismi di certificazione agiscono in modo indipendente nel quadro delle direttive dell'IFPDT. Pertanto, a differenza dei 22

codici di condotta, l'IFPDT non esercita un controllo autonomo, ma solo un'influenza indiretta attraverso l'emanazione di norme sul riconoscimento di una certificazione (art. 13 LDP). La VDSZ, che definisce e specifica i requisiti degli organismi di certificazione, funge da guida.

23 Le certificazioni per la protezione dei dati servono a valutare selettivamente la conformità alla protezione dei dati di un sistema o di singole operazioni di trattamento. I codici di condotta, invece, descrivono tutti o la maggior parte dei requisiti delle attività di trattamento di un'azienda, o il modo in cui devono essere gestite in un settore specifico. In altre parole, i codici di condotta forniscono un quadro generale di orientamento, mentre le certificazioni di protezione dei dati confermano la conformità di una singola operazione. Le certificazioni sono fondamentali per l'attuazione pratica della conformità alla protezione dei dati. Mentre i codici di condotta stabiliscono il comportamento desiderato, analogo alla legge in teoria, le certificazioni servono come strumento per l'attuazione delle regole nella vita quotidiana.

24 Certificazioni e codice di condotta non si escludono quindi a vicenda. Pertanto, sembra essere utile per un'azienda se, oltre a un codice di condotta, si ottengono certificazioni selettive sulla protezione dei dati da parte di organismi qualificati. Ciò è particolarmente vero se lo specifico trattamento dei dati sembra essere atipico, nuovo o particolarmente rischioso per l'azienda interessata.

III. PARERE DELL'IFPDT

25 Le associazioni professionali, settoriali ed economiche autorizzate dai loro statuti a tutelare gli interessi economici dei loro membri sono legittimate a redigere un codice che può essere sottoposto all'esame dell'IFPDT.

26 I singoli responsabili del trattamento o incaricati del trattamento non possono presentare i loro codici di condotta. Ciò è giustificato dal fatto che l'art. 11 DPA mira a una certa standardizzazione all'interno dei singoli settori.

27 Tuttavia, le associazioni e le organizzazioni che hanno una certa rilevanza nazionale o almeno regionale hanno il diritto di presentare i loro codici di condotta, analogamente all'art. 89 CCP. Un'associazione cantonale soddisfa regolarmente questo requisito.

La forma giuridica dell'associazione non è in linea di principio determinante. Tuttavia, le società individuali, in particolare le società per azioni, sono escluse in quanto prive di soci. Per lo stesso motivo, le fondazioni non possono presentare domande. Le organizzazioni dei consumatori e le associazioni di persone interessate non hanno il requisito di rappresentare gli interessi economici dei loro membri. 28

Gli organismi federali hanno sempre il diritto di presentare candidature. Ciò è dovuto ai numerosi requisiti legali e ai vari compiti imposti ai diversi organi. 29

A. Portata giuridica di una presentazione

Secondo l'art. 11 del DPA, la presentazione di un codice di condotta per associazioni e società è in linea di principio facoltativa. Questo principio è mitigato dall'art. 12 DPA. In esso è previsto l'obbligo di sottoporre il codice all'approvazione dell'IFPDT se l'esportazione di dati deve essere giustificata dal codice (art. 12 LDP). Il principio della volontarietà, che si applica sia alla creazione dei codici di condotta sia alla loro presentazione all'IFPDT, viene ora violato da questa costellazione di trasferimenti di dati all'estero. Ciò può essere giustificato da uno standard di sicurezza più elevato, che deriva quasi automaticamente da uno scambio internazionale di dati molto più rischioso. Questo per garantire che il codice di condotta garantisca una sufficiente protezione dei dati. Ciò è sottolineato da un obbligo "vincolante ed esecutivo" per il responsabile del trattamento o l'incaricato del trattamento nel Paese terzo di rispettare il codice di condotta (art. 12 cpv. 3 DPA). Il codice diventa vincolante attraverso misure conformi alla legge applicabile nel rispettivo Paese terzo, come l'inserimento dei codici nello statuto del responsabile del trattamento. 30

A si rivela vantaggioso dal punto di vista della due diligence e della responsabilità all'interno delle aziende rappresentate. Infatti, solo una dichiarazione ufficiale può dimostrare in modo sufficiente che il codice è conforme alla legge sulla protezione dei dati. Un codice di condotta confermato è la prova diretta che l'azienda segue regole chiare in termini di legge sulla protezione dei dati, conformi alla DPA. 31

Poiché i codici di condotta sono misure di autoregolamentazione che hanno effetto sui rispettivi settori e professioni per i quali sono stati creati, essi rappresentano una concretizzazione legale per la pratica. Pertanto, è anche 32

possibile che si formino standard di condotta generalmente accettati in un determinato settore. Ciò rende molto più facile per le aziende conformarsi alla protezione dei dati; esse disporrebbero così di una linea guida concreta e di un parametro di riferimento per il proprio settore di attività.

B. Conseguenze del parere

33 L'IFPDT è tenuto a emettere un parere. Il parere non è un ordine, ma un vero e proprio atto e quindi, in linea di principio, non è vincolante. Tuttavia, una conferma da parte dell'IFPDT può avere diverse conseguenze.

34 Si può sempre prevedere un parere positivo se il codice prevede il rispetto di tutte le disposizioni della RICA. Lo standard per il parere è quindi la legge. L'IFPDT può fornire al parere suggerimenti per il miglioramento e raccomandazioni, in particolare nel caso di una mancata concretizzazione o di una non corretta applicazione della legge. Ai sensi dell'art. 59 della LDP, il parere è a pagamento per i privati. Ai sensi dell'art. 44 cpv. 1 e 2 LADP, l'onorario è calcolato in linea di principio in base al tempo impiegato, con una tariffa oraria compresa tra 150 e 250 franchi, a seconda della funzione del personale incaricato dell'esecuzione.

35 In seguito a un parere positivo, si può presumere che il comportamento conforme al Codice non comporti sanzioni o misure amministrative, ossia che il trattamento dei dati in conformità al Codice sia conforme alla protezione dei dati.

36 Inoltre, si può rinunciare a una valutazione d'impatto sulla protezione dei dati (DIA) se l'IFPDT emette un parere positivo e il codice di condotta si basa su una DIA ancora aggiornata che tutela i diritti personali e fondamentali della persona interessata (art. 22 cpv. 5 lett. a e b LDP). Un codice di condotta approvato è un'alternativa o un'eccezione all'obbligo di preparare una valutazione d'impatto. Per l'analisi dei rischi di un'azienda, è consigliabile collegare i DSFA e i codici di condotta al fine di minimizzare il più possibile qualsiasi rischio ai sensi della legge sulla protezione dei dati.

37 Le conseguenze di una dichiarazione errata sono ora discutibili. In questo caso, il privato ritiene che il proprio codice di condotta sia conforme alla legge sulla protezione dei dati. Pertanto, il trattamento basato su di esso non comporterà alcuna misura o sanzione amministrativa. Se tuttavia il privato viola la protezione dei dati sulla base di informazioni false, può comunque

rischiare sanzioni. Questo perché i requisiti per una valida protezione delle aspettative legittime sono severi. Affinché ciò sia accettato, il codice deve contenere formulazioni sufficientemente specifiche e i fatti accaduti devono essere congruenti con quanto previsto.

L'art. 11 non prevede il caso in cui associazioni diverse stabiliscano nei loro codici regole diverse per fatti identici o sovrapponibili. A condizione che le bozze concorrenti soddisfino di per sé i requisiti di cui sopra, l'IFPDT darà un parere positivo ai codici. Tuttavia, è libero di evidenziare le contraddizioni nel suo parere, poiché l'unificazione delle norme sulla protezione dei dati è inclusa nello scopo della norma. 38

Potrebbe quindi verificarsi una situazione in cui un responsabile del trattamento, membro di diverse associazioni, si impegni a rispettare codici di condotta contrastanti. Poiché l'IFPDT emetterà un parere positivo solo se i requisiti legali della LPD sono soddisfatti, ciò non lo metterà in conflitto con la legge. Tuttavia, è consigliabile aderire a un solo codice di condotta per mantenere rigorosi i principi interni di protezione dei dati dell'azienda. 39

IV. AUTOREGOLAMENTAZIONE AI SENSI DELL'ART. 40 DEL GDPR

Il GDPR prevede anche una norma per l'autoregolamentazione e la concretizzazione della protezione dei dati. L'articolo 40 del GDPR parla di "sviluppo di codici di condotta", redatti da associazioni o organizzazioni simili. Anche in questo caso, l'attenzione è rivolta alle misure di autoregolamentazione da parte delle aziende. Le norme devono essere considerate come un'integrazione e non come un sostituto delle disposizioni di legge. 40

I requisiti e le conseguenze legali dei codici di condotta e delle regole di condotta sono simili. Pertanto, anche i codici di condotta sono sottoposti a un'autorità di vigilanza per un parere, che viene anch'esso pubblicato. In base agli obblighi generali di responsabilità di cui all'art. 5 cpv. 2 del GDPR, il responsabile del trattamento deve rispettare i principi della legge sulla protezione dei dati e deve anche essere in grado di dimostrarlo. La stesura di regole di condotta facilita questo compito. L'art. 40 del GDPR specifica più precisamente i requisiti dei codici di condotta (par. 2 lett. a-k) e prevede varie 41

procedure per garantire una protezione sicura dei dati in tutti gli Stati membri, anche attraverso atti di esecuzione della Commissione.

42 Il GDPR promette inoltre alle aziende vantaggi e semplificazione della prova se si conformano volontariamente ai codici di condotta approvati.

43 A differenza della Svizzera, un codice di condotta presentato dall'autorità nazionale di controllo al Comitato europeo per la protezione dei dati (art. 63 GDPR) e da questo confermato può avere effetto anche a livello dell'Unione. Le regole di condotta possono essere dichiarate valide in tutta l'Unione mediante una dichiarazione di applicabilità generale (art. 40 cpv. 9 GDPR). Un codice di condotta orientato solo all'autorità di protezione dei dati e presentato solo all'IFPDT non garantisce la conformità alla protezione dei dati a livello transnazionale. Sembrerebbe vantaggioso che le associazioni (svizzere) che operano nell'Unione presentino i loro codici anche agli organi competenti dell'UE o che i responsabili del trattamento adottino codici di condotta già approvati. Questo facilita l'accesso al mercato e allo stesso tempo porta a un aumento dell'efficienza, in quanto si devono spendere meno tempo e risorse per i processi burocratici e normativi. Inoltre, si crea un'armonizzazione degli standard, di cui beneficiano soprattutto le aziende che operano sia in Svizzera che nell'UE.

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 12 LPD

Un commentario di Ursula Sury / Jael Inauen

CITAZIONE SUGGERITA

Ursula Sury/Jael Inauen, Commentario all'art. 12 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Sury/Inauen, art. 12 LPD N. XXX.

Art. 12 Registro delle attività di trattamento

[1] I titolari e i responsabili del trattamento tengono ognuno un registro delle rispettive attività di trattamento.

[2] Il registro del titolare del trattamento contiene almeno:

a. l'identità del titolare del trattamento;

b. lo scopo del trattamento;

c. una descrizione delle categorie di persone interessate e delle categorie di dati personali trattati;d.le categorie di destinatari;

e. se possibile, la durata di conservazione dei dati personali o i criteri per determinare tale durata;

f. se possibile, una descrizione generale dei provvedimenti tesi a garantire la sicurezza dei dati personali secondo l'articolo 8;

g. se i dati personali sono comunicati all'estero, le indicazioni relative allo Stato destinatario e le garanzie di cui all'articolo 16 capoverso 2.

3 Il registro del responsabile del trattamento contiene indicazioni in merito alla sua identità e a quella del titolare del trattamento, alle categorie dei trattamenti eseguiti su incarico del titolare del trattamento, come pure le indicazioni di cui al capoverso 2 lettere f e g.

4 Gli organi federali notificano i loro registri all'IFPDT.

5 Il Consiglio federale prevede eccezioni per le imprese con meno di 250 collaboratori i cui trattamenti di dati personali comportano soltanto un rischio esiguo di violazione della personalità delle persone interessate.

STRUTTURA

In breve 200
I. Aspetti generali 201
A. Panoramica 201
B. Storia delle origini 201
C. Scopo della norma 203
II. Contenuto 203
A. Contenuto di un repertorio di trattamento 203
B. Forma dell'elenco 205
C. Obblighi dei privati 205
1. Obblighi di legge 205
3. Eccezioni legali: PMI 206
4. Requisiti contrattuali 207
D. Obblighi degli organi federali (art. 12 cpv. 4 LDP) 208
E. Attuazione della conformità alla protezione dei dati 209
1. Obblighi di informazione 209
2. Il diritto di accesso 210
F. Dati all'estero (art. 12 cpv. 2 lett. g) 211
III. Confronto con il diritto dell'UE 212
Bibliografia 213
I materiali 214

IN BREVE

L'art. 12 della FADP descrive l'obbligo per gli organi federali e i responsabili del trattamento privati e per gli incaricati del trattamento di tenere un registro delle attività di trattamento. I dati devono essere registrati durante tutto il loro ciclo di vita nell'organizzazione. Un registro contiene almeno

- l'identità delle persone responsabili
- le categorie di dati personali trattati
- lo scopo del trattamento
- se possibile, il periodo di conservazione o almeno i criteri per determinarlo
- i destinatari dei dati trattati
- le misure da adottare in conformità con la legge sulla protezione dei dati
- i requisiti per la divulgazione dei dati all'estero

L'elenco non comprende le categorie di dati personali che l'azienda non tratta affatto e le garanzie per la divulgazione dei dati all'estero se non viene effettuata l'esportazione dei dati. Anche i dati che dovrebbero essere ottenuti prima solo con uno sforzo sproporzionato.

Infine, le aziende con meno di 250 dipendenti (PMI) sono legalmente esentate dall'obbligo di creare e mantenere un elenco dei trattamenti per motivi amministrativi. Poiché un registro delle attività di trattamento serve a chiarire internamente i dati trattati e a rispettare gli obblighi di responsabilità e di due diligence, si raccomanda a ogni azienda di tenere un registro.

Il registro delle attività di trattamento, che non è vincolato ad alcun requisito formale, viene registrato all'interno dell'azienda e offre, tra l'altro, la possibilità di un'autoregolamentazione regolamentata, oltre a codici di condotta e certificazioni. Da un lato, l'azienda acquisisce chiarezza sui dati che elabora e, dall'altro, l'IFPDT, a partire dall'entrata in vigore della revisione della LPD, sarà guidato dagli elenchi di trattamento dei dati per verificare la conformità alla protezione dei dati.

I. ASPETTI GENERALI

A. Panoramica

Secondo le disposizioni della legge sulla protezione dei dati (LPD), un repertorio delle attività di trattamento è uno strumento importante per garantire il rispetto delle disposizioni della legge sulla protezione dei dati. Esso fornisce una panoramica sistematica delle attività di trattamento dei dati e costituisce un obbligo sia per gli organi federali che per i privati. Fornisce informazioni sull'origine e sullo scopo dei dati, sugli aspetti della conservazione, nonché sulle misure di sicurezza applicate e sul trasferimento dei dati, eventualmente all'estero. Lo standard sostituisce l'art. 11a aDSG in combinazione con l'art. 11 VDSG. L'art. 11 VDSG specifica e amplia l'obbligo di tenere un registro delle raccolte di dati. Le parti responsabili devono determinare autonomamente e documentare sistematicamente i dati raccolti internamente. Il registro pone quindi maggiore attenzione all'obbligo di documentazione e alle attività di trattamento dei dati. Tuttavia, il registro delle attività di trattamento deve essere distinto dal registro delle raccolte di dati e presenta ulteriori requisiti di contenuto (cfr. n. 6). 1

Grazie al registro delle attività di trattamento, le organizzazioni dispongono di informazioni importanti sui loro dati digitali, hanno una panoramica chiara e aggiornata. Ciò va a vantaggio sia dell'IFPDT, il cui esame della conformità alla protezione dei dati di un'azienda è semplificato, sia dell'azienda stessa. 2

B. Storia delle origini

Ai sensi dell'art. 11a aDSG, il "Commissario", ossia l'IFPDT, teneva un registro delle raccolte di dati ("Registro") accessibile al pubblico. Mentre gli organi federali dovevano registrare tutte le raccolte di dati presso l'IFPDT (art. 11a cpv. 1 aDSG), i privati erano tenuti a registrarsi solo se trasmettevano regolarmente dati personali a terzi (art. 11a cpv. 3 lett. b aDSG) o se trattavano profili della personalità o dati che richiedevano una protezione speciale (art. 11a cpv. 3 lett. aDSG). L'art. 11a cpv. 5 LDSG esonera dall'obbligo di notifica all'IFPDT diversi titolari di raccolte di dati, tra cui i titolari di una certificazione di protezione dei dati o le aziende con un responsabile della protezione dei dati. 3

4 L'art. 11a LADP non specificava di per sé i requisiti per un registro delle raccolte di dati, ma lo faceva l'art. 11 LADP. Secondo questo articolo, il registro deve contenere la descrizione delle strutture organizzative interne e delle procedure di elaborazione e controllo dei dati. Dovevano essere elencate anche le prove relative alla pianificazione, all'implementazione e al funzionamento della raccolta di dati, nonché le risorse informatiche utilizzate. Queste specifiche si applicavano solo al trattamento dei dati soggetti a rendicontazione.

5 Tuttavia, il termine "registro delle attività di trattamento" va oltre una breve panoramica dei dati raccolti. Include anche informazioni su cosa viene fatto con i dati, come vengono raccolti e dove vengono trasmessi. I registri si sovrappongono a un repertorio delle attività di trattamento in termini di contenuto, ma si concentrano in modo più approfondito sulla struttura interna, sulla pianificazione e sull'amministrazione dell'azienda. Nell'attuale FADP, il termine registro delle raccolte di dati non è più presente, in quanto è stato sostituito dall'elenco delle attività di trattamento.

6 L'art. 12 della LPD è più completo e richiede informazioni aggiuntive quali l'identità del responsabile del trattamento, lo scopo del trattamento, la categorizzazione dei dati personali trattati e dei destinatari, il periodo di conservazione e le misure concrete per garantire la sicurezza dei dati. Sebbene vi siano molte sovrapposizioni con l'art. 11 della legge sulla protezione dei dati, i requisiti sono molto più dettagliati, il che dovrebbe anche semplificare la creazione di un elenco. Anche il precedente obbligo generale di documentazione, ossia l'obbligo di segnalare le raccolte di dati, viene sostituito dall'elenco dei trattamenti.

7 Con l'entrata in vigore della nuova FADP, i privati e gli organi federali devono redigere un elenco delle attività di trattamento dei dati ai sensi dell'art. 12 della FADP. Tuttavia, sono solo gli organi federali a dover presentare il proprio elenco dei trattamenti all'IFPDT (art. 12 cpv. 4 RPDT). L'obbligo di tenere un registro, tuttavia, si applica anche ai privati. L'elenco delle attività di trattamento consente di controllare meglio i propri dati. L'elenco delle attività di trattamento è ora classificato nelle disposizioni generali sulla protezione dei dati.

C. Scopo della norma

L'art. 12 della FADP è un obbligo per i responsabili e gli incaricati del trattamento. Lo scopo della norma è aumentare la trasparenza nel trattamento dei dati. Ciò è garantito dai requisiti più severi per l'elenco (art. 12 LADP) rispetto alla precedente controparte, il registro delle raccolte di dati (art. 11a aLADP). Grazie a informazioni minime precise, i responsabili del trattamento dei dati hanno un quadro di orientamento chiaro per quanto riguarda i dati da inserire in un elenco. In questo modo, il trattamento dei dati viene registrato in modo standardizzato. Per il titolare del trattamento diventa più facile tenere traccia dei dati raccolti all'interno dell'azienda. Da un lato, può adempiere adeguatamente al dovere di informazione e, dall'altro, rispettare in modo soddisfacente il diritto all'informazione. 8

Una raccolta sistematica di dati e informazioni è generalmente vantaggiosa per le aziende, non solo nel settore dei dati personali. Un registro dei materiali o un registro delle informazioni soggette a obbligo di riservatezza consentono all'azienda di avere sempre una panoramica aggiornata, corretta e semplificata del flusso interno di informazioni. Anche in questo caso vale il principio secondo cui la raccolta e la compilazione sistematica dei dati costituiscono un importante patrimonio digitale. 9

Lo standard rappresenta anche una semplificazione per l'FDPIC. L'FDPIC beneficia della standardizzazione dell'elenco, in quanto tutte le categorizzazioni o le modifiche pertinenti sono ora direttamente disponibili per l'FDPIC. In futuro, l'FDPIC chiederà l'elenco prima di tutto durante un'indagine. Tuttavia, la mancata tenuta dell'elenco non comporta una sanzione immediata. Tuttavia, fornire informazioni false o rifiutarsi di collaborare a un'indagine dell'IFPDT rimane un reato punibile, come già previsto dalla legge attuale. 10

II. CONTENUTO

A. Contenuto di un repertorio di trattamento

L'art. 12 prevede alcuni requisiti minimi per il contenuto di questo repertorio, come segue: 11

- Chi è il responsabile, art. 12 cpv. 2 lett. a LADP.

Il responsabile è la persona che decide le finalità e i mezzi del trattamento dei dati. Se ci sono più responsabili del trattamento, devono essere elencati tutti.

- Qual è lo scopo del trattamento?, art. 12 cpv. 2 lett. b LADP.
  La finalità può variare; il fattore decisivo è l'obiettivo perseguito con il trattamento dei dati. Di norma, la persona che avvia il trattamento decide anche in merito alla sua finalità.
- Quali persone e quali tipi di dati personali vengono trattati (categorizzazione), art. 12 cpv. 2 lett. c LADP.
  Le categorie di persone interessate sono raggruppamenti tipizzati come "consumatori" o "dipendenti". Le categorie di "dati personali trattati" si riferiscono ai tipi di dati trattati, come i dati personali che richiedono una protezione speciale.
- Chi è il destinatario dei dati trattati, art. 12 cpv. 2 lett. d LADP.
  Anche i destinatari dei dati personali trattati sono suddivisi in categorie, ad esempio le autorità di controllo.
- Per quanto tempo vengono conservati i dati personali o come si può determinare tale durata?, art. 12 cpv. 2 lett. e LADP.
  Ciò riguarda in particolare i periodi di archiviazione dei dati raccolti. Se non esiste una base giuridica o uno scopo definito per la conservazione dei dati personali raccolti, questi devono essere cancellati o resi anonimi (art. 6 cpv. 4 LADP).
- Quali misure vengono adottate per garantire la sicurezza dei dati ai sensi dell'art. 8 e dell'art. 12 cpv. 2 lett. f LADP?
  Si fa riferimento ai principi fondamentali della protezione e della sicurezza dei dati. Questi includono in particolare l'integrità dei dati raccolti, misure tecniche e organizzative adeguate e la "privacy by default" e la "privacy by design".
- Quali sono le misure da adottare per la divulgazione dei dati all'estero?, art. 12 cpv. 2 lett. g LADP.
  Oltre alle misure legali (cfr. art. 16 e segg. LADP), queste comprendono anche clausole standard concordate contrattualmente e standard settoriali definiti a livello internazionale (cfr. a questo proposito l'art. 11 LADP in combinato disposto con l'art. 12 LPD).

L'art. 12 è molto preciso e dettagliato, ma lascia comunque un certo grado di libertà. Ad esempio, l'elenco dovrebbe contenere solo informazioni il cui contenuto è sufficientemente certo. La descrizione deve essere fornita solo se le attività possono essere descritte in termini sufficientemente concreti. A volte non è possibile specificare l'esatto periodo di conservazione. Pertanto, è necessario specificare solo i criteri per il periodo di conservazione. A causa di questa ampia formulazione, sarebbe auspicabile l'elaborazione di linee guida specifiche per il settore, che potrebbero essere applicate uniformemente nei rispettivi settori. Ciò faciliterebbe il lavoro sia delle aziende che dell'FDPIC. L'elaborazione di linee guida settoriali che possano essere applicate in modo uniforme nei rispettivi settori potrebbe rendere più concreta questa ampia formulazione. Ciò aiuterebbe sia i responsabili che l'FDPIC a facilitare il loro lavoro. Le linee guida fornirebbero istruzioni chiare ai responsabili e li aiuterebbero a comprendere e attuare meglio i requisiti di protezione dei dati nel loro settore. Allo stesso tempo, consentirebbero all'IFPDT di effettuare una revisione e un'applicazione più coerente della protezione dei dati nei diversi settori. 12

B. Forma dell'elenco

L'articolo 12 della LPD non disciplina nel dettaglio il modo in cui le attività di trattamento dei dati sono sistematizzate nell'elenco delle attività di trattamento. Non ci sono nemmeno requisiti formali. Un elenco può essere un semplice documento Word o Excel o una soluzione informatica complessa. L'elenco può essere tenuto in modo decentralizzato e la sua manutenzione può anche essere delegata. 13

C. Obblighi dei privati

1. Obblighi di legge

In linea di principio, tutte le aziende e gli altri soggetti privati responsabili sono obbligati a tenere un registro delle attività di trattamento. Ciò deriva dal fatto che quasi tutti i privati raccolgono e trattano dati personali nell'ambito delle loro attività commerciali o senza scopo di lucro. 14

2. L'incaricato del trattamento

15 Il registro delle attività di trattamento deve essere tenuto dal responsabile del trattamento e dall'incaricato del trattamento (art. 12 cpv. 1 LADP). L'incaricato del trattamento è una persona che tratta i dati per conto del responsabile del trattamento (art. 5 lett. k LADP). Un esempio è il fornitore di servizi informatici che ospita un sito web o un dipendente che prende i dati di contatto dei clienti. Il responsabile del trattamento dei dati, invece, è la persona che decide le finalità e i mezzi del trattamento dei dati (art. 5 lett. j LADP).

16 Ogni azienda è l'unica responsabile dei dati trattati internamente. Un incaricato del trattamento non è obbligato a tenere un elenco dei trattamenti per il responsabile del trattamento. I dati del responsabile del trattamento, detto anche "incaricato del trattamento", non devono essere elencati. È solo responsabilità del responsabile del trattamento stesso, che è responsabile dei dati raccolti, ad esempio i dati dei clienti. Altrimenti, ciò porterebbe a una raccolta eccessiva di dati personali. Per le aziende sarebbe quasi impossibile far rispettare questo requisito. Sarebbe necessario raccogliere la totalità dei dati personali del cliente per ogni servizio. Ci si aspetterebbe una proliferazione di elenchi e la conseguente perdita di una visione d'insieme dei dati raccolti. La directory dell'incaricato del trattamento contiene quindi meno informazioni di quella del responsabile del trattamento. D'altra parte, questo elenco crea trasparenza nel rapporto contrattuale tra il responsabile del trattamento e l'incaricato del trattamento, stabilendo che entrambe le parti devono essere chiaramente identificabili. Le condizioni quadro pertinenti sono stabilite dall'art. 9 della FADP, che chiarisce il trattamento dei dati da parte di un incaricato.

3. Eccezioni legali: PMI

17 L'art. 12 cpv. 5, prevede un'eccezione per le aziende che impiegano meno di 250 dipendenti e non trattano dati ad alto rischio. Queste sono esenti dall'obbligo di tenere un registro delle attività di trattamento. Le attività di trattamento dei dati ad alto rischio sono quelle che con maggiore probabilità possono comportare una violazione della personalità (violazione della privacy, dati medici, orientamento sessuale, confessione religiosa ecc.) Questa eccezione è menzionata anche nell'art. 24 dell'ordinanza sulla protezione dei dati (DPA). Tuttavia, l'art. 24 non contiene disposizioni più dettagliate sull'eccezione legale. Si limita a ribadire che le PMI sono esenti dall'obbligo di

repertorio, a meno che non trattino su larga scala dati personali che richiedono una protezione speciale (lett. a) o non effettuino profilazioni ad alto rischio (lett. b). Il termine "rischio elevato" è utilizzato in modo analogo a quello dell'articolo 22 cpv. 2,della LDA.

Lo scopo di questa eccezione è quello di alleggerire l'onere amministrativo delle imprese più piccole. Non si tiene conto solo delle dimensioni dell'azienda, ma anche dei dati trattati e dei rischi ad essi associati. Anche le PMI sono interessate dalle sanzioni previste dalla FADP e alle PMI è richiesto il rispetto dei principi di protezione dei dati. Ciò comporta un obbligo di documentazione indiretto per le aziende, anche se non sono obbligate per legge a creare un repertorio dei trattamenti. Infatti, l'IFPDT si occuperà delle misure di protezione dei dati all'interno di una PMI indipendentemente dall'esistenza o meno di un elenco delle attività di trattamento. La PMI deve quindi presentare comunque i dati trattati. Un registro offre all'azienda una migliore protezione in termini di responsabilità e di due diligence. 18

Se la metà di tutti i dati trattati sono ad alto rischio, rientrano nei requisiti degli obblighi di documentazione rafforzata, ma potrebbero comunque non essere legalmente obbligati a essere elencati in un elenco delle attività di trattamento. La responsabilità e il rischio di eventuali violazioni della protezione dei dati sono sempre a carico del titolare del trattamento. Si raccomanda pertanto la creazione di un elenco delle attività di trattamento se viene effettuato un trattamento di dati ad alto rischio, indipendentemente dalla portata. 19

4. Requisiti contrattuali

È anche possibile prevedere la tenuta di un registro per contratto. Sebbene un tale obbligo sia di natura dispositiva, potrebbe assumere un'importanza maggiore a seconda del settore. Tenendo un registro dei trattamenti, un'azienda può proteggersi non solo dall'IFPDT e dai requisiti di legge, ma anche da altre aziende, che possono essere sia partner che clienti. Se un responsabile del trattamento sa come l'incaricato del trattamento elabora e archivia i dati e con quali mezzi, promuove la fiducia e la cooperazione tra le due parti. Inoltre, l'applicazione di una prassi in cui gli elenchi sono concordati contrattualmente consente l'elaborazione indipendente di elenchi che sono adattati ai rispettivi settori economici e rispondono alle sfide specifiche della protezione dei dati nelle aree di lavoro interessate. 20

21 Nel contrattare gli elenchi, è necessario tenere conto di alcuni aspetti e possono sorgere diversi ostacoli. L'attuazione di questa prassi consentirà alle aziende di creare autonomamente elenchi che soddisfino i requisiti specifici e le sfide in materia di protezione dei dati dei rispettivi settori economici.

22 Uno degli ostacoli consiste nel redigere i contratti in modo da soddisfare i requisiti precisi della legge sulla protezione dei dati. È necessario stipulare accordi chiari sul tipo di dati raccolti, sulle finalità del trattamento dei dati, sul periodo di conservazione, sulle misure di sicurezza e su altri aspetti rilevanti della protezione dei dati. È importante garantire che gli accordi contrattuali siano conformi alla legge e che i diritti degli interessati siano adeguatamente tutelati.

23 Inoltre, l'elaborazione di elenchi settoriali può essere impegnativa. I diversi settori economici hanno requisiti diversi in materia di protezione dei dati e aree di lavoro specifiche che possono presentare sfide specifiche in materia di protezione dei dati. Le aziende devono essere in grado di identificare e incorporare questi requisiti specifici nei loro elenchi, al fine di rispettare le normative sulla protezione dei dati.

24 La collaborazione tra le parti coinvolte, come le aziende, gli esperti di protezione dei dati e, se del caso, le autorità di vigilanza, può essere utile per implementare con successo gli accordi contrattuali e l'elaborazione di elenchi settoriali specifici.

D. Obblighi degli organi federali (art. 12 cpv. 4 LDP)

25 Secondo l'art. 5 lett. i LADP, gli organi federali non sono solo le autorità o gli organi amministrativi centrali, ma qualsiasi autorità o servizio della Confederazione, nonché le persone che svolgono compiti pubblici della Confederazione.

26 Gli organi federali hanno l'obbligo, ai sensi dell'art. 12 cpv. 4 LDP, di comunicare all'IFPDT i loro elenchi di attività di trattamento. Lo stesso IFPDT tiene un registro delle attività di trattamento degli organi federali ai sensi dell'art. 56 LDP, che viene pubblicato.

27 Anche prima della revisione della legge sulla protezione dei dati, gli organi federali erano tenuti a registrare le strutture organizzative e le procedure di trattamento dei dati in un registro delle raccolte di dati. Questo includeva

implicitamente il nome e l'indirizzo dell'organo federale responsabile, la designazione della raccolta di dati, l'organo responsabile del diritto di accesso, nonché la base giuridica e lo scopo. Venivano registrate le categorie di dati personali trattati, i destinatari e i partecipanti alla raccolta di dati (art. 11a della vecchia FADP). Anche i registri delle raccolte di dati dovevano essere registrati presso l'IFPDT ai sensi dell'art. 11a aDSG. In generale, gli organi federali erano soggetti a requisiti più severi. Il Consiglio federale aveva inoltre la facoltà di stabilire norme speciali per la protezione dei dati (art. 16 cpv. 2 aDSG).

Non vi sono quindi cambiamenti significativi negli obblighi degli organi federali. Piuttosto, l'art. 12 LADP estende ai privati gli obblighi che in precedenza si applicavano solo agli organi federali. Gli organismi federali devono quindi tenere un registro delle attività di trattamento, senza eccezioni. Un registro già esistente e tenuto in modo accurato e aggiornato soddisfa già molti dei requisiti di un registro, motivo per cui spesso sono necessarie poche o nessuna modifica per attuare l'attuale legge sulla protezione dei dati. Il cambiamento più significativo è che invece delle raccolte di dati, il trattamento dei dati è ora suddiviso. 28

E. Attuazione della conformità alla protezione dei dati

In linea di principio, il registro delle attività di trattamento non è destinato agli interessati, ma serve principalmente al controllo interno di un'azienda e alle indagini dell'IFPDT. Redigendo un registro delle attività di trattamento, i responsabili del trattamento ottengono chiarezza sulle proprie attività di trattamento dei dati. La tenuta del registro semplifica l'attuazione di alcuni obblighi e l'adempimento dei diritti degli interessati, come il diritto all'informazione (art. 25 LDP). 29

1. Obblighi di informazione

L'art. 19 della FADP prevede un obbligo di informazione per il responsabile del trattamento e l'incaricato del trattamento quando ottengono dati personali. Devono essere comunicati almeno l'identità e i dati di contatto del responsabile del trattamento, lo scopo del trattamento e, se del caso, i destinatari dei dati personali ottenuti. Con la revisione della protezione dei dati, l'obbligo di informazione è stato generalmente esteso. Prima della revisione, si applicava solo all'acquisizione di dati particolarmente sensibili o 30

di profili della personalità, mentre ora si applica a qualsiasi acquisizione di dati personali.

31 Con un elenco delle attività di trattamento, la persona interessata viene informata in modo efficace e uniforme sulla raccolta dei propri dati. Inoltre, è possibile comunicare con precisione le finalità, i mezzi e, in determinate circostanze, il periodo di conservazione, poiché queste informazioni sono già contenute nell'elenco. In questo senso, l'elenco rappresenta uno sgravio amministrativo per le aziende, grazie al quale i processi informativi esterni nei confronti degli interessati o dell'IFPDT possono essere progettati in modo più semplice ed efficiente. Questa progettazione più efficiente presenta diversi vantaggi. In primo luogo, il responsabile riduce l'onere amministrativo, poiché non deve più creare e inviare una notifica separata per ogni singolo trattamento dei dati. Può invece fare riferimento all'elenco, che contiene già tutte le informazioni necessarie. In secondo luogo, la comunicazione con gli interessati è standardizzata. Poiché tutte le informazioni sono contenute nell'elenco, tutti gli interessati ricevono le stesse informazioni su finalità, mezzi e periodo di conservazione, il che porta a una comunicazione più coerente e trasparente. In terzo luogo, l'elenco facilita anche la collaborazione con soggetti esterni, come l'Incaricato federale della protezione dei dati e delle informazioni (IFPDT). Quando l'FDPIC richiede informazioni sul trattamento dei dati, l'azienda può semplicemente fornire l'elenco invece di dover preparare relazioni separate per ogni singolo trattamento dei dati.

2. Il diritto di accesso

32 Il diritto all'informazione di cui all'art. 25 della LDP è un diritto della persona interessata che può essere fatto valere in base alla legge sulla protezione dei dati. Con il diritto all'informazione è possibile verificare la legittimità del trattamento dei dati e l'interessato ha il diritto di chiedere l'autorizzazione o la cancellazione dei dati. Ai sensi dell'art. 25 della FADP, l'interessato riceve tutte le informazioni sui propri dati personali per poter far valere i propri diritti, ovvero l'identità del responsabile del trattamento, le finalità del trattamento e i dati personali trattati. I diritti che possono essere fatti valere in seguito sono, ad esempio, il diritto alla rettifica dei dati personali raccolti in modo errato o all'eliminazione di questi ultimi (art. 32 LDP).

Un registro delle attività di trattamento garantisce e sostiene il diritto di accesso, in quanto comprende pienamente le informazioni che devono essere comunicate all'interessato ai sensi dell'art. 25 LADP. Con un registro correttamente tenuto, l'interessato riceve informazioni complete, uniformi e corrette sui dati raccolti. Si garantisce un'informazione adeguata e si aumenta la sicurezza per entrambe le parti, poiché l'azienda ha una migliore visione d'insieme dei dati raccolti e corre meno rischi di violare le norme sulla protezione dei dati. Se l'elenco non è corretto, il responsabile del trattamento può non registrare correttamente le informazioni sul trattamento dei dati o adottare precauzioni di sicurezza insufficienti. Ciò comporta il rischio di violazioni della protezione dei dati e può comportare conseguenze legali. 33

F. Dati all'estero (art. 12 cpv. 2 lett. g)

Secondo l'art. 12 cpv. 1 lett. g LADP, quando i dati vengono divulgati all'estero, è necessario indicare il rispettivo paese e le garanzie di cui all'art. 16 cpv. 2 LADP. Queste disposizioni garantiscono che la persona interessata sia informata del trasferimento dei suoi dati personali all'estero e che vengano adottate misure di protezione dei dati adeguate. L'elenco delle attività di trattamento può includere questi requisiti indicando lo scopo esatto del trasferimento dei dati all'estero e il nome del paese di destinazione. Inoltre, l'elenco dovrebbe contenere anche informazioni sulle garanzie adottate ai sensi dell'articolo 16, paragrafo 2, della FADP, al fine di rassicurare l'interessato sull'esistenza di garanzie adeguate. È importante che l'interessato sia informato in modo chiaro e comprensibile del fatto che i suoi dati saranno trasferiti all'estero e delle misure di protezione adottate nel processo. In questo modo si garantisce il diritto all'informazione e si protegge la privacy dell'interessato. Questi requisiti rafforzano la protezione dei dati in caso di trattamento e divulgazione transfrontaliera dei dati. In linea di principio, i dati personali possono essere divulgati all'estero solo se il Consiglio federale ha deciso che il Paese in questione garantisce un'adeguata protezione dei dati. I paesi che dispongono di un livello adeguato di protezione dei dati sono stabiliti dal Consiglio federale e pubblicati nell'allegato 1 dell'ordinanza sulla protezione dei dati. Una protezione inadeguata è garantita, tra gli altri, dalla Russia, da gran parte dei Paesi africani e sudamericani, nonché da tutta l'Asia (con l'eccezione di Israele). 34

35 L'art. 16 cpv. 2 LADP richiede un trattato internazionale, clausole contrattuali di protezione dei dati, garanzie specifiche approvate dall'IFPDT, clausole di protezione standard o specifiche interne vincolanti di protezione dei dati aziendali, anch'esse approvate dall'IFPDT (art. 16 lett. a-e LADP). Queste disposizioni si applicano ora in caso di divulgazione di dati non solo se il Paese stesso non garantisce una protezione adeguata, ma anche per tutte le divulgazioni estere.

III. CONFRONTO CON IL DIRITTO DELL'UE

36 L'articolo 12 della LADP, come molti altri articoli dopo la revisione totale, presenta alcuni parallelismi con i requisiti del GDPR. Ad esempio, l'art. 12 è stato redatto in modo analogo all'art. 30 DPA. Sia l'art. 30 DPA che l'art. 12 DPA richiedono che sia gli enti pubblici che i privati tengano un registro. In esso deve essere indicata l'identità del responsabile del trattamento e dell'incaricato del trattamento. Entrambe le disposizioni richiedono informazioni sullo scopo del trattamento, sulla categorizzazione dei dati personali trattati e dei destinatari, sulle garanzie per il trasferimento all'estero, sul periodo di conservazione e sulle misure tecniche e organizzative per l'attuazione della sicurezza dei dati. Anche l'esenzione dalla creazione di un elenco di trattamento dei dati è mantenuta sia nell'art. 30 del GDPR che nell'art. 12 del DPA. L'espressione "se possibile" (comma 1, lettere f e g) consente una certa flessibilità, come nella legge svizzera sulla protezione dei dati. Il contenuto di un elenco non è definito in modo uguale e rigoroso per ogni azienda, ma si basa sulla precisione con cui i dati trattati possono essere circoscritti in primo luogo. Pertanto, non si può sempre dire con certezza quando i dati saranno cancellati, né tutte le aziende seguono misure tecniche e organizzative analoghe e generalmente riconosciute. Un elenco di dati dovrebbe anche essere in grado di adattarsi alla rispettiva attività.

37 Le differenze tra le disposizioni emergono sporadicamente nelle formulazioni e nelle spiegazioni. Analogamente all'IFPDT in Svizzera, l'autorità di controllo della protezione dei dati nell'UE assume funzioni simili, come il controllo della conformità al GDPR o alla LPD. L'articolo 30 del GDPR richiede inoltre che l'identità del responsabile della protezione dei dati sia indicata nell'elenco, se esiste nell'azienda. Il trasferimento all'estero deve essere specificamente indicato ai sensi del GDPR e la forma dell'elenco deve essere scritta. Gli enti pubblici o i privati hanno inoltre l'obbligo, ai sensi del diritto

dell'Unione, di mettere a disposizione dell'autorità di controllo, su richiesta, l'elenco delle attività di trattamento. In genere è richiesta una cooperazione in buona fede con le autorità pubbliche.

Oltre all'art. 30 del GDPR, l'art. 24 della Direttiva 2016/680 elabora il contenuto di un registro delle attività di trattamento. Vale la pena ricordare che l'articolo 24 della direttiva prevede anche l'uso della profilazione (articolo 24 cpv. 1, lett. e) e l'indicazione della base giuridica per il trasferimento dei dati personali (articolo 24 cpv. 1 lett. g)) in un registro dei trattamenti. Ciò non è previsto dalla normativa svizzera, ma può essere coperto da informazioni supplementari nelle finalità del trattamento o nelle categorie di dati personali trattati. 38

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 14 LPD

Un commentario di Martin Steiger

CITAZIONE SUGGERITA

Martin Steiger, Kommentierung zu Art. 14 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Steiger, N. XXX zu Art. 14 DSG.

Sezione 2:
Trattamento da parte di titolari privati con sede o domicilio all'estero

Art. 14 Rappresentante

[1] I titolari privati del trattamento con sede o domicilio all'estero designano un rappresentante in Svizzera se trattano dati personali concernenti persone in Svizzera e il trattamento:

a. è legato a un'offerta di merci o prestazioni o finalizzato a porre sotto osservazione il comportamento di dette persone;

b. è un trattamento su grande scala;

c. è un trattamento periodico; e

d. comporta un rischio elevato per la personalità delle persone interessate.

[2] Il rappresentante funge da interlocutore per le persone interessate e l'IFPDT.

[3] Il titolare del trattamento pubblica il nome e l'indirizzo del rappresentante.

STRUTTURA

In breve 218
I. Aspetti generali 218
A. scopo 218
B. storia delle origini 218
II. obbligo di nominare un responsabile della protezione dei dati (cpv. 1) 219
A. ambito personale 219
B. Ambito di applicazione materiale 220
1. in relazione all'offerta di beni o servizi o all'osservazione del comportamento di persone in Svizzera (lit. a) 220
2. trattamento completo (lit. b) 221
3. trattamento regolare (lett. c) 221
4. rischio elevato per la personalità degli interessati (lett. d). 221
III. funzione del responsabile della protezione dei dati (cpv. 2) 222
IV. nomina volontaria di un responsabile della protezione dei dati 223
V. comunicazione del nome e dell'indirizzo (cpv. 3) 223
Bibliografia 224

IN BREVE

L'art. 14 LPD disciplina l'obbligo di nominare un responsabile della protezione dei dati in Svizzera da parte dei responsabili del trattamento privati con sede all'estero. L'obbligo sussiste solo a determinate condizioni cumulative ed è probabile che nella pratica si applichi solo a pochi responsabili del trattamento. La rappresentanza ha lo scopo di fungere da punto di contatto per le persone interessate e per l'LPD, al fine di facilitare l'applicazione della LPD nei confronti di determinati responsabili del trattamento all'estero. I responsabili del trattamento devono pubblicare il nome e l'indirizzo della loro rappresentanza, ad esempio come parte dell'informativa sulla privacy sul loro sito web.

I. ASPETTI GENERALI

A. scopo

1 I responsabili del trattamento che non hanno una sede legale in Svizzera devono designare una rappresentanza in Svizzera a determinate condizioni, che sono raramente soddisfatte. La formulazione di questi requisiti comporta un'incertezza giuridica sul momento in cui essi sono soddisfatti.

2 L'obbligo può essere giustificato dall'ampio campo di applicazione territoriale della LPD, poiché quest'ultima si applica a tutte le questioni che hanno un impatto in Svizzera, anche se sono state avviate all'estero (art. 3 cpv. 1 LPD). L'obbligo di designare un rappresentante è volto a migliorare l'applicabilità pratica della LPD, analogamente alla rappresentanza per la protezione dei dati nell'UE ai sensi dell'art. 27 LPD.

B. storia delle origini

3 Durante il dibattito parlamentare, la LPD è stata integrata con la rappresentanza per la protezione dei dati ai sensi degli articoli 14 e 15 LPD. I due articoli, insieme alle "Disposizioni generali", formano la seconda sezione "Trattamento dei dati da parte di responsabili privati con sede o domicilio all'estero" del secondo capitolo. La struttura si basa sulla rappresentanza dell'UE per la protezione dei dati ai sensi dell'art. 27 DSGVO. Di conseguenza, il rappresentante per la protezione dei dati può essere una persona giuridica o

una persona fisica. Il Regolamento sulla protezione dei dati (DSGVO) non menziona la rappresentanza.

La rappresentanza per la protezione dei dati accenna alle richieste politiche di un foro competente obbligatorio per le grandi piattaforme Internet straniere, in particolare per le piattaforme di social media, in materia di diritto penale e civile, ma non le attua. Un'eventuale attuazione di queste richieste di un domicilio obbligatorio potrebbe essere realizzata da un progetto di consultazione del Consiglio federale sulla regolamentazione delle grandi piattaforme di comunicazione annunciato per il 2024, secondo il quale tali piattaforme dovrebbero designare un punto di contatto e un rappresentante legale in Svizzera. 4

II. OBBLIGO DI NOMINARE UN RESPONSABILE DELLA PROTEZIONE DEI DATI (CPV. 1)

L'art. 14 cpv. 1 LPD stabilisce le condizioni alle quali i titolari del trattamento devono eccezionalmente nominare un rappresentante per la protezione dei dati in Svizzera. A differenza della rappresentanza dell'UE per la protezione dei dati ai sensi dell'art. 27 cpv. 1 e 2 DSGVO, non esiste un obbligo generale con eccezioni. Di conseguenza, il numero di responsabili del trattamento dei dati interessati sarà probabilmente esiguo. 5

L'IFPDT può ordinare o decretare la designazione di un rappresentante come misura amministrativa (art. 51 cpv. 4 LPD). 6

La violazione dell'obbligo di designare un rappresentante non rientra nelle disposizioni penali di cui agli artt. 60 e segg. LPD. L'inosservanza dell'ordine dell'IFPDT di designare un rappresentante può essere punita con una multa (art. 63 LPD). 7

A. ambito personale

L'obbligo di designare un rappresentante si applica ai responsabili del trattamento privati (art. 5 lett. j LPD) con sede o domicilio all'estero se trattano dati di persone in Svizzera (art. 5 lett. a e b LPD) e se il trattamento soddisfa i requisiti cumulativi di cui all'art. 14 cpv. 1 lett. a-d LPD. A differenza della rappresentazione della protezione dei dati dell'UE, l'obbligo in Svizzera 8

si applica solo ai responsabili del trattamento e non anche agli incaricati del trattamento.

B. Ambito di applicazione materiale

1. in relazione all'offerta di beni o servizi o all'osservazione del comportamento di persone in Svizzera (lit. a)

9 L'art. 14 cpv. 1 lett. a) LPD si basa sui requisiti alternativi per l'ambito territoriale della LPD con l'offerta o l'osservazione di comportamenti (art. 3 cpv. 2 LPD), piuttosto che sul principio dell'effetto ai sensi dell'art. 3 cpv. 1 LPD. Di conseguenza, il requisito si applica solo se l'offerta o l'osservazione di un comportamento ha un effetto su una situazione di fatto in Svizzera. Un semplice collegamento con un'offerta o un'osservazione comportamentale non è sufficiente.

10 Il primo requisito cumulativo di cui all'art. 14 cpv. 1 lett. a LPD è soddisfatto da un lato se il trattamento dei dati personali è connesso all'offerta di beni e servizi a persone in Svizzera. Secondo il considerando 80 dell'art. 27 cpv. 3 DSGVO, è sufficiente un'offerta gratuita o libera.

11 La sola accessibilità delle offerte, ad esempio in un'app su una piattaforma di social media o tramite un sito web, non è sufficiente. Sono necessari indizi concreti del fatto che un'offerta sia effettivamente rivolta a persone in Svizzera. Possibili indicazioni sono, ad esempio, i contenuti nelle lingue nazionali svizzere, le opzioni di consegna in Svizzera, i prezzi in franchi svizzeri, i prezzi con l'indicazione dell'IVA svizzera, la pubblicazione di un numero di telefono svizzero o l'uso di un dominio di primo livello svizzero (.ch o .swiss).

12 Per contro, il primo requisito cumulativo ai sensi dell'art. 14 cpv. 1 lett. a LPD è soddisfatto se il trattamento è effettuato in relazione all'osservazione del comportamento di persone in Svizzera in alternativa all'offerta o contemporaneamente all'offerta. Il termine "osservazione del comportamento" è da intendersi ai sensi dell'art. 3 cpv. 2 DSGVO. La semplice registrazione dell'accesso a un servizio online o a un sito web non è quindi sufficiente. Deve esserci un effettivo targeting di individui in Svizzera o l'osservazione deve portare a una profilazione in relazione agli interessati in Svizzera. Pertanto, la disposizione dovrebbe applicarsi ai fornitori di

piattaforme Internet come ByteDance, Google e Meta, ma non, ad esempio, ai gestori di negozi online, a condizione che il loro modello commerciale non sia incentrato sui dati e che la profilazione degli utenti venga effettuata solo nella misura abituale per i propri scopi di marketing.

2. trattamento completo (lit. b)

Il secondo requisito cumulativo ai sensi dell'articolo 14 cpv. 1 lettera b), LPD è soddisfatto se il trattamento dei dati personali è esteso. Cosa si intenda per "trattamento esteso" non è spiegato nella legge. 13

L'art. 22 cpv. 2 lett. a LPD cita il trattamento esteso di dati personali particolarmente sensibili come esempio di trattamento di dati ad alto rischio, ma non spiega cosa si intenda per "esteso". I criteri possibili sono un numero elevato di persone interessate in Svizzera o una grande quantità di dati su persone in Svizzera. 14

3. trattamento regolare (lett. c)

Il terzo requisito cumulativo ai sensi dell'art. 14 cpv. 1 lett. c LPD è soddisfatto se vi è un trattamento regolare dei dati personali. Cosa si intenda per "trattamento regolare" non è spiegato nella legge. 15

È ovvio che non vi è regolarità se i responsabili del trattamento trattano i dati personali solo occasionalmente o per un periodo di tempo limitato. D'altro canto, è probabile che la regolarità esista se un responsabile del trattamento tratta regolarmente i dati personali per svolgere le proprie attività (ad esempio, l'offerta attraverso un negozio online) o per perseguire un modello di business incentrato sui dati (ad esempio, il monitoraggio attraverso una piattaforma di social media). 16

4. rischio elevato per la personalità degli interessati (lett. d).

Il quarto requisito cumulativo ai sensi dell'art. 14 cpv. 1 lett. d LPD è soddisfatto se il trattamento comporta un rischio elevato per la personalità delle persone interessate. Questo requisito corrisponde all'approccio basato sul rischio della LPD, ma senza menzionare i diritti fondamentali degli interessati (cfr. anche, ad esempio, l'art. 5, lett. g) LPD: profilazione ad alto rischio; l'art. 22 cpv. 1 e 2 LPD: valutazione d'impatto sulla protezione dei dati; l'art. 24 cpv. 1 LPD: notifica delle violazioni della sicurezza dei dati). La 17

mancanza di menzione dei diritti fondamentali degli interessati è probabilmente una svista legislativa, viste le altre menzioni nella LPD.

18 Il trattamento dei dati che presenta un rischio elevato per la personalità degli interessati è probabilmente raro nella pratica. Pertanto, le valutazioni d'impatto sulla protezione dei dati raramente rivelano un rischio elevato o tale rischio viene eliminato con misure appropriate.

III. FUNZIONE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (CPV. 2)

19 Il responsabile della protezione dei dati funge da punto di contatto per gli interessati e l'IFPDT. Gli interessati e l'IFPDT possono contattare la rappresentanza, ma non sono obbligati a farlo. La rappresentanza è considerata giuridicamente come un diritto di assistenza.

20 La rappresentanza è quindi un punto di contatto alternativo per gli interessati e l'IFPDT in quanto autorità speciale accanto al responsabile del trattamento. Se il responsabile del trattamento ha nominato un responsabile della protezione dei dati, esistono in totale tre diversi punti di contatto alternativi (art. 10 cpv. 1 e 2 LPD).

21 Il responsabile della protezione dei dati di un titolare del trattamento non può agire contemporaneamente come responsabile della protezione dei dati dello stesso titolare del trattamento. La rappresentanza sarebbe incompatibile con l'indipendenza del consulente per la protezione dei dati (art. 10 cpv. 3 lett. a e b LPD).

22 Per le persone interessate, la rappresentanza come punto di contatto presenta il particolare vantaggio di poter rivolgere i propri dubbi in materia di protezione dei dati direttamente al responsabile del trattamento in Svizzera, in particolare nell'ambito dei diritti di cui agli artt. 25 e segg. LPD. Nel caso di titolari di archivi di dati senza rappresentanza in Svizzera, ad esempio, gli interessati devono rivolgere le richieste di informazioni ai rispettivi titolari di archivi di dati o ai loro responsabili della protezione dei dati presso la loro sede legale o il loro luogo di residenza all'estero.

23 Per l'IFPDT, la rappresentanza come punto di contatto ha il particolare vantaggio di non dover raggiungere i titolari dei dati all'estero tramite l'assistenza giudiziaria internazionale.

La legge non specifica le lingue in cui gli interessati possono rivolgersi alla rappresentanza. Nel caso di una rappresentanza legata a un'offerta, gli interessati dovrebbero essere in grado di contattare la rappresentanza almeno nella lingua dell'offerta o in una delle lingue dell'offerta. La limitazione alle lingue nazionali non sembra appropriata. L'IFPDT dovrebbe poter contattare la rappresentanza in una delle quattro lingue ufficiali svizzere (art. 33a APG per analogia). 24

IV. NOMINA VOLONTARIA DI UN RESPONSABILE DELLA PROTEZIONE DEI DATI

Il titolare del trattamento può nominare un responsabile della protezione dei dati in Svizzera anche senza l'obbligo di cui all'articolo 14 cpv. 1 LPD. Il titolare del trattamento può anche affidare al rappresentante volontario e a quello obbligatorio compiti che vanno oltre gli obblighi di cui agli artt. 14 e segg. LPD. 25

V. COMUNICAZIONE DEL NOME E DELL'INDIRIZZO (CPV. 3)

Il titolare del trattamento deve comunicare il nome e l'indirizzo del proprio responsabile della protezione dei dati. Nel caso di una persona giuridica come responsabile del trattamento dei dati, la ragione sociale corrisponde al nome. La pubblicazione di un indirizzo e-mail o di un numero di telefono non è espressamente richiesta. Tuttavia, quando si pubblica nello spazio digitale, è ovvio offrire un'opzione di contatto digitale, come in particolare un indirizzo e-mail. In confronto, l'art. 13 cpv. 1 lett. a DSGVO non prevede solo l'"indirizzo", ma anche i "dati di contatto". 26

Per svolgere la funzione di punto di contatto (art. 14 cpv. 2 DSGVO), il nome e l'indirizzo del rappresentante devono essere pubblicati in una forma facilmente reperibile e accessibile. È ovvio pubblicare le informazioni come parte della dichiarazione generale sulla protezione dei dati sul sito web del responsabile del trattamento o, se necessario, anche nell'impronta. 27

Contrariamente agli obblighi di informazione di cui all'art. 13 f. DSGVO, il nome e l'indirizzo della rappresentanza in Svizzera non rientrano nell'obbligo di informazione di cui all'art. 19 f. LPD. 28

29 A differenza dell'incaricato della protezione dei dati (art. 10 cpv. 3 lett. d LPD), non sussiste alcun obbligo di notifica della rappresentanza all'IFPDT. L'IFPDT deve scoprire dalle informazioni pubblicate se il titolare del trattamento ha designato un rappresentante o informarsi direttamente presso il rappresentante.

BIBLIOGRAFIA

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 15 LPD

Un commentario di Martin Steiger

CITAZIONE SUGGERITA

Martin Steiger, Kommentierung zu Art. 15 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Steiger, N. XXX zu Art. 15 DSG.

Art. 15 Obblighi del rappresentante

[1] Il rappresentante tiene un registro delle attività di trattamento del titolare del trattamento; il registro contiene le indicazioni di cui all'articolo 12 capoverso 2.

[2] Su richiesta, il rappresentante trasmette all'IFPDT le indicazioni contenute nel registro.

[3] Su richiesta, il rappresentante fornisce alle persone interessate informazioni su come esercitare i loro diritti.

STRUTTURA

In breve 227
I. Aspetti generali 227
II. compiti del rappresentante per la protezione dei dati 227
A. elenco delle attività di trattamento (cpv. 1) 227
B. obbligo di notifica all'IFPDT (cpv. 2) 228
C. Informazioni agli interessati (cpv. 3) 228
Bibliografia 229

IN BREVE

L'art. 15 LPD elenca alcuni ulteriori obblighi del rappresentante per la protezione dei dati ai sensi dell'art. 14 LPD. Il rappresentante deve tenere un registro delle attività di trattamento per il titolare del trattamento e fornire all'IFPDT le informazioni pertinenti su richiesta. Inoltre, il rappresentante deve fornire agli interessati, su richiesta, informazioni sull'esercizio dei loro diritti.

I. ASPETTI GENERALI

L'art. 15 LPD elenca alcuni ulteriori obblighi del rappresentante per la protezione dei dati oltre a quelli previsti dall'art. 14 cpv. 2 e 3 LPD (funzione di punto di contatto, art. 14 cpv. 2 LPD, e pubblicazione dei dati di contatto, art. 14 cpv. 3 LPD). L'elenco di cui all'art. 15 LPD deve essere inteso come non esaustivo a causa dell'ampio ruolo della rappresentanza come punto di contatto. 1

II. COMPITI DEL RAPPRESENTANTE PER LA PROTEZIONE DEI DATI

A. elenco delle attività di trattamento (cpv. 1)

Secondo la formulazione, il rappresentante per la protezione dei dati deve tenere un registro delle attività di trattamento del responsabile del trattamento (cpv. 1). Questo obbligo va oltre quello previsto dall'articolo 30 cpv. 1 del DSGVO, secondo cui l'autorità di controllo della protezione dei dati dell'UE deve tenere un registro solo per le attività di trattamento che sono soggette alla sua competenza. Questo obbligo eccessivo, che in ogni caso va ben oltre il DSGVO, è probabilmente una svista legislativa. 2

L'esenzione per le aziende con meno di 250 dipendenti ai sensi dell'art. 12 cpv. 5 LPD in combinato disposto con l'art. 24 LPD non si applica. L'art. 24 DPA non si applica alla rappresentanza per la protezione dei dati. Ai sensi dell'art. 14 cpv. 1 lett. a LPD, il rappresentante per la protezione dei dati deve essere designato solo se il trattamento da parte del titolare del trattamento comporta, tra l'altro, un rischio elevato per la personalità degli interessati. Ciò 3

corrisponde all'approccio generale basato sul rischio della LPD, come espresso in particolare nell'art. 24 LPD.

4 Le informazioni contenute nell'elenco devono essere conformi all'art. 12 cpv. 2 LPD. In pratica, il responsabile del trattamento terrà un elenco parziale delle attività di trattamento che hanno un impatto sulla Svizzera e ne metterà una copia a disposizione della rappresentanza.

B. obbligo di notifica all'IFPDT (cpv. 2)

5 La rappresentanza deve notificare all'IFPDT le informazioni contenute nell'elenco su richiesta (cpv. 2), anche senza una procedura amministrativa. In pratica, è probabile che la rappresentanza comunichi il repertorio all'IFPDT anziché limitarsi a fornire le informazioni in esso contenute.

6 L'obbligo si applica quindi indipendentemente dall'obbligo del titolare del trattamento di fornire all'IFPD tutti i documenti necessari nell'ambito di un'indagine (art. 49 cpv. 3 LPD) e anche indipendentemente dal potere dell'IFPD di ordinare l'accesso a tutti gli elenchi necessari delle attività di trattamento nell'ambito di un'indagine (art. 50 cpv. 1 lett. a LPD).

7 Per ottenere le informazioni contenute nell'elenco, l'IFPDT non deve ricorrere all'assistenza giudiziaria internazionale con la rappresentanza come punto di contatto. La rappresentanza in Svizzera può solo fornire informazioni già disponibili.

8 Una rappresentanza designata volontariamente non è tenuta a mantenere un elenco in quanto tale.

C. Informazioni agli interessati (cpv. 3)

9 In qualità di punto di contatto (art. 14 cpv. 2 LPD), la rappresentanza per la protezione dei dati deve fornire agli interessati che ne fanno richiesta informazioni sull'esercizio dei loro diritti ai sensi degli artt. 25 e segg. LPD su richiesta.

10 La rappresentanza deve consentire agli interessati che ne fanno richiesta di esercitare i propri diritti. La rappresentanza deve informare gli interessati, ad esempio, su quali recapiti e con quali mezzi possono esercitare il loro diritto all'informazione (art. 25 e segg. LPD) nei confronti del responsabile del trattamento e se il responsabile del trattamento ha nominato un consulente

per la protezione dei dati (art. 10 LPD) che può essere consultato (art. 10 cpv. 2 LPD).

L'obbligo di informazione del titolare del trattamento (art. 19 e segg. LPD) resta impregiudicato dall'obbligo di informazione della rappresentanza. Il titolare del trattamento può anche incaricare il rappresentante di fornire altre informazioni agli interessati. 11

BIBLIOGRAFIA

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 18 LPD

Un commentario di Apollo Dauag

CITAZIONE SUGGERITA

Apollo Dauag, Commentario all'art. 18 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Dauag, art. 18 LPD N. XXX.

Art. 18 Pubblicazione di dati personali in forma elettronica

La pubblicazione di dati personali per mezzo di servizi d'informazione e di comunicazione automatizzati allo scopo di informare il pubblico non è considerata una comunicazione all'estero, anche se i dati possono essere consultati all'estero.

STRUTTURA

In breve 233
I. Definizione e sistematica 233
II. Intenzione del legislatore 234
III. Presupposti 234
A. Obiettivo: informazione del pubblico attraverso l'accesso generale 234
B. Mezzi: servizi automatizzati di informazione e comunicazione 235
IV. Conseguenze giuridiche 235
V. Significato nella pratica 236
Bibliografia 237
I materiali 237

IN BREVE

Chi rende accessibili in modo legittimo dati personali su Internet a scopo informativo per il pubblico (e quindi per una cerchia indefinita di persone) non è tenuto a soddisfare i requisiti per la comunicazione all'estero.

I. DEFINIZIONE E SISTEMATICA

L'articolo 18 stabilisce le condizioni alle quali la **diffusione generale** di dati personali su Internet non è considerata una comunicazione all'estero. 1

La pubblicazione di dati personali in forma elettronica ai sensi dell'articolo 18 conclude la terza sezione «Comunicazione di dati personali all'estero». Oltre al principio di cui all'art. 16 e alle eccezioni di cui all'art. 17, l'art. 18 descrive le condizioni per la cessazione dell'applicabilità delle suddette disposizioni relative alla comunicazione all'estero. Se le condizioni sono soddisfatte, l'**inapplicabilità degli articoli 16 e 17 ha effetto giuridico**. 2

Si tratta di una **presunzione giuridica**, che è irrefutabile: se la comunicazione soddisfa i presupposti di cui all'articolo 18 (base della finzione), essa non è considerata conforme ai requisiti per la comunicazione all'estero di cui agli articoli 16 e 17 (conseguenza della finzione). 3

Questa presunzione non pregiudica il fatto che si tratti di una comunicazione. Si tratta quindi di un'operazione di trattamento. I **principi generali (di trattamento)** di cui all'art. 6 segg. devono essere rispettati in ogni momento. 4

Nell'ambito della **revisione totale** della LPD, la disposizione relativa alla «comunicazione transfrontaliera» (art. 6 aLPD) è stata trasferita in una sezione separata intitolata «Comunicazione di dati personali all'estero». L'ammissibilità della comunicazione alle condizioni ivi stabilite (precedentemente art. 6 cpv. 1 e cpv. 2 lett. a aLPD) è ora disciplinata come principio nell'art. 16 e le eccezioni (precedentemente art. 6 cpv. 2 lett. b-g aLPD) sono ora elencate nell'art. 17. 5

La «pubblicazione in forma elettronica» (precedentemente art. 5 OPSD) è stata trasferita all'art. 18 con tre precisazioni redazionali. Nel progetto e nel messaggio era citata come art. 15, mentre nel progetto preliminare non era 6

ancora contenuta. Inoltre, questa disposizione non ha destato particolare attenzione nel **processo legislativo**.

7 La conseguenza giuridica dell'articolo 18 è esclusiva, motivo per cui la pubblicazione su Internet **non costituisce un'eccezione** ai sensi dell'articolo 17 capoverso 1 lettere a–f e, di conseguenza, non vi è menzionata.

II. INTENZIONE DEL LEGISLATORE

8 Internet non conosce confini nazionali. La pubblicazione di dati personali su Internet comporta inevitabilmente la loro **accessibilità a livello globale, anche** in paesi privi di un'adeguata protezione dei dati. Poiché la cerchia dei destinatari è globale e indeterminata, il responsabile in Svizzera non può soddisfare i requisiti per una divulgazione ammissibile all'estero. Il legislatore accetta il rischio di violazioni della personalità che ne deriva come una «concessione alla crescente digitalizzazione».

9 L'accessibilità in paesi privi di un'adeguata protezione dei dati può essere resa più difficile dai **blocchi nazionali** (blocchi IP, cosiddetti «geoblocking»), ma non può essere impedita in modo insuperabile.

III. PRESUPPOSTI

10 Due presupposti devono essere soddisfatti **in modo cumulativo**, altrimenti la messa a disposizione generale è considerata una comunicazione all'estero.

A. Obiettivo: informazione del pubblico attraverso l'accesso generale

11 La **pubblicazione** deve (già per definizione logica) mirare a informare il pubblico creando un accesso generale.

12 Non possono essere posti requisiti aggiuntivi al **bisogno di informazione**: esso è soddisfatto se il trattamento dei dati personali per la pubblicazione su Internet è lecito, in particolare proporzionato e conforme allo scopo.

13 Può essere considerato **pubblico** solo un gruppo di destinatari con residenza indeterminabile: se la residenza all'estero è determinabile o la consultabilità è controllabile (ad esempio tramite blocchi per Paese, vedi sopra N. 9), sarebbe ragionevole che la persona responsabile soddisfacesse i requisiti per una

comunicazione ammissibile all'estero. Tuttavia, una restrizione geografica è in contraddizione con l'accesso generale.

Per **accesso generale** si intende che l'informazione è resa accessibile senza restrizioni. L'accesso non deve tuttavia essere gratuito o senza registrazione. La registrazione non modifica il rischio: a causa dell'accessibilità globale, anche i destinatari registrati provenienti da un Paese con un'adeguata protezione dei dati possono trasferirsi in un Paese senza un'adeguata protezione dei dati e consultare da lì i dati personali pubblicati. 14

B. Mezzi: servizi automatizzati di informazione e comunicazione

In una formulazione tecnologicamente neutra, l'articolo 18 menziona i «servizi automatizzati di informazione e comunicazione». Nei commenti si parla di «Internet o servizi basati su Internet» e «siti web, blog o anche servizi di informazione come Twitter ecc.». Rientrano in questa categoria anche «la pubblicazione tramite app, servizi di streaming, portali di video on demand e servizi simili». Sono comprese **tutte le forme di pubblicazione in formato elettronico** che consentono l'accessibilità a livello globale. Ciò vale anche per le newsletter via e-mail. 15

Secondo il presente parere, l'**ubicazione del server** è irrilevante: in primo luogo, il rischio di accessibilità da paesi senza un'adeguata protezione dei dati (senza blocchi nazionali, cfr. sopra N. 9) sussiste indipendentemente dall'ubicazione del server. In secondo luogo, anche in caso di memorizzazione iniziale in Svizzera, non è possibile impedire la duplicazione su server con ubicazioni all'estero. In terzo luogo, la LPD si applica anche a fatti che hanno ripercussioni in Svizzera, anche se sono stati causati all'estero. La distinzione tra server con sede in Svizzera e server con sede all'estero non sembra pertinente in questo caso. 16

IV. CONSEGUENZE GIURIDICHE

Se le **condizioni sono soddisfatte**, la pubblicazione in forma elettronica non è considerata una comunicazione all'estero ai sensi dell'articolo 16 LPD. Non devono essere esaminate le eccezioni di cui all'articolo 17 LPD. 17

Se i **requisiti non sono soddisfatti**, la pubblicazione in forma elettronica è considerata una comunicazione all'estero ai sensi dell'articolo 16 LPD. Possono sussistere eccezioni ai sensi dell'articolo 17 LPD. Una violazione 18

dell'articolo 16 LPD (comunicazione senza adeguata protezione) è considerata una violazione degli obblighi di diligenza e può comportare le conseguenze penali di cui all'articolo 61 lettera a LPD.

V. SIGNIFICATO NELLA PRATICA

19 Di fatto, la presunzione giuridica di cui all'articolo 18 costituisce la **base per la pubblicazione di dati personali su Internet** e consente quindi la partecipazione alla comunicazione mediatica moderna: gli ostacoli applicabili alla comunicazione all'estero non possono essere superati regolarmente dalle persone responsabili con uno sforzo ragionevole.

20 Dal punto di vista giuridico, la soppressione dei presupposti per una comunicazione ammissibile all'estero costituisce solo un **privilegio specifico della persona responsabile in Svizzera**: la pubblicazione di dati personali su Internet deve soddisfare in ogni momento i requisiti del trattamento e della comunicazione. Le pubblicazioni che sono contrarie allo scopo o che violano in altro modo i principi di trattamento non possono essere privilegiate.

21 Ai sensi dell'articolo 3, le disposizioni della LPD si applicano in linea di principio anche al trattamento effettuato all'estero (dei dati personali pubblicati su Internet). Anche se il legislatore accetta il rischio di violazioni della personalità connesso alla reperibilità globale, il testo dell'articolo 18 non contiene **alcun privilegio generale per la persona responsabile all'estero**. Le ulteriori comunicazioni (successive alla pubblicazione su Internet) non sono quindi soggette ai requisiti relativi alla comunicazione all'estero, ma devono comunque soddisfare i requisiti relativi al trattamento e alla comunicazione.

22 Per gli organi federali valgono **requisiti supplementari**: l'articolo 36 capoverso 5 prevede, oltre al requisito di una base giuridica per la pubblicazione di questi dati (ad esempio la legge sulla trasparenza), l'obbligo di cancellare i dati in questione dal «servizio automatizzato di informazione e comunicazione» non appena non sussiste più un interesse pubblico all'accesso pubblico.

23 Per quanto risulta, questa disposizione (né come art. 5a OPSD né come art. 18) non è stata ancora recepita in una sentenza pubblicata.

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 19 LPD

Un commentario di Matthias Glatthaar / Annika Schröder

CITAZIONE SUGGERITA

Matthias Glatthaar/Annika Schröder, Kommentierung zu Art. 19 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Glatthaar/Schröder, N. XXX zu Art. 19 DSG.

Capitolo 3: Obblighi del titolare e del responsabile del trattamento

Art. 19 Obbligo di informare sulla raccolta di dati personali

[1] Il titolare del trattamento informa in modo adeguato la persona interessata sulla raccolta di dati personali; tale obbligo sussiste anche se i dati non sono raccolti presso la persona interessata.

[2] Al momento della raccolta, il titolare del trattamento fornisce alla persona interessata le informazioni necessarie affinché questa possa far valere i propri diritti secondo la presente legge e sia garantito un trattamento trasparente dei dati; fornisce almeno le informazioni seguenti:

a. l'identità e i dati di contatto del titolare del trattamento;

b. lo scopo del trattamento;

c. se del caso, i destinatari o le categorie di destinatari cui sono comunicati dati personali.

[3] Se i dati personali non sono raccolti presso la persona interessata, il titolare del trattamento la informa inoltre sulle categorie di dati personali trattati.

[4] Se i dati personali sono comunicati all'estero, il titolare del trattamento informa la persona interessata sullo Stato o sull'organismo internazionale destinatario e, se del caso, sulle garanzie di cui all'articolo 16 capoverso 2, oppure sull'applicazione di un'eccezione secondo l'articolo 17.

[5] Se i dati personali non sono raccolti presso la persona interessata, il titolare del trattamento le fornisce le informazioni di cui ai capoversi 2–4 entro un mese dalla ricezione dei dati. Se comunica questi dati personali prima della scadenza di detto termine, il titolare del trattamento fornisce alla persona interessata tali informazioni al più tardi al momento della comunicazione dei dati.

STRUTTURA

In breve ... 242
I. Aspetti generali ... 242
A. Scopo della legge ... 242
B. Storia ... 243
C. Classificazione e delimitazione ... 244
D. Note interpretative ... 245
II. Soggetto obbligato e fattore di collegamento (cpv. 1) ... 245
A. Soggetto obbligato ... 245
B. Fattore di connessione ... 246
III. Contenuto delle informazioni (cpv. 2-4) ... 247
A. Informazioni obbligatorie ... 247
1. Generalità ... 247
2. Dati di contatto ... 247
3. Finalità del trattamento ... 248
4. Destinatari dei dati ... 248
5. Dati personali trattati ... 249
6. Stati destinatari ... 250
7. Decisioni individuali automatizzate ... 251
B. Ulteriori informazioni ... 251
IV. Modalità di informazione (cpv. 5; art. 13 DPA) ... 252
A. Tempo ... 252
B. Forma ... 253
C. Messa a disposizione ... 254
D. Comunicazione ... 256
V. Consigli pratici ... 257
A. Procedura e strumenti ... 257
B. Preparazione e progettazione ... 258
VI. Applicazione e conseguenze legali ... 260
A. Diritto amministrativo ... 260
B. Diritto penale ... 260
C. Diritto civile ... 261
D. DSGVO ... 261
VII. Criticità della norma ... 262
Bibliografia ... 262
I Materiali ... 264

IN BREVE

L'obbligo di informazione ai sensi dell'art. 19 LPD riguarda le dichiarazioni sulla protezione dei dati che sono importanti nella pratica e mira specificamente ad aumentare la trasparenza del trattamento dei dati. Esso integra il principio generale di trasparenza e richiede che gli interessati siano informati dei punti chiave del trattamento dei dati ogni volta che vengono raccolti dati personali. Il catalogo delle informazioni minime da fornire è più breve di quello del DSGVO e comprende informazioni di contatto, finalità del trattamento, categorie di dati trattati, categorie di destinatari dei dati, informazioni sui trasferimenti all'estero e informazioni sulle decisioni individuali automatizzate. Tuttavia, l'art. 19 LPD va oltre il DSGVO in un punto e richiede anche l'indicazione degli Stati destinatari, mentre è sufficiente l'indicazione di gruppi di Paesi o regioni. Nella maggior parte dei casi, le informazioni non devono essere comunicate attivamente agli interessati ed è sufficiente che siano facilmente accessibili su Internet. L'obbligo di fornire informazioni è uno dei reati punibili per legge ai sensi della legge sulla protezione dei dati riveduta: Chiunque ometta intenzionalmente di fornire informazioni o fornisca intenzionalmente informazioni false o incomplete può essere multato. Considerando che nella pratica le dichiarazioni sulla protezione dei dati non vengono quasi mai lette o comprese nel dettaglio, sembra discutibile che l'obbligo di fornire informazioni raggiunga effettivamente l'obiettivo di aumentare la trasparenza nel trattamento dei dati.

I. ASPETTI GENERALI

A. Scopo della legge

1 L'art. 19 LPD stabilisce l'obbligo del responsabile del trattamento di fornire informazioni quando ottiene dati personali. Ciò riguarda le comunicazioni sulla protezione dei dati, che sono importanti nella pratica, e le dichiarazioni sulla protezione dei dati, che sono molto comuni nella vita commerciale. L'obbligo di informazione è una delle disposizioni fondamentali della legge sulla protezione dei dati, il che si riflette talvolta nel fatto che è una delle disposizioni della nuova legge sulla protezione dei dati che è punibile per legge.

L'obiettivo dell'obbligo di informazione è aumentare la trasparenza del trattamento dei dati. La trasparenza del trattamento dei dati personali è un principio fondamentale della legge sulla protezione dei dati e l'aumento della trasparenza è stato un obiettivo dichiarato della revisione della LPD. Gli interessati devono sapere che i dati che li riguardano vengono trattati e devono avere la possibilità di conoscere i punti chiave del trattamento. 2

La trasparenza del trattamento dei dati dovrebbe consentire agli interessati di prendere una decisione informata sull'utilizzo di offerte e servizi e di esercitare i diritti garantiti dalla legge sulla protezione dei dati. L'obbligo di fornire informazioni serve quindi indirettamente anche a rafforzare i diritti degli interessati, il che corrisponde a un altro obiettivo della revisione. 3

Infine, secondo il messaggio, l'obbligo di informazione mira a sensibilizzare la popolazione sulla protezione dei dati e quindi a promuovere la protezione dei dati in generale. 4

B. Storia

L'art. 19 LPD amplia l'obbligo di fornire informazioni già contenuto nella precedente LPD quando si ottengono dati personali. Secondo la vecchia legge, gli interessati dovevano essere informati solo in caso di acquisizione di dati personali particolarmente sensibili o di profili della personalità. Ora i responsabili del trattamento devono informare gli interessati ogni volta che ottengono dati personali. Anche il catalogo delle informazioni obbligatorie è stato moderatamente ampliato dalla nuova LPD. La nuova LPD riunisce inoltre le disposizioni che in precedenza erano suddivise in diversi articoli e crea un regolamento uniforme per il trattamento dei dati da parte dei responsabili privati e degli organi federali. 5

L'aumento della trasparenza del trattamento dei dati è stato uno dei principali obiettivi della revisione della LPD. Inoltre, la Convenzione 108 sulla protezione dei dati, vincolante per la Svizzera, prescrive l'obbligo generale di fornire informazioni quando si ottengono dati personali, che deve essere attuato nel diritto nazionale. Anche la direttiva (UE) 2016/680, rilevante per lo spazio Schengen, prevede un obbligo di informazione. L'estensione dell'obbligo di informazione era quindi indiscussa in linea di principio nel processo legislativo. Con poche modifiche, il testo diventato legge corrisponde alla versione della bozza. 6

C. Classificazione e delimitazione

7 L'art. 19 LPD integra l'obbligo generale di trasparenza dell'art. 6 LPD. Mentre l'obbligo di trasparenza crea un livello base di trasparenza, l'obbligo di fornire informazioni si basa su questo e risponde a un'esigenza di informazione più ampia. Il responsabile del trattamento deve non solo garantire che la raccolta dei dati sia riconoscibile come tale, ma anche fornire agli interessati determinate informazioni sulle finalità e sulle modalità del trattamento. Il paragone alimentare di David Rosenthal è esemplificativo: deve essere immediatamente riconoscibile per i consumatori che il prodotto in questione è una marmellata di fragole (requisito di trasparenza), mentre l'elenco degli ingredienti e altri dettagli si trovano sull'etichetta dell'alimento, che può essere consultata se interessati (requisito di informazione).

8 A differenza dell'obbligo di trasparenza, l'obbligo di informazione non è una concretizzazione del diritto della personalità di cui all'art. 28 del Codice Civile, ma ha natura di diritto pubblico. La violazione dell'obbligo di informazione non costituisce pertanto una violazione dei diritti della personalità. Di conseguenza, la violazione non può essere giustificata ai sensi dell'art. 31 LPD. Le eccezioni e le limitazioni all'obbligo di informazione sono esaustivamente normate nell'art. 20 LPD.

9 L'art. 19 LPD è a sua volta integrato dall'art. 21 LPD, che prevede un obbligo speciale di informazione in caso di automazione completa di decisioni importanti, e concretizzato dall'art. 13 LPD, che stabilisce i requisiti per il tipo e le modalità di informazione.

10 L'obbligo di informazione deve essere distinto dal concetto di consenso. Una dichiarazione di protezione dei dati garantisce la trasparenza richiesta dalla legge, ma non costituisce un consenso ai sensi della legge sulla protezione dei dati e non legittima un atto di protezione dei dati che richiede una giustificazione ai sensi dell'art. 30 f. FADP. LPD e non legittima un trattamento dei dati che richiede una giustificazione. Esiste tuttavia una connessione tra l'obbligo di informazione e il consenso nella misura in cui, da un lato, la base informativa necessaria per un consenso valido può essere creata mediante una dichiarazione sulla protezione dei dati e, dall'altro, l'adempimento dell'obbligo di informazione e l'ottenimento del consenso possono coincidere in singoli casi (ad esempio, se una dichiarazione di consenso contiene tutte le informazioni obbligatorie richieste dall'art. 19 LPD).

D. Note interpretative

L'obbligo di fornire informazioni nella legge sulla protezione dei dati rivista è modellato sull'obbligo di fornire informazioni contenuto nel DSGVO. Tuttavia, l'art. 19 LPD non si limita a riprodurre l'obbligo di informazione contenuto nel DSGVO, ma stabilisce un regolamento che si discosta deliberatamente da alcune parti del DSGVO. Ad esempio, l'LPD prescrive un numero inferiore di informazioni minime rispetto al DSGVO e concede esenzioni più ampie dall'obbligo di informazione. Come illustrato da Thomas Steiner, l'art. 19 LPD deve quindi essere interpretato autonomamente e la prassi del GDPR deve essere consultata solo per confermare e verificare la plausibilità del risultato dell'interpretazione svizzera. 11

Con David Vasella, va sostenuta anche un'interpretazione prudente dell'obbligo di informazione: Da un lato, l'art. 19 LPD è anche una norma penale e il principio di legalità del diritto penale richiede quindi un'interpretazione restrittiva. In secondo luogo, l'adempimento dell'obbligo di informazione comporta spese considerevoli per le aziende, che incidono sulla libertà economica ai sensi dell'art. 27 Cost. ed è ammissibile solo se l'interferenza è proporzionata e limitata alla misura necessaria. Infine, è necessaria una certa moderazione nell'interpretazione, poiché la trasparenza di base è già garantita dall'obbligo di trasparenza di cui all'art. 6 LPD e l'obbligo di fornire informazioni protegge solo un bisogno di informazioni che va oltre. 12

II. SOGGETTO OBBLIGATO E FATTORE DI COLLEGAMENTO (CPV. 1)

A. Soggetto obbligato

L'obbligo di informazione è rivolto al responsabile del trattamento, ossia alla persona privata o all'ente federale che decide lo scopo e i mezzi del trattamento. Gli incaricati del trattamento che sono vincolati da istruzioni non sono soggetti ad alcun obbligo di informazione in relazione al trattamento effettuato per conto del responsabile del trattamento. 13

Il responsabile non è tenuto ad adempiere personalmente all'obbligo di informazione. Può anche delegare la fornitura di informazioni a un incaricato del trattamento o a un terzo (ad esempio, a un'agenzia web quando gestisce un 14

sito web). Anche in questi casi, tuttavia, il responsabile del trattamento rimane responsabile del corretto adempimento dell'obbligo di informazione.

B. Fattore di connessione

15 L'obbligo di informazione scatta in caso di raccolta di dati personali, indipendentemente dal fatto che il titolare del trattamento li raccolga direttamente dall'interessato o indirettamente. Il tipo di raccolta dei dati è rilevante solo per il momento dell'informazione. Inoltre, non è determinante se si tratta di una raccolta permanente o ripetuta o, come nel caso di una lotteria isolata, di una sola volta. In entrambi i casi, le informazioni devono essere fornite. Una raccolta (rinnovata) che fa scattare l'obbligo di informazione è anche quando i dati personali già esistenti vengono utilizzati per uno scopo nuovo o aggiuntivo.

16 Non è necessario fornire informazioni se il titolare del trattamento riceve dati personali per caso o in altro modo senza alcuna azione da parte sua. Ne sono un esempio le richieste di giornalisti, le candidature alla cieca, le raccomandazioni dei dipendenti o le richieste di e-mail non richieste. Tuttavia, le informazioni devono essere fornite se tali dati personali ottenuti involontariamente devono essere utilizzati per scopi nuovi o aggiuntivi.

17 Il collegamento dell'obbligo di informazione all'acquisizione dei dati significa, in termini di diritto transitorio, che gli interessati non devono essere informati sul trattamento dei dati già in corso al momento dell'entrata in vigore della nuova LPD (a meno che l'informazione non sia già stata fornita in un momento precedente). Tuttavia, le persone interessate, ad esempio i clienti esistenti, devono essere informate al più tardi quando si ottengono nuovi dati, ad esempio gli abbonati a un servizio online quando effettuano il prossimo accesso o i partecipanti a un programma di fidelizzazione dei clienti quando effettuano il prossimo acquisto.

III. CONTENUTO DELLE INFORMAZIONI (CPV. 2-4)

A. Informazioni obbligatorie

1. Generalità

L'art. 19 LPD contiene nei paragrafi 2-4 un catalogo di informazioni obbligatorie che devono essere fornite agli interessati: Dati di contatto del responsabile del trattamento, finalità del trattamento, destinatari o categorie di dati, categorie di dati trattati, nonché gli Stati destinatari in caso di trasferimento all'estero e la loro salvaguardia. Alcuni dettagli obbligatori aggiuntivi si trovano in altre disposizioni della LPD, come l'art. 21 LPD relativo alle decisioni individuali automatizzate e l'art. 14 cpv. 3 LPD relativo alla rappresentanza in Svizzera. 18

Rispetto al DSGVO, il catalogo della LPD è breve. Questo è positivo e lascia almeno un po' di spazio al di fuori del campo di applicazione del DSGVO per informare con un senso di proporzione e per contrastare il "sovraccarico di informazioni" che oggi dilaga. La flessibilità del regolamento della LPD consente di limitare le informazioni ai dettagli rilevanti in base al rischio e di omettere i dettagli non necessari. 19

2. Dati di contatto

In primo luogo, devono essere forniti il nome e i dati di contatto del responsabile del trattamento. La legge non specifica quali dati di contatto debbano essere comunicati. Tuttavia, è ovvio fornire almeno un indirizzo postale e un indirizzo e-mail. È anche possibile fornire un numero di telefono, ma vista la possibilità di contatti invadenti da parte di malintenzionati, questo è insolito e sconsigliato. 20

I responsabili del trattamento domiciliati all'estero devono inoltre pubblicare il nome e i dati di contatto di eventuali rappresentanze in Svizzera nominate ai sensi dell'art. 14 LPD (art. 14 cpv. 3 LPD). 21

La divulgazione dei dati di contatto di qualsiasi consulente per la protezione dei dati nominato è volontaria. Ciò è in contrasto con la DSGVO, dove i dati di contatto del responsabile della protezione dei dati devono essere forniti. Tuttavia, la LPD fornisce un (piccolo) incentivo a pubblicare i dati di contatto del consulente per la protezione dei dati, in quanto i responsabili del 22

trattamento dei dati privati possono avvalersi dell'esenzione dalla notifica all'IFPDT solo in caso di rischi residui elevati, dopo aver effettuato una valutazione dell'impatto sulla protezione dei dati. A tal fine, è sufficiente la pubblicazione di una casella di posta elettronica funzionale (ad es. datenschutz@unternehmen.ch); non è necessario indicare il nome del consulente per la protezione dei dati.

3. Finalità del trattamento

23 Il responsabile del trattamento deve indicare le finalità del trattamento dei dati personali. Gli interessati devono quindi essere in grado di sapere per quali finalità vengono trattati i loro dati.

24 Il livello di dettaglio con cui vengono descritte le finalità del trattamento è lasciato al responsabile del trattamento. In genere sono ammesse descrizioni brevi come "comunicazione", "elaborazione di contratti", "sviluppo di prodotti" o "marketing". Tuttavia, descrizioni più dettagliate o esempi esplicativi sono più utili, il che è raccomandato anche in considerazione del principio di limitazione delle finalità, poiché formulazioni poco chiare verrebbero interpretate in modo restrittivo in base al principio di fiducia, in caso di dubbio, a svantaggio del responsabile.

25 Oltre alle finalità di trattamento attuali, è possibile elencare anche possibili finalità di trattamento future. Ciò è consentito anche se il trattamento in questione non è ancora concretamente previsto, ma è solo una possibilità. Alla luce del principio di limitazione delle finalità di cui all'art. 6 cpv. 3 LPD, molte aziende saranno propense a redigere tali informative eccessive al fine di mantenere il più possibile aperti i nuovi utilizzi dei dati, il che tuttavia non favorisce la chiarezza delle informative sulla protezione dei dati.

4. Destinatari dei dati

26 Occorre poi specificare le categorie di destinatari a cui vengono comunicati i dati personali. L'inserimento dell'espressione "se del caso" nel testo normativo ha scarsa rilevanza pratica, poiché tra i destinatari rientrano anche gli incaricati del trattamento degli ordini utilizzati dal responsabile del trattamento e al giorno d'oggi quasi nessun responsabile del trattamento può fare a meno degli incaricati del trattamento degli ordini. Anche i corresponsabili sono considerati destinatari, così come, ovviamente, i "terzi" veri e propri. Anche le società del gruppo appartenenti allo stesso gruppo

sono destinatarie, ma non le entità appartenenti alla stessa persona giuridica, come i singoli dipartimenti o le filiali.

Le categorie possono essere definite dal responsabile a propria discrezione; la legge non prevede alcuna specificazione al riguardo. Sono ipotizzabili, ad esempio, categorie definite in modo piuttosto ristretto come "fornitore di servizi informatici", "società di logistica" o "fornitore di servizi di riscossione", ma sono ammesse anche categorie più ampie come "incaricato del trattamento degli ordini". 27

Invece di categorie di destinatari, possono essere nominati anche singoli destinatari. Tuttavia, l'indicazione dei singoli destinatari è facoltativa; l'indicazione delle categorie è sufficiente. In pratica, si rinuncia a indicare i singoli destinatari, in quanto la maggior parte delle aziende ha un numero piuttosto elevato di destinatari (in particolare i responsabili degli ordini) e la compilazione di un elenco corrispondente richiederebbe molto tempo. La divulgazione di destinatari specifici è diventata piuttosto diffusa nel settore online, dove gli strumenti di terze parti utilizzati sono talvolta elencati singolarmente in relazione ai cookie e a tecnologie simili. 28

5. Dati personali trattati

Vanno poi indicate le categorie di dati personali trattati. Anche in questo caso, il responsabile del trattamento è libero di definire le categorie a propria discrezione e di scegliere il livello di dettaglio che ritiene ragionevole e adeguato per fornire informazioni sufficienti agli interessati. Sono ipotizzabili categorie come "dati anagrafici", "dati comportamentali" o "dati di preferenza". Anche i "dati personali che richiedono una protezione speciale" o, in senso più stretto, i "dati sulla salute" sono categorie possibili. Di solito è utile specificare le categorie, talvolta piuttosto sfuggenti, con esempi di tipi di dati (ad esempio "nome", "indirizzo e-mail", "luogo di residenza") e renderle più tangibili. È inoltre utile, ma non obbligatorio, assegnare le singole categorie di dati a finalità di trattamento concrete. 29

Ai sensi dell'art. 19 cpv. 3 LPD, le categorie di dati trattati devono essere specificate solo se i dati non sono ottenuti direttamente dalla persona interessata. Ciò si basa sull'idea che, in questo caso, l'interessato ha solo bisogno di informazioni. Se, invece, l'interessato comunica personalmente i propri dati personali (ad esempio, compilando un modulo online o un 30

biglietto della lotteria o presentando una domanda di lavoro), conosce già i dati trattati dal responsabile del trattamento.

31 Seguendo questa idea, la restrizione deve essere interpretata in modo restrittivo e limitata ai casi in cui la persona interessata divulga consapevolmente i dati. D'altra parte, devono essere indicate anche le categorie di dati trattati, ad esempio se i dati sono raccolti direttamente dall'interessato, ma senza il suo coinvolgimento attivo e quindi potrebbe non essere a conoscenza del fatto che i dati che lo riguardano vengono trattati. È il caso, ad esempio, della raccolta automatizzata dei dati relativi alle transazioni quando si fanno acquisti nei negozi o nel commercio online o del web tracking su Internet. Per le stesse considerazioni, devono essere indicate anche le categorie di dati trattati se il responsabile del trattamento ricava nuovi dati dai dati ricevuti dall'interessato, ad esempio informazioni su interessi e affinità personali.

6. Stati destinatari

32 Se i dati personali vengono divulgati all'estero, devono essere indicati gli Stati destinatari. Ai sensi dell'art. 5 lett. e LPD, la divulgazione comprende non solo la trasmissione ma anche qualsiasi accesso ai dati personali dall'estero. Tali trasferimenti all'estero sono molto comuni nel mondo delle imprese, ad esempio quando si utilizzano servizi basati sul cloud.

33 Con l'obbligo di divulgare gli Stati destinatari, la LPD è inutilmente più severa del DSGVO, che richiede solo informazioni sulla divulgazione all'estero in sé, ma non sugli Stati destinatari. La LPD non tiene conto di quanto sia diventato internazionale il traffico di dati. Dopo tutto, anche ai sensi della LPD, non è necessario elencare i singoli Paesi, cosa che difficilmente sarebbe praticabile nella pratica. È sufficiente indicare gruppi di Paesi o regioni, ad esempio "UE/SEE" o "Europa". È ammessa anche l'indicazione "in tutto il mondo". Gli interessati possono vedere che i loro dati possono essere trattati in qualsiasi paese del mondo.

34 Se tra i Paesi destinatari ci sono Paesi che non hanno un livello adeguato di protezione dei dati, è necessario fornire informazioni aggiuntive: In tali costellazioni, devono essere rese note le garanzie fornite ai sensi dell'art. 16 cpv. 2 LPD per assicurare un livello adeguato di protezione dei dati o l'eccezione invocata ai sensi dell'art. 17 LPD. In questo caso, ad esempio, è

sufficiente fare riferimento alla stipula delle clausole contrattuali standard riconosciute dalla Commissione europea e dall'IFPDT, che sono di gran lunga lo strumento più diffuso per tutelare i trasferimenti all'estero.

7. Decisioni individuali automatizzate

Se il responsabile del trattamento utilizza decisioni individuali automatizzate, deve informare gli interessati di ciò e della possibilità di sottoporre la decisione a revisione umana su richiesta dell'interessato (art. 21 LPD). Le decisioni individuali automatizzate sono decisioni completamente automatizzate che hanno conseguenze legali per gli interessati o che li riguardano in altro modo significativo. L'obbligo di fornire informazioni si applica pertanto solo alle decisioni completamente automatizzate; non è necessario fornire informazioni sulle decisioni solo parzialmente automatizzate o assistite da computer. 35

B. Ulteriori informazioni

Nella pratica commerciale, molte aziende andranno oltre le informazioni obbligatorie sopra descritte e saranno generalmente guidate dal catalogo più completo del DSGVO. Soprattutto (ma non solo) le aziende più grandi e con orientamento internazionale si impegnano a redigere informative sulla protezione dei dati "conformi al GDPR", sia su base volontaria sia perché le loro operazioni di trattamento dei dati rientrano nell'ambito di applicazione (extraterritoriale) del GDPR. In particolare, il catalogo del DSGVO prevede anche informazioni sul periodo di conservazione, la base giuridica applicabile, gli eventuali interessi legittimi perseguiti, i diritti degli interessati e il diritto di ricorso. 36

Tuttavia, l'inclusione di tali informazioni aggiuntive nell'ambito della LPD non è solitamente richiesta dalla legge. Le informazioni che vanno oltre il catalogo minimo devono essere fornite solo se sono necessarie in un caso specifico per garantire un trattamento dei dati ragionevolmente trasparente (art. 19 cpv. 2 LPD). Ciò avverrà raramente ed è tanto più probabile quanto più sensibili sono i dati trattati, quanto più esteso è il trattamento, quanto più critiche sono le modalità del trattamento, quanto più critica è la finalità del trattamento e quanto più nuove sono le tecnologie utilizzate per il trattamento. Ai sensi dell'art. 19 cpv. 2 LPD, il principio guida è ciò che gli interessati devono sapere per poter esercitare i propri diritti. 37

38 È probabile che il catalogo del DSGVO rappresenti una sorta di limite superiore. È difficile immaginare i casi in cui, ai sensi della LPD, potrebbe essere necessario andare oltre le informazioni richieste dal DSGVO.

39 Il regolamento della LPD lascia teoricamente spazio anche alla possibilità di specificare la gestione dell'obbligo di informazione per un settore specifico in un codice di condotta ai sensi dell'art. 11 LPD. Tuttavia, tali codici di condotta settoriali non sono ancora riusciti ad affermarsi nella pratica e probabilmente svolgeranno solo un ruolo minore in futuro.

IV. MODALITÀ DI INFORMAZIONE (CPV. 5; ART. 13 DPA)

A. Tempo

40 A seconda che i dati personali siano ottenuti direttamente dalla persona interessata o indirettamente, le informazioni devono essere fornite in momenti diversi. L'acquisizione diretta avviene quando l'interessato fornisce al titolare del trattamento i propri dati di propria iniziativa (ad esempio, compilando un modulo o creando un account utente) o quando il titolare del trattamento raccoglie i dati attraverso l'osservazione stessa o con mezzi automatizzati (ad esempio, registrando le transazioni di acquisto o raccogliendo i dati di movimento attraverso un fitness tracker). L'acquisizione indiretta, invece, avviene quando il responsabile raccoglie i dati da fonti pubbliche (ad esempio, da notizie dei media o da registri pubblici), riceve dati da terzi (ad esempio, da un commerciante di indirizzi o da un'agenzia di credito) o ricava nuovi dati da banche dati esistenti (ad esempio, ricavando le preferenze analizzando i dati delle transazioni).

41 Nel caso di appalti diretti, le informazioni devono essere fornite contemporaneamente all'appalto. In pratica, ciò significa che le informazioni richieste devono essere facilmente accessibili al momento dell'appalto, ad esempio sul sito web del responsabile del trattamento. La fornitura di informazioni subito dopo la prima acquisizione dei dati, che era ancora consentita dalla vecchia legge, non è più consentita dalla nuova legge. Al contrario, le informazioni possono essere fornite prima dell'acquisizione, a condizione che il collegamento tra l'informazione e l'acquisizione sia sufficientemente riconoscibile per gli interessati.

Nel caso degli appalti indiretti, le informazioni non devono essere fornite immediatamente, ma solo entro un mese dal ricevimento dei dati (art. 19 cpv. 5 LPD). Tuttavia, il periodo di tolleranza di un mese richiede che i dati personali non vengano divulgati dal responsabile del trattamento a nessun altro destinatario. Se, invece, il responsabile del trattamento comunica i dati personali prima della scadenza del termine, il periodo di attesa non si applica e l'informazione deve essere fornita al più tardi al momento della comunicazione. Dal momento che anche le comunicazioni agli incaricati del trattamento degli ordini rientrano in questa fattispecie (ad esempio, l'archiviazione nel cloud), il rinvio delle informazioni ha un significato pratico limitato e le informazioni devono essere fornite immediatamente anche nel caso di appalti indiretti, che spesso richiedono una comunicazione attiva. Se ciò risulta impossibile da attuare, l'unico ricorso a disposizione del titolare del trattamento è quello di avvalersi di un'eccezione ai sensi dell'art. 20 LPD. 42

B. Forma

La LPD non prevede requisiti formali per la comunicazione delle informazioni. Sono sufficienti anche informazioni orali, ad esempio sotto forma di annunci su nastro. Nella pratica, tuttavia, si raccomanda di solito la forma testuale, se non altro per motivi di prova. 43

In pratica, il modo più comune di adempiere all'obbligo di informazione è attraverso dichiarazioni sulla protezione dei dati ("avviso sulla privacy" o "politica sulla privacy"). Una procedura comune è quella di descrivere un'ampia gamma di trattamenti dei dati in una nota generale sulla privacy (dall'attività con i clienti all'assunzione di personale alla collaborazione con i partner commerciali) e di integrarla con note sulla privacy specifiche per prodotti o servizi. In pratica, sono comuni anche le dichiarazioni speciali sulla protezione dei dati online ("cookie notice" o "cookie policy") per il trattamento dei dati in relazione alla visita di un sito web o di un'app. 44

Le dichiarazioni sulla protezione dei dati rappresentano un'informazione unilaterale per il titolare del trattamento e come tali possono essere adattate in modo flessibile per tenere conto della natura dinamica di molte operazioni di trattamento dei dati. Da un punto di vista pratico, l'unilateralità dell'informazione significa anche che non è necessaria una conferma o un'accettazione attiva della dichiarazione di protezione dei dati da parte degli interessati e quindi, nella maggior parte dei casi, si può fare a meno delle 45

caselle di controllo spesso presenti nei moduli online o nei processi di ordinazione.

46 È anche possibile includere le note sulla protezione dei dati nelle condizioni generali di contratto (CGC). A differenza delle dichiarazioni sulla protezione dei dati, tuttavia, le avvertenze sulla protezione dei dati contenute nelle CGV diventano parte del contratto e possono quindi essere modificate solo emendando il contratto, il che spesso si rivela troppo complicato nella pratica. Inoltre, l'obbligo di informazione può essere adempiuto solo nei confronti dei partner contrattuali (ma non nei confronti di altri soggetti interessati) per mezzo delle CGC. Si sconsiglia pertanto di integrare gli avvisi sulla protezione dei dati nelle CGC e di inserire nelle CGC solo un riferimento alla dichiarazione sulla protezione dei dati. Ulteriori disposizioni sulla protezione dei dati nelle CG sono giustificate al massimo se si vuole ottenere il consenso ai sensi della legge sulla protezione dei dati, sebbene il consenso ottenuto tramite le CG sia talvolta considerato in modo critico.

47 Le comunicazioni sulla protezione dei dati vengono interpretate in base alla regola dell'inusualità e dell'ambiguità, vale a dire che occorre fare particolare riferimento ai punti inusuali e che le formulazioni poco chiare vengono interpretate a svantaggio dell'autore. Ciò vale anche se le informative sulla protezione dei dati sono concepite come dichiarazioni sulla protezione dei dati o comunque come informazioni unilaterali, almeno nella misura in cui non sono puramente informative e possono anche avere un effetto legale, ad esempio definendo gli scopi del trattamento o come base informativa per eventuali consensi. Le informative sulla protezione dei dati integrate nelle CG sono inoltre soggette al controllo degli abusi ai sensi dell'art. 8 LCSl.

C. Messa a disposizione

48 Le informazioni obbligatorie devono essere facilmente accessibili agli interessati (art. 13 LPD). Non è necessario che gli interessati prendano effettivamente nota delle informazioni. Il principio dell'accesso non si applica, ma è sufficiente che gli interessati abbiano la possibilità di accedere alle informazioni senza grandi sforzi. L'accesso alle informazioni può quindi richiedere la collaborazione dell'interessato, anche perché la trasparenza di base è già garantita dall'obbligo di trasparenza e l'obbligo di fornire informazioni serve solo a soddisfare un'esigenza di informazione più ampia.

Tuttavia, i passi che l'interessato deve compiere per ottenere le informazioni devono essere ragionevoli. Non sarebbe più facilmente accessibile e quindi non sufficiente, ad esempio, la semplice designazione di una persona di contatto o l'invio della dichiarazione sulla protezione dei dati solo su richiesta. Per contro, è molto diffusa l'indicazione delle informazioni sulla protezione dei dati su un sito web. L'informazione su Internet è sufficiente, purché sia garantito che le informazioni sulla protezione dei dati siano facilmente reperibili sul sito e raggiungibili con pochi clic. In pratica, si è dimostrata efficace una sottopagina separata per la dichiarazione sulla protezione dei dati e il suo collegamento permanente nel cosiddetto footer, cioè nell'area in fondo a un sito web. 49

Le informazioni su Internet sono generalmente sufficienti anche se il trattamento dei dati avviene offline. Gli interessati sono ormai abituati a trovare le informazioni sulla protezione dei dati sul sito web dell'azienda e le danno addirittura per scontate. Le informative sulla protezione dei dati rese disponibili su Internet offrono anche diversi vantaggi, come una navigazione semplificata e ampie possibilità di progettazione user-friendly. Nella maggior parte dei casi, quindi, il passaggio a Internet è ragionevole. Solo in casi particolari, ad esempio quando si tratta di un trattamento delicato di dati personali particolarmente sensibili, quando si tratta di gruppi di persone anziane o quando l'accesso a un sito web non è ragionevole in termini di tempo a causa della situazione, può essere necessario, in via eccezionale, che gli interessati possano accedere a tutte le informazioni obbligatorie ai sensi dell'art. 19 LPD senza dover cambiare mezzo di comunicazione. 50

Un mezzo utile per facilitare il cambio di supporto è la visualizzazione di codici QR che possono essere scansionati con un telefono cellulare e che conducono all'informativa sulla protezione dei dati su Internet. Tali codici QR sono sempre più comuni nella pratica (ad esempio nella segnaletica per la videosorveglianza), ma non sono obbligatori per legge. 51

Non solo è consentita, ma è anche generalmente orientata alle esigenze degli interessati, l'informativa a più livelli, in cui al primo livello viene fornita solo una panoramica iniziale del trattamento dei dati e l'informativa completa viene fornita solo a un livello successivo. In linea di principio, il titolare del trattamento può definire a propria discrezione quali informazioni fornire a quale livello. Non esistono "informazioni di base" che devono essere fornite al primo livello. 52

53 La versione o la datazione dell'informativa sulla protezione dei dati può essere utile, ma non è richiesta dalla legge, così come non lo è l'archiviazione e la messa a disposizione delle versioni precedenti, che talvolta si riscontra nella pratica.

D. Comunicazione

54 La fornitura delle informazioni richieste è di solito sufficiente e non è necessaria una comunicazione attiva agli interessati. Anche i riferimenti alla dichiarazione sulla protezione dei dati nei moduli, nelle firme di posta elettronica, sulla carta intestata, nonché nelle conversazioni telefoniche e in altre comunicazioni simili, che talvolta si riscontrano nella pratica, non sono necessari secondo il punto di vista qui rappresentato; anche nei contratti, un riferimento esplicito alla dichiarazione sulla protezione dei dati sembra spesso superfluo. Nel caso della videosorveglianza, un pittogramma chiaramente visibile all'ingresso dell'area di vendita è di solito sufficiente a stabilire la trasparenza di base richiesta, a condizione che l'operatore sia riconoscibile nelle circostanze. In questi casi, si può prevedere che gli interessati consultino il sito web se desiderano saperne di più sul trattamento dei dati da parte dell'azienda in questione. Lo faranno anche intuitivamente e daranno per scontato che le note sulla protezione dei dati si trovino sul sito web.

55 La comunicazione attiva agli interessati è necessaria solo se l'interessato non sa (e non ha bisogno di sapere) che l'azienda in questione tratta dati che lo riguardano. Ciò accade spesso quando i dati personali non vengono raccolti direttamente dall'interessato, ma anche nei casi di raccolta diretta quando la raccolta dei dati avviene senza che l'interessato ne sia consapevole (ad esempio, quando le persone vengono registrate automaticamente quando entrano in un'area pubblica e vengono tracciati i percorsi a piedi). In questi casi, gli interessati devono essere informati attivamente dell'informativa sulla protezione dei dati (ad esempio, indicando l'URL o fornendo un codice QR), altrimenti non penserebbero nemmeno di consultare il sito web dell'azienda per informarsi sul trattamento dei dati.

56 Per le stesse ragioni, le modifiche alla dichiarazione sulla protezione dei dati devono essere comunicate ai clienti esistenti nell'ambito di obblighi continuativi, almeno se le finalità del trattamento sono ampliate e la modifica equivale quindi a un nuovo appalto. In caso contrario, gli interessati non

avrebbero alcuna indicazione del fatto che la dichiarazione sulla protezione dei dati potrebbe essere cambiata e che sarebbe quindi consigliabile visitare il sito web. In pratica, tali informazioni vengono solitamente inviate via e-mail o tramite banner pop-up in un negozio online o quando si accede a un account cliente. È possibile anche un avviso nella spedizione della fattura.

V. CONSIGLI PRATICI

A. Procedura e strumenti

Le informative sulla protezione dei dati dovrebbero essere preparate in stretta collaborazione con i responsabili commerciali e tecnici delle aree che effettuano il trattamento dei dati, in quanto queste funzioni conoscono meglio quali dati vengono utilizzati per quali scopi e in che modo. Spesso i portatori di conoscenze rilevanti si trovano nelle unità aziendali responsabili del trattamento intensivo dei dati, ad esempio i reparti di marketing, di analisi dei dati e le unità HR. In pratica, un approccio partecipativo basato su workshop che coinvolge questi portatori di conoscenza si è dimostrato efficace. Tuttavia, è anche possibile raccogliere informazioni tramite questionari strutturati o interviste. 57

Anche l'elenco dei trattamenti ai sensi dell'art. 12 LPD o dell'art. 30 DSGVO fornisce una prima panoramica delle operazioni di trattamento e spesso offre una buona base per identificare le operazioni di trattamento dei dati rilevanti. Inoltre, nella maggior parte dei casi l'elenco dei trattamenti contiene informazioni che possono essere utilizzate per preparare i dati obbligatori, come ad esempio informazioni sui tipi di dati trattati, sulle finalità del trattamento e sulle (categorie di) destinatari. 58

In pratica, esistono diversi strumenti che supportano le aziende nella preparazione delle comunicazioni sulla protezione dei dati, tra cui modelli di dichiarazioni sulla protezione dei dati che possono essere utilizzati come punto di partenza e adattati alle proprie esigenze. Ad esempio, le seguenti offerte sono ampiamente utilizzate: 59

- Modello di dichiarazione generale sulla protezione dei dati, che copre numerose attività di trattamento standard ed è allineato sia alla LPD che al

DSGVO, preparato da due rinomati studi legali svizzeri e disponibile sul sito https://dsat.ch/download/ (gratuitamente);

- Generatore di protezione dei dati di Datenschutzpartner per la creazione di una dichiarazione di protezione dei dati per i siti web con formulazioni campione per numerosi strumenti web comuni, disponibile all'indirizzo https://www.datenschutzpartner.ch/angebot-datenschutz-generator/ (a pagamento);
- Esempio di dichiarazione di protezione dei dati del professore universitario tedesco Thomas Hoeren per i gestori di siti web, disponibile all'indirizzo https://www.itm.nrw/wp-content/uploads/Musterdatenschutzerkaerung-nach-der-DSGVO_Stand_September_2022-1.docx (gratuito).

60 Secondo la comune concezione di governance, l'approvazione del contenuto della dichiarazione di protezione dei dati dovrebbe essere effettuata dagli organi di gestione responsabili del trattamento dei dati, ad esempio il comitato esecutivo. Il ruolo del responsabile della protezione dei dati o del consulente per la protezione dei dati e di altre funzioni legali e di conformità dovrebbe essere limitato, anche in considerazione del regime sanzionatorio, a una funzione di coordinamento e consulenza.

B. Preparazione e progettazione

61 L'ordinanza di attuazione della legge sulla protezione dei dati richiede informazioni precise e comprensibili (art. 13 LPD). Tuttavia, si tratta di criteri difficilmente giustiziabili (e nemmeno sanzionabili) e nella pratica dominano ancora testi di flusso dall'aspetto legalistico. A quanto pare, molte aziende ritengono che sia difficile ottenere un posizionamento positivo nei confronti della protezione dei dati e che quindi non valga la pena di investire risorse significative nella preparazione di avvisi sulla protezione dei dati di facile utilizzo.

62 Inoltre, non aiuta il fatto che la legge sulla protezione dei dati incentivi a considerare le informative sulla protezione dei dati principalmente come uno strumento difensivo e non come una comunicazione incentrata sul cliente: da un lato, in vista di strumenti normativi e sanzioni più severe, le aziende sono ansiose di includere formulazioni di apertura e clausole generali, proteggendosi così dalle accuse di informative sulla protezione dei dati errate

o incomplete. Dall'altro lato, in considerazione del principio della limitazione delle finalità, le aziende non vogliono precludersi alcun margine di manovra e si limitano a elencare possibili future finalità di trattamento nelle informative sulla protezione dei dati.

Nonostante questa sfortunata struttura di incentivi, nella pratica esistono diversi approcci promettenti per rendere le informative sulla protezione dei dati più facili da leggere e più in linea con le esigenze dei destinatari: 63

- Informazioni a più livelli ("approccio a strati"), in cui gli aspetti principali del trattamento dei dati sono presentati in primo luogo in modo chiaro e le informazioni dettagliate seguono solo a un livello successivo. Le informazioni stratificate comprendono anche testi pieghevoli ed esempi tangibili per illustrare le spiegazioni, a volte piuttosto astratte.
- L'uso di pittogrammi per la protezione dei dati che consentono agli interessati di ottenere rapidamente una prima panoramica del trattamento dei loro dati. Un esempio sono i pittogrammi standardizzati pubblicati dall'associazione Privacy Icons, che rendono riconoscibili a colpo d'occhio alcuni aspetti tipicamente rilevanti per gli interessati e sono già utilizzati da diverse importanti aziende svizzere.
- Cruscotti sulla protezione dei dati che forniscono un facile punto di accesso e consentono agli interessati di stabilire autonomamente le priorità e di ottenere informazioni mirate sui punti essenziali.
- Video esplicativi che introducono gli interessati all'argomento e forniscono loro una comprensione semplice dei contenuti più importanti.
- Elementi di gamification che trasmettono agli interessati gli aspetti chiave del trattamento dei dati in modo ludico.

Tali approcci di "legal design" possono aumentare significativamente l'accessibilità e la facilità di lettura delle informative sulla protezione dei dati e sono quindi da accogliere con favore in termini di trasparenza del trattamento dei dati. Tuttavia, non vi è alcun obbligo legale di utilizzare tali approcci di facile comprensione per il cliente, nemmeno ai sensi del DSGVO. 64

VI. APPLICAZIONE E CONSEGUENZE LEGALI

A. Diritto amministrativo

65 Se le persone interessate non sono state informate correttamente sul trattamento dei dati, l'IFPD può avviare un'indagine e ordinare la fornitura di informazioni conformi alla legge come misura amministrativa (art. 51 cpv. 3 lett. c LPD). L'IFPDT può agire d'ufficio o su segnalazione.

66 In linea di principio è possibile anche vietare il trattamento dei dati o ordinare una rettifica da parte dell'IFPD (art. 51 cpv. 1 LPD). Tuttavia, nella maggior parte dei casi, una misura così drastica non sarebbe proporzionata sulla base di informazioni non corrette.

B. Diritto penale

67 L'obbligo di fornire informazioni è uno degli obblighi della LPD soggetto a sanzioni penali. Chiunque non fornisca informazioni ai sensi dell'art. 19 LPD o fornisca informazioni false o incomplete può essere punito con una multa fino a 250.000 franchi svizzeri (art. 60 cpv. 1 LPD). L'obbligo di informazione è un dovere con un grande impatto esterno e la minaccia di una sanzione ha quindi il potenziale per essere usata specificamente come mezzo di pressione contro un'azienda o i dipendenti o i decisori responsabili.

68 Alcuni si chiedono se l'art. 19 LPD soddisfi il requisito di certezza del diritto penale di cui all'art. 1 CP e se una violazione dell'obbligo di informazione possa quindi essere sanzionata dal diritto penale. In ogni caso, si deve pretendere che, per quanto riguarda la completezza, vengano prese in considerazione solo le informazioni obbligatorie ai sensi dell'art. 19 cpv. 2-4 LPD. Eventuali informazioni aggiuntive da fornire ai sensi della clausola generale dell'art. 19 cpv. 2 non devono essere prese in considerazione.

69 In linea di principio, non è l'azienda a essere perseguibile, ma la persona o le persone fisiche responsabili della violazione (art. 64 cpv. 1 LPD in combinato disposto con l'art. 6 del Codice di procedura penale). Può trattarsi di personale direttivo che ha l'obbligo legale di garantire la conformità alla protezione dei dati, o di persone che hanno la responsabilità dei processi operativi all'interno dell'azienda e sono autorizzate a prendere decisioni su questioni relative all'obbligo di informazione. D'altro canto, coloro che si limitano a fornire assistenza sono complici e, in quanto tali, non sono punibili.

In alcuni casi, la persona fisica può non essere punita e l'azienda può invece essere multata. Ciò avviene se l'identificazione del colpevole richiederebbe misure investigative sproporzionate ed è possibile una multa non superiore a 50.000 franchi svizzeri (art. 64 cpv. 2 LPD in combinato disposto con l'art. 7 Codice di procedura penale).

Sono punibili solo gli atti intenzionali. Ciò include anche il dolo eventuale, ossia l'accettazione del reato. La commissione negligente del reato, invece, rimane impunita. Chi dimentica una dichiarazione, formula qualcosa in modo impreciso o omette deliberatamente qualcosa perché ritiene che non faccia parte delle informazioni obbligatorie non agisce intenzionalmente e rimane impunito. Al fine di escludere il più possibile l'azione intenzionale, le decisioni relative all'obbligo di informazione devono essere documentate in modo comprensibile in ogni caso, ad esempio per le considerazioni che vengono omesse o per le informazioni che vengono omesse. 70

L'art. 60 cpv. 1 LPD è un reato di applicazione. Una violazione dell'obbligo di informazione è quindi perseguibile solo su richiesta, ma non d'ufficio. Qualsiasi interessato può presentare un reclamo, ma non l'IFPDT. 71

C. Diritto civile

La violazione dell'art. 19 LPD, in quanto disposizione di diritto pubblico, non comporta di per sé una violazione dei diritti della personalità e non può quindi essere fatta valere dagli interessati in giudizio. 72

Gli interessati possono tuttavia far valere la violazione del principio generale di trasparenza come principio di trattamento e intentare un'azione legale su questa base presso il tribunale civile competente. 73

D. DSGVO

Nell'ambito di applicazione del DSGVO, le violazioni dell'obbligo di informazione possono essere punite con un'ammenda fino a 20 milioni di euro o al 4% del fatturato mondiale totale annuo (art. 83(5) DSGVO). Si tratta della sanzione più elevata tra le due previste dal DSGVO. A differenza del DSGVO, l'ammenda prevista dalla LPD è diretta principalmente contro l'azienda e non contro le persone fisiche che agiscono per conto dell'azienda. 74

75 Ai sensi del DSGVO, una violazione dell'obbligo di informazione può anche rendere nulla la base giuridica richiesta per il trattamento e quindi rendere illegale il trattamento dei dati.

VII. CRITICITÀ DELLA NORMA

76 L'obbligo di informazione è espressione di una concezione di base del diritto della protezione dei dati basata sull'autodeterminazione informativa. L'idea di base è che gli interessati si informino sul trattamento dei dati e, sulla base di ciò, decidano con cognizione di causa se acconsentire o meno al relativo trattamento dei loro dati e se esercitare uno dei diritti di protezione dei dati loro riconosciuti.

77 Nell'attuale mondo digitalizzato e basato sui dati, i limiti di questa comprensione di base stanno diventando sempre più evidenti. Il trattamento dei dati personali riguarda oggi tutti i settori della vita e gli interessati si trovano costantemente di fronte ad avvisi completi sulla protezione dei dati, per i quali spesso non hanno il tempo e di solito nemmeno le competenze necessarie. Il risultato è un sovraccarico di informazioni e una costante sensazione di essere sopraffatti. Per molti è economicamente razionale risparmiarsi questo sforzo e rimanere disinformati.

78 Ci si chiede quindi se il dovere di informazione raggiunga ancora l'obiettivo prefissato e giustifichi le spese ad esso associate. La sua base concettuale risale agli albori della protezione dei dati, quando il trattamento dei dati era ancora semplice. Da allora, tuttavia, il nostro mondo si è evoluto tecnologicamente e il moderno trattamento dei dati è spesso complesso. È quasi come chiedere a una compagnia aerea di pubblicare informazioni tecniche complete e aspettarsi che i potenziali passeggeri le utilizzino per farsi un'opinione sull'aeronavigabilità dell'aereo. Anche in questo caso, non si tratta di una soluzione né realistica né mirata. Sarebbe opportuno sviluppare nuovi approcci alla protezione dei dati che non si basino su una trasparenza superficiale.

BIBLIOGRAFIA

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).

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 20 LPD

Un commentario di Matthias Glatthaar / Annika Schröder

CITAZIONE SUGGERITA

Matthias Glatthaar/Annika Schröder, Kommentierung zu Art. 20 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Glatthaar/Schröder, N. XXX zu Art. 20 DSG.

Art. 20 Eccezioni all'obbligo di informare e limitazioni

[1] L'obbligo di informare secondo l'articolo 19 non sussiste se:

a. la persona interessata dispone già delle pertinenti informazioni;b.il trattamento dei dati personali è previsto dalla legge;c.il titolare del trattamento è un privato tenuto per legge a serbare il segreto; od.sono adempiute le condizioni di cui all'articolo 27.

[2] Se i dati personali non sono raccolti presso la persona interessata, l'obbligo di informare non sussiste inoltre qualora l'informazione:

a. non sia possibile; o

b. richieda un onere sproporzionato.

[3] Il titolare del trattamento può limitare o differire l'informazione oppure rinunciarvi se:

a. interessi preponderanti di un terzo lo esigono;

b. l'informazione pregiudica lo scopo del trattamento;

c. è un privato e:

lo esigono i suoi interessi preponderanti, e
non comunica i dati personali a terzi; o

d. è un organo federale e:

lo esige un interesse pubblico preponderante, in particolare la salvaguardia della sicurezza interna o esterna della Svizzera, o l'informazione rischia di compromettere un'indagine, un'istruzione o un procedimento amministrativo o giudiziario.

[4] Le imprese appartenenti al medesimo gruppo non sono considerate terzi ai sensi del capoverso 3 lettera c numero 2.

STRUTTURA

In breve 268
I. Aspetti generali 268
A. Scopo della legge 268
B. Storia delle origini 268
C. Sistema 269
D. Note interpretative 269
II. Eccezioni (cpv. 1 e 2) 269
A. Generalità 269
B. Conoscenza preventiva delle informazioni (cpv. 1 lett. a) 270
C. Trattamento prescritto dalla legge (cpv. 1 lett. b) 271
D. Obblighi di riservatezza previsti dalla legge (cpv. 1 lett. c) 272
E. Privilegio dei media (cpv. 1 lett. d) 274
F. Impossibilità di ottenere informazioni (cpv. 2 lett. a) 274
G. Sforzo sproporzionato (cpv. 2 lett. b) 275
III. Restrizioni 276
A. Generale 276
B. Interessi prevalenti di terzi (cpv. 3 lett. a) 276
C. Vanificazione dello scopo (cpv. 3 lett. b) 277
D. Interessi superiori della persona responsabile (cpv. 3 lett. c) 278
E. Interessi pubblici prevalenti (cpv. 3 lett. d n. 1) 279
F. Minaccia al procedimento (cpv. 3 lett. d n. 2) 279
Bibliografia 280
I Materiali 280

IN BREVE

L'art. 20 LPD contiene una serie di esenzioni dall'obbligo di informazione: da un lato, esenzioni in cui l'obbligo di informazione non si applica affatto, ad esempio se l'interessato dispone già delle informazioni pertinenti o se il trattamento è effettuato in adempimento di un obbligo legale. D'altro canto, la disposizione contiene restrizioni in cui l'obbligo di informazione continua a sussistere, ma l'informazione può essere limitata, rinviata o sospesa in singoli casi, ad esempio se l'informazione vanificherebbe lo scopo del trattamento o se interessi prevalenti sono in conflitto con l'informazione. L'articolo 20 LPD funge da correttivo a un obbligo di informazione completo e garantisce che l'obbligo di informazione non diventi un onere eccessivo per i responsabili del trattamento e rimanga limitato ai casi in cui è necessario per la protezione degli interessati.

I. ASPETTI GENERALI

A. Scopo della legge

1 L'art. 20 LPD prevede una serie di esenzioni dall'obbligo di fornire informazioni. La disposizione mira a garantire che l'obbligo di informazione si applichi quando è necessario per un trattamento trasparente dei dati e per la protezione degli interessati, mentre non si applica nei casi in cui sarebbe superfluo o sproporzionato. È un'espressione dello sforzo legislativo di trovare un equilibrio di interessi e di creare agevolazioni mirate. Rispetto al DSGVO, il catalogo di eccezioni dell'art. 20 LPD è piuttosto ampio.

B. Storia delle origini

2 L'art. 20 LPD riunisce le eccezioni e le limitazioni presenti in vari articoli della vecchia legge (art. 9, art. 14 cpv. 4 e 5, art. 18a e art. 18b aDSG) e le integra moderatamente. L'art. 20 LPD è rimasto indiscusso in linea di principio nelle deliberazioni parlamentari, anche se l'eccezione per lo sforzo sproporzionato è stata considerata troppo ampia da alcune parti del Parlamento. Il privilegio di gruppo ai sensi dell'art. 20 cpv. 4 LPD è stato aggiunto nelle deliberazioni parlamentari.

C. Sistema

La disposizione distingue tra eccezioni, in cui l'obbligo di fornire informazioni non si applica affatto, e restrizioni, in cui l'obbligo di fornire informazioni continua ad applicarsi in linea di principio, ma il responsabile del trattamento può limitare, rinviare o sospendere la fornitura di informazioni in singoli casi. L'art. 20 LPD si applica sia ai responsabili del trattamento dei dati privati che agli organi federali, ma distingue tra organi privati e organi federali nelle singole eccezioni e limitazioni. 3

Le eccezioni e le limitazioni contenute nell'art. 20 LPD sono esaustive. Una violazione dell'obbligo di informazione non può essere giustificata nemmeno ai sensi dell'art. 31 LPD, poiché l'obbligo di informazione di cui all'art. 19 LPD è di natura pubblicistica e non è una concretizzazione dei principi di trattamento di cui all'art. 6 LPD. 4

D. Note interpretative

Le eccezioni di cui all'art. 20 LPD sono piuttosto ampie e comprendono i casi in cui il trattamento dei dati è identificabile (base giuridica, cpv. 1 lett. b) o la riservatezza dei dati personali trattati è garantita (obbligo legale di segretezza, cpv. 1 lett. c), ma il bisogno di informazioni dell'interessato protetto dall'obbligo di informazione rimane insoddisfatto. È quindi opportuno interpretare i fatti in modo piuttosto restrittivo e allinearli allo scopo dell'obbligo di informazione. 5

II. ECCEZIONI (CPV. 1 E 2)

A. Generalità

L'art. 20 LPD prevede ai cpv. 1 e 2 un totale di sei situazioni in cui il responsabile del trattamento è completamente esonerato dall'obbligo di informare gli interessati. In queste situazioni, l'interessato non deve essere informato dell'applicabilità dell'eccezione. L'unica possibilità è quella di esercitare il diritto di accesso, anche se spesso l'interessato non ha motivo di chiedere l'accesso ai propri dati se non è a conoscenza del trattamento e il diritto di accesso è a sua volta soggetto a restrizioni simili (art. 26 LPD). 6

B. Conoscenza preventiva delle informazioni (cpv. 1 lett. a)

7 L'obbligo di fornire informazioni non si applica se l'interessato è già in possesso delle informazioni pertinenti. Gli interessati non devono essere informati su cose che già conoscono, il che è ovvio. Un'eccezione analoga all'obbligo di informazione si trova anche nel DSGVO. Nella vecchia LPD, l'eccezione era ancora un po' più ristretta e si riferiva al processo di informazione e non all'esistenza dell'informazione in sé (art. 14 cpv. 4 e art. 18a cpv. 3 aDSG: "se l'interessato è già stato informato").

8 L'eccezione significa inizialmente che gli interessati non devono essere nuovamente informati in caso di successivi acquisti di dati se sono già stati informati in occasione di un precedente acquisto. Il prerequisito è che le acquisizioni siano correlate dal punto di vista fattuale e non troppo distanti nel tempo. Si potrebbe pensare a singoli ordini in un negozio online, ad esempio, se le informazioni erano già state fornite al momento della creazione dell'account, o a un trattamento medico successivo se le informazioni erano già state fornite in relazione al trattamento iniziale.

9 Un'altra applicazione dell'eccezione si ha quando la persona interessata ha acconsentito al trattamento dei dati, in quanto un consenso valido ai sensi dell'art. 6 cpv. 6 LPD richiede per definizione informazioni sufficienti. Le informazioni richieste dall'art. 19 LPD possono quindi essere fornite anche tramite una dichiarazione di consenso.

10 Secondo il messaggio, l'eccezione dovrebbe coprire anche le situazioni in cui la persona interessata invia i propri dati personali al responsabile del trattamento senza l'intervento di quest'ultimo. Si tratta di un'eccezione di ampia portata, poiché la conoscenza dell'interessato si limita all'acquisizione dei dati. Tuttavia, esiste un interesse informativo legittimo in ulteriori circostanze del trattamento dei dati, nell'esempio di una domanda di lavoro menzionata dall'invio, ad esempio se (e per quanto tempo) i documenti di candidatura vengono conservati anche per lavori futuri, a chi possono essere trasmessi e dove vengono conservati.

11 Infine, rientrano nell'eccezione anche i casi in cui è chiaro che la persona interessata ha rinunciato al diritto alle informazioni ai sensi dell'art. 19 LPD o non ha alcun interesse nelle informazioni. Tuttavia, questo deve essere limitato a casi evidenti e in ogni caso non si può presumere se la persona

interessata ha reso i suoi dati personali pubblicamente accessibili (ad esempio, su un profilo di social media).

C. Trattamento prescritto dalla legge (cpv. 1 lett. b)

L'obbligo di informazione non si applica nemmeno se il trattamento dei dati è previsto dalla legge. Il ragionamento è che in questi casi il legislatore ha già definito i cardini del trattamento dei dati, ponderando i vari interessi, e informare gli interessati non fornirebbe quindi alcuna protezione aggiuntiva significativa. Il DSGVO contiene un'eccezione simile, ma limitata al caso degli appalti indiretti e soggetta alla condizione che la norma legislativa disciplini esplicitamente il trattamento dei dati e preveda misure adeguate per tutelare gli interessi legittimi degli interessati. 12

Per rientrare nell'eccezione, il trattamento stesso dei dati deve essere prescritto dalla legge o deve essere indispensabile per l'adempimento di un obbligo legale. Per quanto riguarda i responsabili del trattamento privati, è sufficiente una base sufficientemente precisa in una legge in senso sostanziale. Per gli organi federali, si applica lo standard dell'art. 34 LPD ed è necessaria una legge in senso formale se si tratta del trattamento di dati personali particolarmente sensibili, se viene effettuata una profilazione o se si tratta di una grave violazione dei diritti fondamentali. 13

I trattamenti di dati richiesti dalla legge sono numerosi nell'ordinamento giuridico e l'eccezione è quindi di grande importanza pratica. Tra gli esempi si possono citare la tenuta del registro delle azioni e la convocazione e lo svolgimento dell'assemblea generale degli azionisti nel caso di società per azioni; gli obblighi di identificazione e di determinazione del titolare effettivo ai fini della lotta al riciclaggio di denaro; gli obblighi di notifica delle autorità sanitarie in relazione alle malattie trasmissibili; il pagamento delle retribuzioni e la preparazione dei certificati da parte del datore di lavoro nel rapporto di lavoro; gli obblighi contabili ai sensi della normativa fiscale e previdenziale. 14

L'eccezione può essere invocata anche nel caso in cui il responsabile del trattamento dei dati abbia determinato egli stesso l'obbligo legale, ad esempio gli obblighi di identificazione ai sensi della legge sul riciclaggio di denaro attraverso l'avvio del rapporto commerciale o il trattamento indicato dalla legge sul lavoro attraverso la conclusione del contratto di lavoro. 15

16 Se il trattamento dei dati va oltre l'obbligo legale (ad esempio, se i dati raccolti per combattere una pandemia devono essere utilizzati anche per scopi di marketing), l'eccezione non si applica e occorre fornire informazioni. Non sono esenti dall'obbligo di informazione nemmeno le operazioni di trattamento dei dati che vengono effettuate solo a livello generale all'interno di un quadro giuridicamente definito, ma che sono eseguite volontariamente. Nel settore dei dipendenti, le informazioni sono quindi regolarmente richieste, ad esempio sotto forma di dichiarazione di protezione dei dati dei dipendenti. Anche se il quadro stabilito dall'art. 328b CO non viene superato, il trattamento dei dati nell'area dei dipendenti di solito va oltre quanto effettivamente prescritto dalla legge.

17 Nel caso degli organi federali, il trattamento dei dati personali ai sensi dell'art. 34 LPD si basa nella maggior parte dei casi su una base giuridica. Tuttavia, le relative disposizioni di legge sono spesso piuttosto generiche e spesso non sono in grado di garantire da sole la trasparenza richiesta dall'obbligo di informazione. Il cpv. 1 lett. b esonera quindi gli organi federali dall'obbligo di informazione solo se il trattamento dei dati è espressamente previsto dalla legge ed è descritto con sufficiente precisione. Come esempio di trattamento dei dati descritto con precisione nella legge, si possono utilizzare gli artt. 69f e 69g RTVA in combinazione con gli artt. 67 e 67a RTVA. Si possono citare gli artt. 67 e 67a RTVO. D'altro canto, esentare gli organi federali dall'obbligo di fornire informazioni per qualsiasi trattamento basato sulla legge sulla base del cpv. 1 lett. b comporterebbe un onere eccessivo per la trasparenza del trattamento dei dati da parte della Confederazione e renderebbe in gran parte obsoleta l'applicabilità dell'art. 19 LPD agli organi federali di per sé e le restrizioni previste dall'art. 20 cpv. 3 LPD specificamente per gli organi federali.

D. Obblighi di riservatezza previsti dalla legge (cpv. 1 lett. c)

18 Le persone fisiche soggette a un obbligo legale di riservatezza sono esenti dall'obbligo di fornire informazioni. Ciò vale in particolare per i gruppi professionali di cui all'art. 321 CP, come il clero, gli avvocati, i farmacisti e i medici. L'eccezione si applica solo (ma sempre) all'area di attività protetta dal segreto, ma non a qualsiasi altra attività di una persona appartenente a questi gruppi professionali. Se, ad esempio, l'avvocato o il medico generico tratta dati personali per l'acquisizione di clienti (inviti a eventi o invio di

informazioni sui clienti) o per la fornitura del proprio sito web, è soggetto all'obbligo di divulgazione per queste attività.

L'eccezione non si applica alla persona giuridica presso la quale la persona soggetta all'obbligo di riservatezza è impiegata o per la quale lavora. Un organismo di avvocati o un centro medico deve quindi fornire informazioni anche sul trattamento dei dati nell'area di attività protetta dal segreto (ad esempio, sui servizi di avvocati nell'area del monopolio o sui servizi sanitari). L'eccezione non si applica nemmeno agli organi federali. 19

Secondo il messaggio, l'eccezione di cui al cpv. 1, lettera c), regola un possibile conflitto di norme tra l'obbligo di riservatezza e l'obbligo di informazione, ma ciò non è convincente: anche nell'ambito delle attività protette da segreto, non verrebbero divulgati dati personali fornendo le informazioni richieste dall'art. 19 LPD e quindi non verrebbero divulgati segreti. Un avvocato, ad esempio, potrebbe facilmente informare in modo generico che i dati personali contenuti in un documento legale saranno trasmessi alla controparte e al tribunale competente. Allo stesso modo, un medico potrebbe informare della divulgazione di dati personali alla compagnia di assicurazione sanitaria ai fini della fatturazione. In questi casi il segreto professionale non verrebbe intaccato. Se tuttavia dovesse esistere un conflitto nel singolo caso, potrebbe anche essere risolto attraverso una delle restrizioni previste dal cpv. 3 (ad esempio, nel caso di interessi prevalenti). 20

L'esenzione generalizzata dall'obbligo di informazione per le persone soggette a un obbligo di segretezza è sorprendente anche perché, sebbene la riservatezza dei dati personali trattati sia garantita quando si applica un obbligo di segretezza previsto dalla legge, la necessità di informazioni tutelata dall'obbligo di informazione non viene automaticamente meno. Ad esempio, rimane aperto per quali scopi la persona con l'obbligo di riservatezza tratta i dati personali, ad esempio se il medico o l'avvocato effettua anche la profilazione e utilizza i dati raccolti per scopi di marketing. 21

Il DSGVO contiene un'eccezione analoga per il caso in cui i dati personali raccolti siano soggetti a segreto professionale. È allo stesso tempo più ampia e più ristretta dell'eccezione del DPA: l'eccezione del DPA non è limitata ai privati, ma si applica solo in caso di approvvigionamento indiretto. 22

E. Privilegio dei media (cpv. 1 lett. d)

23 Un'altra eccezione riguarda le attività di ricerca dei media in relazione alla pubblicazione di un lavoro giornalistico e alla protezione delle fonti. Alle stesse condizioni in cui le informazioni possono essere rifiutate, si può anche rinunciare alle informazioni: L'art. 20 cpv. 1 lett. d LPD fa riferimento all'art. 27 LPD. L'eccezione tutela la funzione di informazione e controllo dei media. Se le persone oggetto di ricerche investigative dovessero essere informate e le fonti di informazione dovessero essere divulgate, il lavoro giornalistico sarebbe reso impossibile e i media non potrebbero svolgere la funzione democratica che si prefiggono.

24 L'eccezione al cpv. 1 lett. d è disponibile solo nel caso di trattamento di dati personali in vista della pubblicazione nella sezione editoriale di un mezzo di comunicazione periodico (ad esempio un giornale o una rivista online). L'eccezione non può essere invocata per i cosiddetti "advertorial" e altre pubblicazioni a carattere prevalentemente pubblicitario, né può essere invocata per le attività di ricerca relative a un film documentario o a un altro supporto non periodico. Tuttavia, nel caso di tali attività di ricerca, è possibile invocare un altro motivo di eccezione o restrizione, ad esempio l'art. 20(3)(b) LPD (frustrazione dello scopo).

F. Impossibilità di ottenere informazioni (cpv. 2 lett. a)

25 Se i dati personali non sono ottenuti direttamente dall'interessato, cioè indirettamente, l'obbligo di informazione non si applica anche se non è possibile fornire le informazioni. Nei casi di acquisizione diretta, l'eccezione non è disponibile, il che è logico. Logicamente, non è possibile la raccolta diretta dei dati presso l'interessato, ma non è possibile la sua informazione.

26 L'impossibilità di effettuare l'informazione esiste, ad esempio, se l'interessato non può essere identificato in alcun modo. Nell'esempio della foto di uno sconosciuto menzionato nel dispaccio, ciò non può essere assunto senza ulteriori indugi alla luce delle odierne possibilità tecnologiche. L'eccezione ha poca rilevanza pratica per altri aspetti: Se non è possibile identificare la persona interessata, di solito i dati in questione non sono personalmente identificabili e la questione dell'obbligo di informazione non si pone nemmeno.

G. Sforzo sproporzionato (cpv. 2 lett. b)

Infine, l'obbligo di informazione non si applica se i dati personali sono ottenuti indirettamente e informare gli interessati richiederebbe uno sforzo sproporzionato. Anche in questo caso, l'eccezione non può essere invocata in caso di acquisizione diretta. Chiunque raccolga dati personali direttamente dall'interessato deve essere tenuto a informarlo della raccolta. 27

La misura in cui lo sforzo è ancora proporzionato deve essere determinata caso per caso e si basa sullo sforzo richiesto al responsabile del trattamento in relazione all'interesse informativo degli interessati. Il fattore decisivo non è l'interesse informativo specifico delle singole persone, ma un interesse informativo generalizzato. Quanto più sensibili sono i dati trattati, quanto più esteso è il trattamento, quanto più critiche sono le modalità del trattamento, quanto più critica è la finalità del trattamento e quanto più nuove sono le tecnologie utilizzate per il trattamento, tanto maggiore è la spesa che si può prevedere per il titolare del trattamento. 28

Il dispaccio cita il trattamento dei dati personali a fini di archiviazione come esempio di sforzo sproporzionato. Nel caso di un gran numero di persone, le informazioni sarebbero associate a un grande sforzo, mentre l'interesse per le informazioni delle persone interessate in questi casi sarebbe regolarmente limitato. L'analoga disposizione di esenzione del DSGVO cita come ulteriori esempi il trattamento a fini di ricerca scientifica o storica e a fini statistici. Le informazioni degli interessati possono anche essere sproporzionate se vengono utilizzate quantità molto elevate di dati per l'addestramento di modelli linguistici di grandi dimensioni e di modelli di IA simili, ad esempio se l'IA viene addestrata con "l'intera Internet". In pratica, è consigliabile documentare in ogni caso le considerazioni in base alle quali le informazioni dell'interessato non sono più considerate proporzionate. 29

I fatti del cpv. 2 lett. b sono concepiti come un'eccezione, ma una restrizione sarebbe stata più appropriata. Se l'informazione è sproporzionata, ad esempio a causa dell'elevato numero di persone interessate, l'omissione completa dell'informazione non sembra appropriata. Un rimedio più blando (e ovvio) in questi casi sarebbe quello di fornire una dichiarazione sulla privacy sul sito web della società interessata, rinunciando alla notifica individuale. 30

III. RESTRIZIONI

A. Generale

31 L'art. 20 LPD contiene nel cpv. 3 un totale di cinque costellazioni in cui le informazioni possono essere limitate, rinviate o sospese. A differenza delle eccezioni di cui ai cpv. 1 e 2, in questi casi l'obbligo di fornire informazioni non cessa completamente e le informazioni possono essere limitate solo nella misura richiesta dal motivo corrispondente nel singolo caso. Se il motivo della restrizione cessa di essere valido, le informazioni devono essere fornite successivamente. Come per le eccezioni, anche nel caso delle restrizioni ai sensi del cpv. 3 non è necessario informare l'interessato dell'applicazione e della portata della restrizione, e l'unico ricorso dell'interessato è quello di far valere il diritto all'informazione.

32 Le possibilità di limitare le informazioni si basano in gran parte su un bilanciamento di interessi, in cui la ragione specifica di una restrizione deve essere stabilita in relazione alla necessità di informazioni delle persone interessate. Al contrario, nel caso delle eccezioni, l'esistenza di una circostanza specifica (ad esempio, il fatto che l'interessato sia già in possesso delle informazioni) di solito determina se l'eccezione può essere utilizzata o meno.

B. Interessi prevalenti di terzi (cpv. 3 lett. a)

33 È possibile limitare le informazioni se ciò è necessario a causa di interessi prevalenti di terzi. Il termine "terzi" di cui al cpv. 3 lett. a non va inteso esclusivamente al plurale e per poter limitare le informazioni è sufficiente anche il prevalente interesse di un singolo terzo. Questa possibilità di restrizione esiste sia per i responsabili del trattamento dei dati privati che per gli organi federali.

34 La restrizione può essere utilizzata nei casi in cui i terzi abbiano interesse a non fornire informazioni all'interessato e tale interesse sia superiore al bisogno di informazioni dell'interessato. Ciò è particolarmente concepibile nelle costellazioni in cui l'interessato otterrebbe anche dettagli di terzi attraverso le informazioni e i suoi interessi alla riservatezza verrebbero così compromessi. In pratica, tuttavia, è probabile che tali costellazioni si

verifichino solo raramente, poiché le informazioni in quanto tali non rivelano di solito alcun dato personale.

C. Vanificazione dello scopo (cpv. 3 lett. b)

La limitazione delle informazioni per i responsabili del trattamento dei dati privati e gli organi federali è possibile anche se le informazioni vanificano lo scopo del trattamento dei dati. L'art. 20 cpv. 3 lett. b LPD lascia aperto il problema se sia sufficiente una semplice compromissione dello scopo del trattamento per limitare l'informazione o se questa debba essere completamente impedita. Secondo il messaggio, le disposizioni dell'art. 20 cpv. 3 LPD devono essere interpretate in modo restrittivo, per cui si deve presumere che l'impedimento debba essere completo. 35

Nel caso di più finalità perseguite con il trattamento dei dati, l'informazione alla persona interessata deve vanificare l'effettiva finalità principale, che, secondo il messaggio, deve essere anche di notevole importanza. La possibilità di limitare l'informazione è inoltre ulteriormente limitata dal fatto che gli interessi puramente economici non rientrano generalmente nel campo di applicazione della restrizione ai sensi del cpv. 3 lett. b. In pratica, quindi, saranno pochi i casi in cui le parti responsabili private potranno avvalersi di questa restrizione. Le possibilità di applicazione sono più ampie nel caso degli organi federali, soprattutto nell'ambito dell'azione penale, anche se in questo caso la possibilità di restrizione ai sensi del cpv. 3 lett. d n. 2 è probabilmente applicabile nella maggior parte dei casi. 36

Un esempio di applicazione della restrizione è rappresentato dalle attività di ricerca nell'ambito del giornalismo investigativo, che non rientrano nell'eccezione di cui all'art. 20 cpv. 1 lett. d LPD, ad esempio perché la ricerca viene effettuata per un documentario e non per un mezzo di comunicazione pubblicato periodicamente. La sospensione dell'informazione ai sensi del cpv. 3 lettera b può essere giustificata anche nel caso in cui i dati personali vengano elaborati nell'ambito della conservazione di prove per un processo successivo e l'informazione della persona interessata renderebbe impossibile la raccolta delle prove. Altrettanto ipotizzabile è il rinvio dell'informazione quando si conducono studi comportamentali in cui le persone interessate devono mostrare un comportamento il più naturale possibile e l'informazione prima dello svolgimento dello studio falsificherebbe i risultati. Anche nel caso di un'osservazione giustificata di una persona da parte di un investigatore 37

privato, il suo scopo sarebbe vanificato dal fornire informazioni alla persona osservata.

D. Interessi superiori della persona responsabile (cpv. 3 lett. c)

38 La possibilità di limitare le informazioni sulla base di interessi prevalenti del responsabile del trattamento è aperta solo ai responsabili del trattamento privati. Gli organi federali non possono fare riferimento a questa possibilità.

39 A differenza del cpv. 3 lett. b, in questo caso sono in gioco anche interessi economici come la promozione delle vendite o lo sviluppo del prodotto. Poiché la possibilità di restrizione è rivolta solo ai responsabili privati, in molti casi saranno proprio questi gli interessi economici in gioco. Tuttavia, l'effettiva restrizione delle informazioni deve essere preceduta da un bilanciamento tra gli interessi del responsabile del trattamento e le esigenze informative delle persone interessate. Si tratta di uno standard piuttosto aperto ed è quindi consigliabile che i responsabili del trattamento dei dati documentino perché i loro interessi prevalgono.

40 Un altro prerequisito per limitare le informazioni ai sensi del cpv. 3, lettera c), è che i dati non vengano divulgati a terzi. Ciò significa che i dati devono essere comunicati a soggetti responsabili indipendenti, ad esempio a partner di cooperazione o a reti pubblicitarie, ma anche alle autorità. Tuttavia, non sono dannose le comunicazioni agli incaricati del trattamento che eseguono il trattamento dei dati per conto del titolare del trattamento secondo le istruzioni impartite, nonché ai corresponsabili. Se si vogliono includere anche le comunicazioni agli incaricati del trattamento e ai corresponsabili, la LPD parla solitamente di "destinatari" anziché di "terzi".

41 Ai sensi del cpv. 4, anche la divulgazione di dati a società del gruppo è generalmente innocua, anche se il destinatario all'interno del gruppo è a sua volta un responsabile del trattamento. Nel caso di divulgazione di dati personali all'interno del proprio gruppo, ad esempio nell'area delle risorse umane, le condizioni per la possibilità di restrizione sono quindi ancora soddisfatte. Questo privilegio di gruppo non era originariamente previsto nel progetto di legge ed è stato aggiunto durante le consultazioni parlamentari. Di conseguenza, solo la divulgazione a persone responsabili distinte al di fuori del gruppo di appartenenza porterà all'esclusione della possibilità di restrizione di cui al cpv. 3 lett. c.

Cpv. 3 lettera c, offre un notevole margine di manovra per l'applicazione pratica di una restrizione delle informazioni, poiché per un gran numero di operazioni di trattamento dei dati è possibile far valere un interesse prevalente del titolare del trattamento. Di norma, si deve presumere che vi sia un interesse prevalente, ad esempio, nel caso di trattamenti di dati a bassa soglia, come le semplici misure di fidelizzazione dei clienti, in cui le circostanze e le modalità del trattamento dei dati sono ovvie e un'informazione completa non avrebbe quindi alcun valore aggiunto per gli interessati. 42

E. Interessi pubblici prevalenti (cpv. 3 lett. d n. 1)

Per gli organi federali è possibile limitare le informazioni se ciò è necessario per tutelare interessi pubblici prevalenti. Per i responsabili privati, non è possibile basare una restrizione delle informazioni sul cpv. 3 lett. d. 43

Ciò che deve essere inteso come interesse pubblico è definito in modo piuttosto ampio. La norma cita, a titolo di esempio, gli interessi alla sicurezza interna o esterna della Svizzera, che possono essere rilevanti in particolare nel contesto delle attività di intelligence. Tuttavia, gli interessi pubblici sono coinvolti anche se, ad esempio, sono in gioco il rispetto di obblighi di diritto internazionale, scopi diplomatici o il mantenimento di relazioni con l'estero. Un organo federale potrebbe quindi, ad esempio, limitare la fornitura di informazioni se la comunicazione alle persone interessate danneggiasse le relazioni di politica estera con un altro Paese. 44

Anche in questo caso, l'interesse pubblico deve "prevalere" ed è quindi necessario un bilanciamento degli interessi perché un organo federale possa avvalersi della possibilità di restrizione. Tuttavia, un bilanciamento tra la necessità di informazione delle (singole) persone interessate e gli interessi della sicurezza nazionale è spesso favorevole alla possibilità di restrizione. 45

F. Minaccia al procedimento (cpv. 3 lett. d n. 2)

Infine, il cpv. 3 lett. d n. 2 prevede la possibilità di restrizione se le informazioni mettono in pericolo un'indagine, un'inchiesta o un procedimento ufficiale o giudiziario. Anche questa possibilità è riservata agli organi federali e non può essere utilizzata dai privati incaricati. I responsabili 46

privati devono ricorrere a un'altra eccezione o ragione di restrizione in caso di minaccia al procedimento.

47 La possibilità ha una prossimità sostanziale con la restrizione delle informazioni se questa vanifica lo scopo effettivo del trattamento dei dati. A differenza di quanto previsto dal cpv. 3 lettera b in cui lo scopo deve essere effettivamente frustrato, una minaccia è sufficiente per l'opzione di restrizione di cui al cpv. 3 lettera d. Non è quindi necessario che il pericolo si concretizzi effettivamente; il rischio è sufficiente.

BIBLIOGRAFIA

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).

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 21 LPD

Un commentario di Liliane Obrecht / Anna Kuhn

CITAZIONE SUGGERITA

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

Breve citazione: OK-Obrecht/Kuhn, art. 21 LPD N. XXX.

Art. 21 Obbligo di informare sulle decisioni individuali automatizzate

[1] Il titolare del trattamento informa la persona interessata di ogni decisione basata esclusivamente su un trattamento di dati personali automatizzato che abbia per lei effetti giuridici o conseguenze significative (decisione individuale automatizzata).

[2] Il titolare del trattamento dà su richiesta alla persona interessata la possibilità di esprimere un parere. Se la persona interessata lo esige, la decisione individuale automatizzata va riesaminata da una persona fisica.

[3] I capoversi 1 e 2 non si applicano se:

a. la decisione individuale automatizzata è in relazione diretta con la conclusione o l'esecuzione di un contratto tra il titolare del trattamento e la persona interessata e la richiesta di quest'ultima è soddisfatta; o

b. la persona interessata ha dato il suo espresso consenso a che la decisione sia presa in maniera automatizzata.

[4] Se la decisione individuale automatizzata è presa da un organo federale, questi la designa come tale. Il capoverso 2 non si applica nei casi in cui in virtù dell'articolo 30 capoverso 2 della legge federale del 20 dicembre 1968[6] sulla procedura amministrativa (PA) o di un'altra legge federale l'organo federale non è tenuto a sentire la persona interessata prima di prendere la decisione.

STRUTTURA

In breve ... 287
I. Considerazioni generali ... 287
A. Panoramica e struttura ... 287
B. Finalità normativa ... 287
C. Genesi ... 288
II. Obbligo di informazione in caso di decisione individuale automatizzata (cpv. 1) ... 291
A. Contesto tecnico ... 292
1. Livelli di automazione ... 292
2. Sviluppo ... 294
B. Decisione individuale automatizzata ... 294
1. Automazione completa ... 294
2. Conseguenza giuridica o pregiudizio significativo ... 295
3. Ulteriori presupposti ... 297
4. Valutazione ... 297
C. Obbligo di informazione ... 298
1. Momento, contenuto e forma ... 298
2. Valutazione ... 300
III. Diritti dell'interessato (cpv. 2) ... 300
A. Diritto di esporre il proprio punto di vista ... 300
1. Privati ... 301
2. Stato ... 301
B. Diritto al controllo da parte di una persona fisica ... 302
IV. Eccezioni (comma 3) ... 303
V. Decisione individuale automatizzata da parte di un organo federale (cpv. 4) ... 303
A. Obbligo di contrassegnare ... 304
B. Inapplicabilità dell'art. 21 cpv. 2 LPD ... 305
C. Mancanza di un intento generale di ammissibilità ... 305
VI. Applicazione ... 306
VII. Riferimenti di diritto comparato ... 308
A. Normativa europea (art. 22 DSGVO) ... 308
B. Casistica ... 309
1. Sulla distinzione tra decisioni parzialmente e completamente automatizzate ... 309
a. Austria: algoritmo AMAS ... 309
b. Germania: il caso della Schufa ... 310
2. Sulla gravità del pregiudizio ai sensi dell'art. 21, cpv. 2, della LPD ... 312
a. Paesi Bassi: sistema SyRI ... 312
b. Tribunale distrettuale di Amsterdam: servizio di taxi Uber ... 312
c. Tribunale distrettuale di Amsterdam: app Ola ... 313
3. Implicazioni per l'ordinamento giuridico svizzero ... 313

VIII. Prospettive 314
Bibliografia 314
I materiali 321

IN BREVE

L'art. 21 della LPD prevede un obbligo di informazione in caso di decisioni individuali completamente automatizzate che comportino un pregiudizio significativo per l'interessato o che comportino conseguenze giuridiche per lo stesso. Inoltre, la disposizione riconosce all'interessato diversi diritti di tutela: il diritto di esprimere il proprio punto di vista e il diritto alla verifica da parte di un essere umano.

Inoltre, la norma obbliga gli organi federali a contrassegnare espressamente come tali le decisioni individuali interamente automatizzate. Una lacuna sostanziale della disposizione consiste nel fatto che essa non include nel proprio ambito di applicazione le decisioni parzialmente automatizzate.

I. CONSIDERAZIONI GENERALI

A. Panoramica e struttura

Con la revisione della legge sulla protezione dei dati, nel settembre 2023 è stato introdotto nel diritto svizzero il **concetto** di decisione individuale automatizzata. L'art. 21 LPD disciplina gli obblighi del responsabile del trattamento ai sensi dell'art. 5 lett. j LPD e i diritti dell'interessato in caso di decisione individuale automatizzata. Cpv. 1 definisce la decisione individuale automatizzata e stabilisce un obbligo di informazione al riguardo. Cpv. 2 enuncia i diritti dell'interessato, tra cui figurano il diritto di essere ascoltato e il diritto alla verifica della decisione da parte di una persona fisica. Il cpv. 3 prevede delle eccezioni ai cpv. 1 e 2. Il cpv. 4 stabilisce una disposizione speciale per gli organi federali. 1

La LPD è concretizzata dall'**OPDa**. Quest'ultimo non contiene finora ulteriori disposizioni relative alle decisioni individuali automatizzate. 2

B. Finalità normativa

Secondo il messaggio del Consiglio federale, l'art. 21 LPD mira ad allinearsi alle disposizioni vigenti **del diritto internazionale**. Dal punto di vista contenutistico, il Consiglio federale motiva la nuova disposizione con il fatto che le decisioni individuali automatizzate sono in costante aumento a seguito 3

degli sviluppi tecnologici. Non viene tuttavia effettuata un'analisi dettagliata dei rischi connessi alle decisioni individuali automatizzate né della conseguente necessità di regolamentazione.

4 Il messaggio cita tuttavia esempi di come possano essere prese decisioni **erronee** basate su dati falsi o incompleti. Ciò lascia supporre che uno dei motivi all'origine dell'introduzione del nuovo art. 21 LPD fosse proprio il timore di tali decisioni. Come potenziale obiettivo normativo si può quindi considerare la tutela della dignità umana, il cui scopo è, tra l'altro, quello di proteggere le persone dal semplice ridurle a oggetti di decisioni automatizzate. Un ulteriore possibile obiettivo normativo può essere individuato nella tutela contro la discriminazione da parte dello Stato: se una decisione individuale automatizzata si basa su processi di apprendimento automatico, essa non segue regole stabilite dall'uomo, ma apprende da grandi quantità di dati (i cosiddetti «dati di addestramento»), che possono riflettere svantaggi sociali, modelli ricorrenti o ruoli di genere obsoleti (il cosiddetto *data bias*). In questo modo, una decisione individuale automatizzata può riprodurre svantaggi e produrre un effetto discriminatorio. La nuova disposizione concede alle persone interessate la possibilità di esercitare un'influenza qualora siano oggetto di una decisione individuale automatizzata («diritto all'udienza umana»). Secondo il messaggio, ciò dovrebbe contrastare le decisioni errate e le loro conseguenze. Peraltro, il legislatore valuta implicitamente le decisioni umane come superiori, poiché a suo avviso le decisioni automatizzate errate possono essere evitate grazie all'intervento umano. Su questo presupposto si basa anche la disposizione relativa alle decisioni individuali automatizzate ai sensi della DSGVO (cfr. N. 69 e segg.), che il messaggio cita come ulteriore motivazione dell'art. 21 LPD.

C. Genesi

5 Il dibattito giuridico sulle decisioni individuali automatizzate ha preso slancio solo con l'introduzione esplicita dell'art. 21 LPD. Come si vedrà di seguito, tuttavia, il concetto risale già a diversi decenni fa. L'art. 21 LPD è quindi il risultato di uno sviluppo graduale che si basa su precedenti tentativi di riforma e su orientamenti internazionali.

6 **1981:** Nei materiali relativi alla direttiva sul trattamento dei dati personali nell'amministrazione federale del 16 marzo 1981 si faceva riferimento ai rischi che potevano derivare dalla creazione di profili della personalità e dal

processo decisionale automatizzato basato su di essi. Nel diritto svizzero, tuttavia, non fu introdotta una normativa esplicita in materia di decisioni individuali automatizzate.

2003: Nell'ambito della revisione parziale della LPD nel 2003, il Consiglio federale intendeva introdurre un obbligo esplicito di informazione in caso di decisioni individuali automatizzate. Il Parlamento, tuttavia, respinse tale proposta. 7

2017 – 2020: La versione dell'art. 21 LPD proposta dal Consiglio federale nel messaggio sulla revisione totale del 2017 è stata sostanzialmente ripresa dal Parlamento. Mentre la consultazione era stata ancora oggetto di controversie, la presente disposizione è rimasta in gran parte incontestata nel corso della procedura parlamentare. Come mostra la tabella di concordanza che segue, le modifiche apportate si sono limitate a precisazioni redazionali: 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.

Tabella 1: Tabella di concordanza relativa all'evoluzione dell'art. 21 LPD (elaborazione propria)

2018: Un nuovo impulso alla regolamentazione giuridica delle decisioni individuali automatizzate è stato dato nel quadro dell'attuazione della direttiva (UE) 2016/680, vincolante per la Svizzera, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nel settore della cooperazione giudiziaria e di polizia. A tal fine, nell'ambito della Legge sulla protezione dei dati di Schengen (LPD-Schengen; in vigore fino al 31 agosto 2023) è stata introdotta una disposizione relativa alle decisioni individuali automatizzate (art. 11 SDSG). Tale disposizione obbligava gli organi federali, nei settori contemplati, a informare le persone interessate in merito alle decisioni individuali automatizzate e garantiva loro i relativi diritti di partecipazione. Con l'entrata in vigore della legge sulla protezione dei dati riveduta, la SDSG è stata abrogata (art. 68 in combinato disposto con l'allegato 1 LPD). L'art. 21 LPD è subentrato, dal punto di vista del contenuto, all'art. 11 LPSD. 9

2019 – 2023: L'introduzione dell'art. 21 LPD serve inoltre ad adempiere agli obblighi internazionali della Svizzera. La Convenzione modernizzata sulla protezione dei dati del Consiglio d'Europa (Convenzione 108+, Convenzione del Consiglio d'Europa 108+), che la Svizzera ha firmato il 21 novembre 2019 e ratificato il 7 settembre 2023, obbliga espressamente gli Stati contraenti a garantire il diritto all'informazione e all'audizione in caso di decisioni individuali automatizzate (art. 8 cpv. 1 lett. e e art. 9 cpv. 1 lett. a Convenzione del Consiglio d'Europa 108+). Inoltre, con l'introduzione dell'art. 21 LPD, il legislatore ha perseguito l'obiettivo di creare un livello di protezione dei dati che, nei rapporti con l'Unione europea, continui ad essere considerato «adeguato» ai sensi dell'art. 45 della DSGVO. 10

II. OBBLIGO DI INFORMAZIONE IN CASO DI DECISIONE INDIVIDUALE AUTOMATIZZATA (CPV. 1)

La decisione individuale automatizzata è definita giuridicamente nell'art. 21, cpv. 1, della LPD. Per poter inquadrare il concetto (B.), occorre innanzitutto formulare alcune osservazioni sull'automazione e sul suo sviluppo tecnico (A.). Successivamente vengono precisati i presupposti giuridici fondamentali (C.). 11

A. Contesto tecnico

1. Livelli di automazione

12 Per automazione si intende il trasferimento di compiti dall'uomo alle macchine. Una decisione individuale automatizzata può presentare diversi livelli di automazione. In linea di massima, è possibile distinguere tra automazione parziale e automazione completa.

13 Il concetto di automazione parziale presenta diversi significati. Da un lato, può trattarsi di un **supporto decisionale**. In questo caso, il sistema automatizzato prepara la decisione (raccolta, compilazione o valutazione di informazioni; creazione di panoramiche). La decisione vera e propria, tuttavia, viene presa da una persona fisica responsabile.

- *Ad esempio, i sistemi parzialmente automatizzati possono essere utilizzati per formulare diagnosi mediche analizzando radiografie, tomografie computerizzate o risonanze magnetiche.*
- *I sistemi parzialmente automatizzati possono essere impiegati nella definizione delle condizioni contrattuali.*
- *L'automazione parziale può rivelarsi utile anche per estrarre dati rilevanti da grandi quantità di testo. Ad esempio, nell'amministrazione fiscale, un sistema di supporto decisionale può mettere a disposizione dell'autorità dati aggiuntivi non ricavabili direttamente dalla dichiarazione dei redditi del contribuente, oppure evidenziare le clausole contrattuali rilevanti in contratti di notevole lunghezza.*
- *Nei procedimenti penali, in particolare negli Stati Uniti, vengono utilizzati sistemi parzialmente automatizzati che calcolano la probabilità di recidiva dei criminali.*

14 D'altra parte, il sistema parzialmente automatizzato può fungere da **verifica decisionale**, venendo impiegato per controllare una decisione presa da una persona fisica.

15 La **piena automazione**, invece, significa che un sistema esegue autonomamente ogni singolo passo del processo decisionale. In senso stretto,

anche la programmazione e l'avvio del processo decisionale devono essere effettuati dal sistema stesso.

- *Nel settore privato, ad esempio, le decisioni relative alle richieste di credito possono essere prese in modo completamente automatizzato, verificando automaticamente la solvibilità e la disponibilità al pagamento della persona interessata. In questo contesto, la stipula dei contratti avviene in modo automatizzato.*
- *È inoltre ipotizzabile l'automazione del processo di reclutamento. Si pensi, ad esempio, alla preselezione completamente automatizzata delle candidature di potenziali lavoratori. In questo caso, è il sistema a decidere se invitare una persona fisica a un colloquio di lavoro.*
- *I sistemi completamente automatizzati possono assegnare ai futuri studenti un posto di studio e, di conseguenza, un istituto di istruzione superiore.*

16 Nel settore pubblico, la completa automazione si presta particolarmente alle **procedure di amministrazione di massa**, grazie ai processi standardizzati e alla disponibilità di grandi quantità di dati. Si tratta di quei settori della pubblica amministrazione in cui viene preso un gran numero di decisioni relative a fattispecie quasi identiche.

- *Ad esempio, data la disponibilità di grandi quantità di dati, la procedura di accertamento fiscale si presta ad essere essere svolta in modo parzialmente, ma anche completamente automatizzato.*
- *Nel settore delle assicurazioni sociali, la decisione relativa al diritto alla riduzione dei premi si rivela idonea alla completa automazione.*
- *Anche nella procedura di concessione delle licenze edilizie si sta valutando la possibilità di introdurre decisioni individuali completamente automatizzate.*

17 Il potenziale dei sistemi automatizzati è considerato particolarmente elevato nel prossimo futuro nell'amministrazione pubblica per i sistemi parzialmente automatizzati. In questo modo, i compiti esistenti dovrebbero essere svolti in modo più efficiente, preciso e quindi più sicuro dal punto di vista giuridico.

2. Sviluppo

18 Le origini della decisione individuale automatizzata risalgono ai cosiddetti **sistemi esperti**. Questi si basano su schemi strutturati «se-allora» (i cosiddetti sistemi basati su regole) e, in questo senso, non vanno oltre i processi decisionali cognitivi delle persone fisiche.

19 In particolare, l'avvento della **Big Data Analytics** – ovvero la possibilità di analizzare insiemi di dati molto grandi e non strutturati – e il conseguente sviluppo tecnico hanno permesso l'affermazione dei processi di apprendimento automatico (spesso definiti in modo un po' generico come «Intelligenza Artificiale» [IA]). Ciò comporta, in un certo senso, un cambiamento di prospettiva: al posto delle causalità – ad esempio nell'impiego di reti neurali artificiali – entrano in gioco correlazioni o probabilità. I set di dati non vengono più elaborati mediante schemi «se-allora», ma sono piuttosto i sistemi stessi a stabilire le proprie regole per giungere a un risultato. In questo contesto, spesso non è chiaro come i sistemi giungano a tale risultato. Nella letteratura non sempre viene distinta in modo univoco quando si tratta di una «semplice» automazione o di un «semplice» sistema automatizzato e quando invece vengono impiegati processi di apprendimento automatico.

B. Decisione individuale automatizzata

1. Automazione completa

20 Si ha una decisione individuale automatizzata ai sensi dell'art. 21 LPD quando una decisione si basa **esclusivamente su un trattamento automatizzato** e comporta una conseguenza giuridica per la persona interessata o la pregiudica in modo significativo (art. 21 cpv. 1 LPD) . È necessario che venga presa una decisione riguardante una determinata persona (decisione individuale) basata sul trattamento di dati personali. Dal punto di vista del diritto pubblico, una decisione individuale automatizzata può anche essere definita «decisione automatizzata».

21 È determinante che il trattamento avvenga «senza l'intervento di una persona fisica». Si tratta quindi di una **valutazione dei fatti slegata da una persona fisica**, nonché dell'adozione di una decisione, e quindi di una completa automazione ai sensi della distinzione operata nel presente commento (cfr. N.

15). Se la decisione non può più essere modificata, secondo il messaggio non osta alla completa automazione il fatto che essa venga comunicata alla persona interessata da una persona fisica. Diversi autori ritengono invece che si sia comunque in presenza di una decisione individuale automatizzata anche quando una persona fisica sia coinvolta nella programmazione. Se si segue questa opinione, una decisione individuale automatizzata ai sensi dell'art. 21 cpv. 1 LPD non deve necessariamente essere presa in modo del tutto indipendente dall'intervento umano.

2. Conseguenza giuridica o pregiudizio significativo

22 Una decisione individuale automatizzata presuppone inoltre che sia collegata a una **conseguenza giuridica** o che comporti un pregiudizio significativo per l'interessato. Secondo il messaggio del Consiglio federale, la decisione è collegata a una **conseguenza giuridica** se comporta conseguenze immediate e previste dalla legge per l'interessato. La decisione produce sempre un effetto giuridico quando incide sulla situazione giuridica della persona interessata – ovvero quando per quest'ultima costituisce, modifica o revoca un diritto. A differenza di quanto avviene in caso di pregiudizio (cfr. N. 24), non è richiesta una particolare rilevanza della conseguenza giuridica. Come esempio, il Consiglio federale cita la stipula e la risoluzione di contratti, che comportano in entrambi i casi una conseguenza giuridica per la persona interessata in qualità di parte contraente. In concreto, viene menzionata la stipula automatizzata di un contratto di assicurazione. In questo caso, la copertura assicurativa e l'obbligo di pagamento del premio dovrebbero essere considerati conseguenze giuridiche. Le fatture dei premi inviate periodicamente e in modo automatizzato sulla base del contratto di assicurazione non sono invece considerate, secondo il messaggio, una decisione individuale automatizzata, tanto più che l'emissione della fattura, in quanto conseguenza giuridica, deriva già dalla stipula del contratto. Non costituisce una conseguenza giuridica nel senso sopra indicato nemmeno il fatto qualora non si giunga alla conclusione di un contratto con una persona. La mancata conclusione del contratto può tuttavia essere intesa, in questo esempio, come una decisione individuale automatizzata e comportare un obbligo di informazione, qualora la persona interessata ne subisca un pregiudizio significativo (cfr. N. 24).

23 Nel contesto del diritto pubblico, sussiste sostanzialmente una conseguenza giuridica in caso di emanazione di **decisioni** ai sensi dell'art. 5 PA, nonché in caso di atti reali ai sensi dell'art. 25a PA. Come esempio, il messaggio cita le liquidazioni fiscali automatizzate.

24 Una decisione individuale automatizzata comporta inoltre un obbligo di informazione qualora la persona interessata ne sia **sostanzialmente lesa**. Ciò si presume quando la decisione ha un effetto negativo sugli interessi economici o personali della persona interessata. La situazione deve raggiungere un certo grado di gravità; un semplice fastidio non è sufficiente. Determinanti per il grado di gravità richiesto sono aspetti quali l'importanza del bene leso per la persona interessata, la durata dell'effetto della decisione o la possibilità di ricorrere ad alternative. Se la persona interessata subisca un pregiudizio significativo deve quindi essere determinato mediante una valutazione delle circostanze complessive nel singolo caso. Come possibile esempio, il messaggio cita l'assegnazione di prestazioni mediche o la mancata stipula di un contratto sulla base di una decisione individuale automatizzata.

25 Tra gli **esempi** di decisioni individuali automatizzate che comportano una conseguenza giuridica o un pregiudizio significativo per la persona interessata figurano inoltre:

- *la stipula o la mancata stipula di un contratto di leasing, comprese le relative modalità (ad es. tasso d'interesse, termine di pagamento), nella misura in cui tali elementi dipendano da una valutazione automatizzata della situazione finanziaria della persona interessata (conseguenza giuridica o pregiudizio significativo in caso di mancata stipula);*
- *il rifiuto da parte di un'assicurazione sanitaria di stipulare un contratto con l'interessato sulla base della valutazione automatizzata dei suoi dati sanitari (pregiudizio significativo);*
- *l'invio automatizzato di multe stradali sulla base di immagini del rispettivo proprietario del veicolo (conseguenza giuridica);*
- *il rifiuto automatizzato di una richiesta di credito online o di una candidatura online senza intervento umano (pregiudizio significativo);*
- *la definizione delle condizioni contrattuali, ad esempio per una determinazione personalizzata dei prezzi (conseguenza giuridica);*

Non si considera invece una decisione individuale automatizzata: 26

- *l'invio di pubblicità personalizzata, poiché manca la conseguenza giuridica o il necessario grado di gravità del pregiudizio.*

3. Ulteriori presupposti

Secondo il messaggio del Consiglio federale, non occorre basarsi esclusivamente sul criterio della «persona fisica», ma occorre considerare anche quello della **complessità del sistema** e della **particolare incidenza** sulla persona interessata. Si ha una decisione individuale automatizzata quando l'automazione presenta una certa complessità e comporta una conseguenza giuridica particolarmente lesiva per la persona interessata. Le semplici «decisioni del tipo "se-allora"» non sono da classificare come decisioni individuali automatizzate. 27

- *Come esempio, il Consiglio federale cita il prelievo di denaro presso un bancomat. Se il saldo del conto è sufficientemente elevato, il prelievo viene concesso.*

A parte questo esempio, il messaggio non specifica quale sia il livello di complessità richiesto per tali decisioni, che rimane quindi per il momento poco chiaro. Il Consiglio federale preciserà tuttavia, se necessario, in un'ordinanza quando si ha una decisione basata esclusivamente su un trattamento automatizzato. 28

Nel contesto statale, alcuni autori si concentrano sul margine di discrezionalità nel processo decisionale. Altre voci, invece, affermano esplicitamente che non si possa prendere una decisione individuale automatizzata fintantoché all'autorità sia concesso un margine di discrezionalità. Facendo riferimento al criterio della complessità, Braun Binder sostiene che la complessità richiesta possa essere determinata mediante un ragionamento a contrario: non costituiscono decisioni individuali automatizzate quelle che non richiedono alcuna accertamento dei fatti. 29

4. Valutazione

Né dal testo di legge né dal messaggio è possibile dedurre con esattezza quando si sia in presenza di una decisione individuale automatizzata. Il criterio di riferimento della «complessità» del sistema è di scarso aiuto. Ciò 30

potrebbe dare l'impressione che la norma sia applicabile solo a procedure decisionali completamente automatizzate, basate su processi di apprendimento automatico (o appunto «IA») , mentre qualsiasi procedura basata su schemi «se-allora» ne resterebbe esclusa. Ciò difficilmente può valere, in particolare, per la pubblica amministrazione, poiché la maggior parte degli algoritmi da essa utilizzati si basa su schemi «se-allora». La normativa in materia di protezione dei dati risulterebbe quindi priva di qualsiasi contenuto. Per evitare che l'art. 21 LPD rimanga lettera morta, devono essere inclusi anche gli schemi «se-allora» basati su regole. L'ostacolo rappresentato dal requisito della complessità non dovrebbe quindi risultare eccessivamente elevato nella pratica.

31 È inoltre deplorevole che le decisioni basate su un'automazione parziale – nella loro forma di supporto o verifica decisionale (cfr. N. 13 e segg.) – non rientrino nella nozione di decisione individuale automatizzata ai sensi dell'art. 21 cpv. 1 LPD. L'applicabilità della disposizione sarà ostacolata in molti casi nella pratica. Ciò è tanto più discutibile in quanto, sia nell'automazione parziale che in quella totale, sorgono questioni rilevanti per la personalità e i diritti fondamentali (ad esempio in materia di discriminazioni, cfr. N. 4). Ciò vale a maggior ragione quando la semi-automazione si basa su complessi metodi di apprendimento automatico.

C. Obbligo di informazione

32 L'art. 21 cpv. 1 LPD stabilisce che il responsabile del trattamento deve informare l'interessato in merito a una decisione individuale automatizzata. Considerata la definizione di decisione individuale automatizzata (cfr. N. 20 segg.), l'obbligo di informazione sussiste quindi solo se la decisione comporta una conseguenza giuridica o un pregiudizio significativo per l'interessato (cfr. N. 22 segg.) .

1. Momento, contenuto e forma

33 Né nella legge né nel messaggio si trovano indicazioni dettagliate riguardo al momento, alla forma e al contenuto dell'obbligo di informazione in caso di decisione individuale automatizzata.

34 Per quanto riguarda il **momento**, il titolare del trattamento è libero di scegliere se informare l'interessato prima (*ex ante*) o dopo (*ex post*) che sia

stata presa la decisione individuale automatizzata. Anche se vi fossero validi motivi a favore di un'informazione preventiva – come ad esempio la possibilità di sottrarsi a una decisione individuale automatizzata senza dover ricorrere alle vie legali –, e sarebbe opportuna una corrispondente precisazione normativa, ciò non è previsto dal testo della norma. In questo senso, attualmente si ritiene che anche l'esercizio dei diritti degli interessati ai sensi dell'art. 21 cpv. 2 LPD (esposizione del proprio punto di vista e successiva verifica umana della decisione, cfr. N. 49 e segg.) sia sufficientemente garantito, in quanto uno degli obiettivi normativi dell'obbligo di informazione, mediante un'informazione *ex post*.

Per quanto riguarda la **forma**, ci si può rifare all'art. 13 dell'OPDa, che 35
prescrive una comunicazione in forma precisa, trasparente, comprensibile e facilmente accessibile. Tale disposizione si riferisce in linea di principio all'obbligo di informazione in occasione della raccolta di dati personali. Un'applicazione analogica all'art. 21 cpv. 1 della LPD è giustificata dal testo identico («informato») . Il titolare del trattamento può adempiere all'obbligo di informazione, ad esempio, pubblicando le informazioni in un'informativa sulla privacy facilmente reperibile sul proprio sito web o inserendo un link a tale informativa in un contratto. L'indicazione della decisione individuale automatizzata (cfr. N. 57 e segg.) è vincolante solo per gli organi federali e, *e contrario*, facoltativa per i privati.

L'obbligo di informazione è finalizzato alla trasparenza e all'obiettivo di 36
mettere a disposizione dell'interessato tutte le informazioni necessarie per far valere i propri diritti ai sensi dell'art. 21 cpv. 2 LPD. Per garantire ciò, è indispensabile che il responsabile fornisca informazioni sui seguenti punti:

- Informazione sul fatto che verrà presa o è stata presa una decisione individuale automatizzata (a seconda del momento in cui viene fornita l'informazione);
- l'indicazione chiara di quali decisioni o categorie di decisioni vengono prese in modo automatizzato (tenendo conto che sono comprese solo quelle che rientrano nell'art. 21 cpv. 1 LPD);
- la possibilità di esercitare il diritto di presentare le proprie osservazioni e di richiedere la revisione della decisione individuale automatizzata, nonché le indicazioni relative all'attuazione concreta di tali diritti (ad es. i recapiti del responsabile del trattamento).

37 Secondo l'interpretazione qui sostenuta, non è necessario informare **B in merito**B alla logica alla base della decisione individuale automatizzata. Per ottenere tali informazioni, l'interessato può piuttosto far valere il diritto di accesso. Di conseguenza, il responsabile del trattamento deve comunicargli esplicitamente l'esistenza della decisione individuale automatizzata nonché la logica alla base della stessa (cfr. art. 25 cpv. 2 lett. f LPD).

38 L'obbligo di informazione ai sensi dell'art. 21 cpv. 1 LPD deve essere adempiuto dal responsabile del trattamento sempre in aggiunta all'obbligo generale di informazione in sede di raccolta dei dati ai sensi dell'art. 19 LPD. È tuttavia possibile che le informazioni siano messe a disposizione nello stesso punto o nello stesso documento (cfr. in merito ai requisiti formali N. 35).

2. Valutazione

39 Anche l'obbligo di informazione richiede implicitamente che si tratti di una decisione individuale **completamente automatizzata**. Per la valutazione di questa circostanza da parte delle autrici, cfr. N. 31.

III. DIRITTI DELL'INTERESSATO (CPV. 2)

40 L'art. 21, cpv. 2, LPD conferisce all'interessato oggetto di una decisione individuale automatizzata diversi diritti. Essa può esporre il proprio punto di vista (A.) nonché far riesaminare la decisione da una persona fisica (B.). Ciò consente di sottolineare che l'informazione ai sensi del cpv. 1 deve consentire all'interessato di far valere i diritti sanciti dal cpv. 2.

A. Diritto di esporre il proprio punto di vista

41 L'interessato oggetto di una decisione individuale automatizzata deve avere la possibilità di esporre il proprio punto di vista. **Su richiesta**, da un lato deve poter esprimere il proprio punto di vista in merito all'esito della decisione individuale automatizzata. Dall'altro lato, deve poter ricevere informazioni sulle modalità di formazione della decisione individuale automatizzata. Le informazioni relative al processo di formazione della decisione individuale automatizzata devono in particolare impedire che il trattamento dei dati si basi su dati incompleti, inesatti o obsoleti.

1. Privati

I privati avranno interesse al diritto di presentare le proprie osservazioni in particolare quando la decisione individuale automatizzata risulta **erroneamente negativa** per l'interessato. Se, ad esempio, viene negata l'affidabilità creditizia del privato interessato, ciò può avere conseguenze negative anche per il titolare del trattamento privato, qualora a causa della decisione non si instauri alcun rapporto contrattuale tra le parti. 42

La legge non stabilisce il **momento** in cui devono essere presentate le osservazioni. Di conseguenza, ciò è possibile sia prima che dopo l'adozione della decisione. Dal punto di vista del titolare del trattamento privato ciò non comporta difficoltà, purché tale possibilità sussista in *qualsiasi* momento. 43

Il titolare del trattamento privato può applicare **costi** per la concessione del diritto di presentare le proprie osservazioni. Tuttavia, può essere nel suo interesse mantenerli bassi per non impedire la potenziale conclusione di un contratto. 44

2. Stato

Nel contesto statale, l'esposizione del proprio punto di vista ai sensi della normativa sulla protezione dei dati va intesa come conseguenza del **diritto di essere ascoltati** ai sensi dell'art. 29 cpv. 2 Cost. In quanto garanzia procedurale costituzionale fondamentale, il diritto di essere ascoltati deve essere concesso obbligatoriamente in ogni procedimento statale. 45

Secondo la giurisprudenza del Tribunale federale, la persona interessata da una decisione statale deve poter prendere posizione (per iscritto) sugli elementi rilevanti del caso **prima che** venga presa una decisione che incida sulla sua posizione giuridica. Secondo il messaggio relativo alla LPD, tuttavia, l'esposizione del proprio punto di vista può avvenire anche dopo l'emanazione della decisione, ad esempio mediante l'interposizione di un ricorso. Poiché il diritto di essere sentiti conferisce il diritto di esprimersi dinanzi all'autorità che ha emesso la decisione, è tuttavia ammissibile solo un ricorso non devolutivo – ad esempio un'opposizione con funzione di ricorso. L'obiettivo è ottenere una decisione sotto forma di decisione sull'opposizione da parte dell'autorità di primo grado. 46

47 Il **termine di opposizione** è disciplinato dalle leggi procedurali pertinenti. Esso è di norma di 30 giorni. Le basi giuridiche devono essere adeguate di conseguenza, qualora si intenda introdurre decisioni individuali automatizzate.

48 L'esposizione del proprio punto di vista nel procedimento amministrativo non deve comportare **costi (procedurali)** così elevati da indurre l'interessato a rinunciarvi. In linea di principio, è quindi consentito riscuotere costi per la presentazione della domanda. Alla luce del principio di legalità, tuttavia, ciò è ammesso solo se previsto dalla legge.

B. Diritto al controllo da parte di una persona fisica

49 L'art. 21 cpv. 2 LPD prevede inoltre il diritto dell'interessato al controllo umano della decisione individuale automatizzata. Ciò può risultare particolarmente importante qualora l'interessato sospetti di essere stato svantaggiato dalla decisione individuale automatizzata.

50 La verifica deve essere effettuata da una **persona fisica con potere decisionale**, affinché possa, se del caso, revocare la decisione. Tuttavia, essa è libera nelle proprie valutazioni e non è obbligata a revocare la decisione. L'unico requisito, secondo il presente parere, è che essa riesamini la decisione in buona fede.

51 Nella pratica, questo diritto al riesame a posteriori è ritenuto **non sufficiente**, in particolare in considerazione del potenziale di discriminazione. Si dovrebbe verificare in via preventiva se i sistemi decisionali automatizzati prendano decisioni involontariamente discriminatorie.

52 Né
la legge né il messaggio relativo alla LPD si pronunciano su un determinato **termine** entro il quale debba essere fatto valere il diritto al riesame da parte di una persona fisica. Per i privati non sarà possibile fissare un termine di validità generale, ma esso deriverà dalle circostanze del singolo caso. Gli organi federali possono orientarsi ai termini previsti per il riesame, poiché questi conferiscono un diritto analogo. La richiesta di riesame non è in linea di principio vincolata ad alcun termine, fatte salve le disposizioni di leggi speciali. In considerazione del principio di legalità e al fine di evitare l'arbitrarietà, appare tuttavia opportuno che un termine sia esplicitamente stabilito almeno a livello di ordinanza.

IV. ECCEZIONI (COMMA 3)

L'art. 21 cpv. 3 LPD prevede, per le decisioni individuali automatizzate, **due casi di eccezione** in cui non si applicano né l'obbligo di informazione né i diritti supplementari della persona interessata. Come giustamente osservano Vasella e Henseler, alla luce della chiara disposizione di legge e della posizione sistematica della norma, si deve presumere che le eccezioni all'obbligo di informazione previste dall'art. 20 LPD, previste per la raccolta di dati personali, non siano trasferibili all'obbligo di informazione relativo alle decisioni individuali automatizzate ai sensi dell'art. 21 cpv. 1 LPD. Tale distinzione è confermata anche dal testo dell'art. 20 cpv. 1 LPD. Anche se una decisione individuale automatizzata si basa su una base legale (cfr. art. 20 cpv. 1 lett. b LPD), il responsabile del trattamento non può invocare un'eccezione all'obbligo di informazione ai sensi dell'art. 21 cpv. 1 LPD. 53

La **prima eccezione** ai sensi dell'art. 21 cpv. 3 lett. a LPD si applica quando la decisione individuale automatizzata è direttamente connessa alla conclusione o all'esecuzione di un contratto tra il responsabile del trattamento e l'interessato e corrisponde pienamente alla sua richiesta. In tale contesto, il legislatore ha ritenuto che non sussista alcun interesse degno di tutela da parte dell'interessato a ricevere ulteriori informazioni o ad esercitare ulteriori diritti. 54

Come **secondo caso di eccezione**, l'art. 21 cpv. 3 lett. b LPD menziona il consenso esplicito dell'interessato alla decisione individuale automatizzata. I materiali non contengono informazioni dettagliate sui requisiti che il consenso deve soddisfare. Secondo l'intenzione del legislatore, un consenso valido presuppone almeno un'informazione preventiva e adeguata. Diversi autori della dottrina ritengono tuttavia che i requisiti generali per il consenso al trattamento dei dati siano adeguati anche nel contesto delle decisioni individuali automatizzate. 55

V. DECISIONE INDIVIDUALE AUTOMATIZZATA DA PARTE DI UN ORGANO FEDERALE (CPV. 4)

Infine, l'art. 21 cpv. 4 LPD contiene una disposizione speciale per gli organi federali ai sensi dell'art. 5 lett. i LPD. La disposizione impone a questi ultimi l'obbligo di contrassegnare le decisioni individuali automatizzate (A.). Inoltre, in determinati casi è prevista la non applicabilità dell'art. 21 cpv. 2 LPD (B.). La 56

disposizione non consente tuttavia agli organi federali, a causa della scarsa densità normativa, di adottare decisioni individuali automatizzate (C.).

A. Obbligo di contrassegnare

57 L'obbligo di contrassegnare le decisioni adottate in modo automatizzato ha lo scopo di rendere riconoscibile all'interessato che la **decisione non è stata presa da una persona fisica**. Contro le decisioni l'interessato ha in linea di principio la possibilità di presentare ricorso. Il contrassegno gli consente di di far valere, nel procedimento di ricorso, il proprio diritto di essere sentita (art. 29 cpv. 2 Cost.), esponendo il proprio punto di vista e facendo sì che la decisione venga riesaminata da una persona fisica.

58 È discutibile come l'obbligo di contrassegno si concili con l'obbligo di informazione ai sensi dell'art. 21 cpv. 1 LPD. Quest'ultimo, infatti, a differenza dell'obbligo di informazione in caso di raccolta di dati personali ai sensi dell'art. 19 cpv. 1 LPD, non viene meno se il trattamento è previsto dalla legge (art. 20 cpv. 1 lett. b LPD). Considerando che in futuro le decisioni automatizzate individuali nell'amministrazione saranno introdotte in particolare nei procedimenti di massa (cfr. N. 16), ci si chiede in che modo il responsabile statale debba adempiere all'obbligo di informazione (nel singolo caso). L'indicazione, invece, appare più mirata alla luce dell'economia processuale.

59 L'indicazione deve figurare in modo evidente e facilmente riconoscibile sulla decisione automatizzata. Secondo l'opinione qui sostenuta, si ritiene opportuno inserire l'avviso dopo il contenuto effettivo del provvedimento, ma prima delle indicazioni sui mezzi di ricorso. In questo modo l'interessato viene a sapere innanzitutto che la decisione è stata adottata in modo automatizzato, prima di essere informato sulle sue possibilità di tutela giuridica. Ciò corrisponde a un ordine di lettura naturale. Se l'indicazione fosse riportata dopo le indicazioni sui mezzi di ricorso, sussisterebbe il rischio che l'interessato prendesse atto di tale informazione troppo tardi o non ne prendesse affatto atto, prendendo così una decisione non informata in merito alla tutela giuridica.

B. Inapplicabilità dell'art. 21 cpv. 2 LPD

I diritti dell'interessato ai sensi dell'art. 21 cpv. 2 LPD, ovvero di esporre il proprio punto di vista e di far verificare la decisione individuale automatizzata da una persona fisica, si applicano in linea di principio anche alle decisioni individuali automatizzate adottate da organi federali. Ai sensi dell'art. 21 cpv. 4 LPD tali diritti vengono tuttavia meno se, ai sensi dell'art. 30 cpv. 2 PA o di un'altra legge federale, l'interessato non deve essere sentito. 60

L'art. 30 PA concretizza il diritto di essere sentiti ai sensi dell'art. 29 cpv. 2 PA. Ai sensi del cpv. 1, le parti devono in linea di principio essere ascoltate prima dell'emanazione di una decisione. Tale diritto è limitato dal comma 2. Si hanno eccezioni al diritto di essere ascoltati, ad esempio, quando una decisione è impugnabile mediante opposizione (art. 30 cpv. 2 lett. b PA) o quando le autorità accolgono integralmente le richieste delle parti (art. 30 cpv. 2 lett. c PA) . Ciò ha lo scopo di evitare duplicazioni nel processo decisionale e di non compromettere la sostanza del diritto di essere ascoltati. Nel procedimento di opposizione è possibile far valere a posteriori il diritto di essere ascoltati. In caso di piena accoglimento delle richieste delle parti, tale interesse viene invece meno. 61

In definitiva, la deroga prevista dalla normativa sulla protezione dei dati comporta che la LPD non riconosca alle persone interessate da una decisione individuale automatizzata dello Stato diritti più ampi di quelli già previsti dalla PA: se le parti devono comunque essere ascoltate ai sensi dell'art. 30 cpv. 1 PA, esse godono anche dei diritti – non più ampi – ai sensi dell'art. 21 cpv. 2 della LPD. Se è applicabile un'eccezione ai sensi dell'art. 30 cpv. 2 della PA e la parte non deve essere ascoltata, essa non può nemmeno fare valere il diritto di essere ascoltata ai sensi dell'art. 21 cpv. 2 della LPD. I diritti di cui all'art. 21 cpv. 2 LPD, in relazione alle decisioni automatizzate di diritto federale, sono **di natura dichiarativa** e, in alcuni casi, hanno addirittura creato maggiore incertezza giuridica per la persona interessata. 62

C. Mancanza di un intento generale di ammissibilità

Nella dottrina giuridica si solleva la questione se il legislatore, con l'introduzione dell'art. 21 cpv. 1 della LPD, intendesse introdurre in Svizzera una norma generale di ammissibilità per le decisioni individuali automatizzate. Secondo il Consiglio federale, le decisioni individuali 63

automatizzate dello Stato costituiscono «decisioni ordinarie» ai sensi dell' art. 5 PA, emanate senza intervento umano. A differenza della normativa europea, che con l'art. 22 cpv. 1 DSGVO stabilisce un divieto di principio dell'automazione con riserva di autorizzazione e prevede quindi una generale inammissibilità (cfr. N. 69 segg.), il diritto svizzero sembra così presupporre un'ammissibilità di tali decisioni sostanzialmente senza condizioni. Il rinvio generico all'art. 21 LPD dà l'impressione che la LPD funga da norma generale di ammissibilità per l'adozione di decisioni individuali automatizzate nel procedimento amministrativo svizzero. Tale intenzione, tuttavia, non può essere dedotta né dal messaggio relativo alla LPD né è compatibile con il principio di legalità (art. 5 cpv. 1 Cost.). Quest'ultimo richiede, oltre a una base legale formale (art. 164 cpv. 1 Cost.), anche una sufficiente determinatezza della norma. Sebbene la LPD sia una legge formale, ma la sua determinatezza appare insufficiente per quanto riguarda le decisioni emanate in modo completamente automatizzato. Risulta inoltre discutibile il fatto che la disposizione non preveda ambiti di applicazione concreti, ma si limiti semplicemente a presupporre l'esistenza di decisioni individuali automatizzate.

64 A ciò si aggiunge il fatto che, nel corso della revisione totale della LPD nel 2020, altre leggi sono state integrate con il termine «decisione individuale automatizzata». La LPD funge quindi da punto di partenza per questi riferimenti incrociati nelle leggi (procedurali) pertinenti.

VI. APPLICAZIONE

65 La legge prevede innanzitutto sanzioni penali. I privati sono puniti con multe fino a CHF 250'000 se, tramite una decisione individuale automatizzata, forniscono informazioni false, incomplete o non forniscono alcuna informazione (cfr. art. 60 cpv. 1 lett. a LPD). La sanzione presuppone la presentazione di una denuncia entro i termini previsti e l'azione dolosa. La normativa sulle multe non si applica agli organi federali.

66 Inoltre, la LPD prevede **misure di vigilanza**. Le violazioni degli obblighi di cui all'art. 21 LPD possono essere segnalate all'IFPDT. In tal caso, l'IFPDT può obbligare il responsabile del trattamento a fornire le informazioni alla persona interessata e a concederle la possibilità di esporre il proprio punto di vista o di far verificare la decisione individuale automatizzata da una persona fisica (cfr.

art. 51 cpv. 3 lett. c LPD). Ciò vale in egual misura per i responsabili del trattamento del settore privato e di quello pubblico.

67 La LPD non contiene alcuna disposizione che stabilisca se e in che modo il responsabile del trattamento debba **correggere** una decisione individuale automatizzata errata. Per questo motivo, talvolta viene mossa l'accusa di non offrire una protezione sufficiente ed efficace dalle conseguenze delle decisioni individuali automatizzate. Nel caso specifico in cui la violazione dell'obbligo di informazione e di audizione violi i principi di trattamento di cui all'art. 6 LPD, si può ravvisare in ciò un trattamento illecito dei dati da parte dell'organo federale (art. 41 cpv. 1 LPD) o una violazione della personalità da parte dei responsabili privati (art. 30 LPD). Nel contesto delle decisioni individuali automatizzate, è ovvia la violazione del principio di finalità (art. 6 cpv. 3 LPD). Di conseguenza, la persona interessata ha la facoltà di esigere l'eliminazione delle conseguenze negative del trattamento illecito dei dati (cfr. art. 41 cpv. 1 lett. b LPD per gli organi federali e art. 32 cpv. 2 LPD per i privati).

68 Nell'ambito dell'applicazione del diritto nel contesto del diritto pubblico, **non è chiaro** quale sia il rapporto tra il suddetto diritto alla riparazione e i mezzi di ricorso previsti dal diritto procedurale amministrativo in caso di violazione del diritto di essere sentiti. Tale incertezza giuridica è dovuta al fatto che il diritto all'audizione o al riesame ai sensi dell'art. 21 cpv. 2 della LPD non conferisce diritti che vadano oltre il diritto di essere ascoltati già previsto dall'art. 30 cpv. 1 della PA. La problematica si accentua qualora l'operato delle autorità, in relazione all'emanazione di una decisione che violi gli obblighi di cui all'art. 21 della LPD, venisse qualificato come trattamento illecito dei dati (cfr. art. 41 cpv. 1 della LPD) . Ai sensi della LPD, in tale contesto l'interessato ha la possibilità di richiedere l'eliminazione delle conseguenze di un trattamento illecito (art. 41 cpv. 1 lett. b LPD). Ciò suggerisce che una decisione emanata in violazione del diritto di essere sentiti dovrebbe essere revocata in quanto conseguenza di un trattamento illecito dei dati. Ciò metterebbe in discussione la definitività delle decisioni, in particolare dopo la scadenza dei termini di ricorso.

VII. RIFERIMENTI DI DIRITTO COMPARATO

A. Normativa europea (art. 22 DSGVO)

69 La DSGVO contiene una disposizione paragonabile all'art. 21 LPD. Sotto il titolo «Decisioni automatizzate in singoli casi, compresa la profilazione», l'**art. 22 cpv. 1 DSGVO** riconosce all'interessato il diritto di non essere sottoposto a una decisione basata esclusivamente su un trattamento automatizzato – compresa la profilazione – che produca effetti giuridici nei suoi confronti o che la leda in modo analogo.

70 La differenza rispetto all'art. 21 della LPD risiede in particolare nell'**approccio normativo**. I pareri della dottrina giuridica sull'art. 22 della DSGVO non sono concordi sul fatto che la disposizione europea vieti in linea di principio le decisioni individuali automatizzate o che alle persone interessate venga concesso un diritto di opposizione. La Corte di giustizia dell'Unione europea (CGUE) dell'Aia parte – senza fornire una motivazione approfondita – da un divieto di principio delle decisioni individuali automatizzate. Al contrario, il testo dell'art. 21 cpv. 1 LPD ammette in linea di principio le decisioni automatizzate.

71 **L'art. 22, cpv. 2, della DSGVO** consente tuttavia, in via eccezionale – ed esaustiva –, le decisioni automatizzate individuali qualora la decisione sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento (lett. a), se è consentita in virtù di disposizioni legislative dell'Unione o degli Stati membri a cui è soggetto il titolare del trattamento e tali disposizioni prevedono misure adeguate a tutela dei diritti, delle libertà e degli interessi legittimi dell'interessato (lett. b) oppure se è effettuata con il consenso esplicito dell'interessato (lett. c). Nel complesso, la normativa svizzera risulta quindi meno restrittiva rispetto alla DSGVO.

72 Ai sensi dell'**art. 22 cpv. 3 della DSGVO**, nei casi di cui all'art. 22 cpv. 2 lett. a e c della DSGVO, il responsabile del trattamento adotta misure adeguate al fine di tutelare i diritti e le libertà nonché gli interessi legittimi dell'interessato, tra cui rientrano almeno il diritto di ottenere l'intervento di una persona da parte del titolare del trattamento, di esprimere il proprio punto di vista e di contestare la decisione. Ulteriori requisiti relativi alle decisioni automatizzate che determinano effetti individuali derivano da una serie di altre disposizioni

della DSGVO, quali gli obblighi di informazione e il diritto di accesso. Il diritto europeo va, sotto il profilo sostanziale, oltre l'art. 21 della LPD.

Infine, **l'art. 22 cpv. 4 della DSGVO**, a differenza della normativa della LPD, prevede limitazioni specifiche per i dati personali particolarmente sensibili (secondo la terminologia svizzera). 73

B. Casistica

La LPD introduce il concetto di decisione individuale automatizzata nel diritto svizzero. Finora in Svizzera non esiste giurisprudenza su questo tema. Sebbene la LPD (svizzera) e la DSGVO (europea) sanciscano principi diversi in merito all'impiego delle decisioni individuali automatizzate – la LPD parte dalla ammissibilità di principio di tali decisioni, mentre la DSGVO stabilisce una norma di divieto con riserva di autorizzazione (cfr. N. 69 e segg.) – e la prassi dell'UE non può quindi essere recepita senza riserve, essa fornisce tuttavia indicazioni per la Svizzera. 74

1. Sulla distinzione tra decisioni parzialmente e completamente automatizzate

L'art. 21 della LPD contiene esclusivamente disposizioni relative alle decisioni individuali completamente automatizzate (cfr. N. 20 e segg.). I primi esempi provenienti dall'ambito europeo dimostrano che la distinzione rispetto alle decisioni parzialmente automatizzate può risultare difficile. Di seguito vengono presentati due esempi selezionati su questo tema, che sono stati valutati dalla Corte di giustizia dell'Unione europea (CGUE). 75

a. Austria: algoritmo AMAS

In un primo esempio, l'utilizzo sperimentale del «Sistema automatizzato di assistenza alle opportunità sul mercato del lavoro» (AMAS) da parte del Servizio austriaco per il mercato del lavoro (AMS) ha portato a una sistematica discriminazione a sfavore delle donne e delle persone con disabilità. Il sistema selezionava (in modo automatizzato) le candidature relative a una determinata descrizione del posto di lavoro sulla base dei dati contenuti nei fascicoli di candidatura degli ultimi vent'anni. Poiché in passato gli uomini venivano assunti più frequentemente delle donne, queste ultime (così come le persone con disabilità) non venivano nemmeno invitate a un colloquio di lavoro. L'Autorità austriaca per la protezione dei dati è 76

intervenuta contro tale pratica. Nel dicembre 2020, il Tribunale amministrativo federale austriaco ha emesso una sentenza relativa all'AMAS. La questione principale non riguardava il divieto di discriminazione, bensì la base giuridica per l'utilizzo dell'AMAS. La risposta a questa domanda dipendeva in ultima analisi dal fatto che la procedura in questione fosse un processo completamente o parzialmente automatizzato, poiché questi sono soggetti a requisiti diversi.

77 Le parti hanno avanzato le seguenti argomentazioni divergenti:

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 Il tribunale austriaco ha seguito l'argomentazione del Servizio per il mercato del lavoro. La direttiva sarebbe concreta per quanto riguarda lo svolgimento della procedura e stabilirebbe che il valore calcolato in modo automatizzato debba essere discusso nel corso di un colloquio di consulenza con le persone in cerca di lavoro. Il tribunale ha quindi classificato la procedura come parzialmente automatizzata.

79 Per la giurisprudenza svizzera ciò può costituire un'indicazione del fatto che, ai fini della distinzione tra parzialmente e completa non debba essere determinante esclusivamente il coinvolgimento di una persona fisica nel processo. Occorre piuttosto considerare le circostanze complessive del singolo caso.

b. Germania: il caso della Schufa

80 La Schufa è un ente gestito dagli istituti di credito tedeschi e da altre imprese, presso il quale le controparti contrattuali possono richiedere informazioni sui potenziali mutuatari. Su richiesta, essa fornisce un punteggio o un valore che dovrebbe indicare in che misura la persona in questione adempia in modo affidabile ai propri obblighi di pagamento.

Dopo che alcune persone in Germania avevano intentato causa contro la Schufa, tra l'altro perché le loro registrazioni non erano state cancellate e non era stato loro concesso l'accesso ai propri dati, il Tribunale amministrativo di Wiesbaden ha sottoposto il caso alla Corte di giustizia dell'Unione europea (CGUE) affinché chiarisse se il sistema di scoring della Schufa costituisse una decisione basata su un trattamento automatizzato – compresa la profilazione – ai sensi dell'art. 22 della DSGVO. 81

Il 7 dicembre 2023 la Corte di giustizia dell'Unione europea ha stabilito che il punteggio della Schufa rientra nell'ambito di applicazione dell'articolo 22 della DSGVO relativo alle decisioni automatizzate. Ha ritenuto soddisfatte le seguenti tre condizioni, che ai sensi dell'articolo 22, cpv. 1, della DSGVO devono essere soddisfatte cumulativamente: 82

- *Decisione:* la Corte di giustizia dell'Unione europea ha considerato il scoring creditizio come base per il successivo rifiuto del credito (anch'esso) una decisione, tanto più che le decisioni possono includere anche misure e, di conseguenza, il termine deve essere inteso in senso ampio. Secondo la Corte, un'interpretazione più restrittiva comporta il rischio di eludere l'art. 22 della DSGVO, in quanto, ad esempio, il calcolo del punteggio di credito non sarebbe soggetto alle disposizioni relative al trattamento di categorie particolari di dati personali (art. 22, cpv. 4, della DSGVO).
- *Trattamento dei dati esclusivamente automatizzato:* tale presupposto è soddisfatto, tanto più che il trattamento dei dati da parte della Schufa costituisce una profilazione ai sensi dell'art. 4, n. 4 della DSGVO e il valore di probabilità è stato inoltre determinato in modo completamente automatizzato.
- *Effetto giuridico o pregiudizio significativo:* poiché la Schufa ha basato la propria decisione, e quindi il rifiuto del credito, in modo determinante sul valore di probabilità del punteggio di credito, sussiste un pregiudizio significativo per l'interessato.

La sentenza anticipa l'applicabilità dell'art. 22 della DSGVO al credit scoring effettuato dalla Schufa, che precede la decisione effettiva di non concedere il credito. La Corte di giustizia dell'Unione europea (CGUE) richiede tuttavia, in via restrittiva, che la decisione automatizzata di negare il credito si basi in modo determinante sul punteggio di credito come una sorta di decisione preliminare. Le conseguenze di questa sentenza sono di ampia portata, in 83

quanto le decisioni automatizzate ai sensi dell'art. 22, cpv. 1, della DSGVO sono, in linea di principio, considerate vietate. Un'eccezione si applica solo se la decisione, ai sensi del cpv. 2, in alternativa:

- è necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento (lett. a);
- è consentita in virtù di disposizioni di legge dell'Unione o degli Stati membri (lett. b);
- avviene con il consenso esplicito dell'interessato (lett. c).

2. Sulla gravità del pregiudizio ai sensi dell'art. 21, cpv. 2, della LPD

84 La questione della gravità del pregiudizio arrecato all'interessato dalla decisione automatizzata individuale può essere valutata solo alla luce delle circostanze del singolo caso. Tre casi provenienti dai Paesi Bassi illustrano quando un pregiudizio è grave o non lo è.

a. Paesi Bassi: sistema SyRI

85 Nel 2014 è stata approvata nei Paesi Bassi una legge per l'introduzione del sistema antifrode SyRI (Systeem Risico Indicatie). SyRI era uno strumento algoritmico per il rilevamento delle frodi, limitato ai quartieri con popolazione colpita dalla povertà o dalle minoranze nei Paesi Bassi, che elaborava profili di rischio di singoli individui al fine di individuare diverse forme di frode – ad esempio in ambito fiscale e delle prestazioni sociali. Nel 2020 un tribunale olandese ha ordinato la sospensione immediata del programma, in quanto questo violava la CEDU.

86 Sebbene il sistema non emettesse decisioni individuali automatizzate, il caso illustra chiaramente quando sussiste evidentemente un pregiudizio significativo. Infatti, secondo le considerazioni del giudice, già una semplice segnalazione di rischio ha un impatto significativo sulla vita privata della persona a cui si riferisce la segnalazione.

b. Tribunale distrettuale di Amsterdam: servizio di taxi Uber

87 È stata intentata un'azione legale contro il servizio di taxi Uber per violazione dell'art. 22 della DSGVO, dopo che Uber aveva disposto il blocco automatico degli account di autisti in caso di sospetto di attività fraudolente. Poiché questi ultimi potevano riattivare i propri account dopo una verifica, il

Tribunale distrettuale ha negato la violazione dell'art. 22 della DSGVO. Il blocco temporaneo degli account non comportava conseguenze significative, a lungo termine o permanenti, come richiesto dall'art. 22 della DSGVO. Inoltre, i dati raccolti erano dati oggettivi, quali la posizione e il traffico, acquisiti indipendentemente dal comportamento del conducente.

c. Tribunale distrettuale di Amsterdam: app Ola

88 L'app «Ola» aveva imposto ai propri utenti detrazioni dal credito di viaggio o multe sulla base dei dati raccolti dal sistema. Il Tribunale distrettuale ha riconosciuto l'esistenza di effetti significativi ai sensi dell'art. 22 della DSGVO. Con l'imposizione di sanzioni pecuniarie, le conseguenze per gli interessati sarebbero state immediate e definitive. Inoltre, sarebbero stati raccolti «dati sulle prestazioni» completi, relativi al comportamento generale e continuativo di una persona.

3. Implicazioni per l'ordinamento giuridico svizzero

89 La distinzione tra decisioni individuali completamente automatizzate ai sensi dell'art. 21 cpv. 1 LPD e decisioni parzialmente automatizzate potrebbe rivelarsi difficile nella pratica. Un punto di riferimento può essere costituito dal margine di discrezionalità umana nel singolo caso. Se questo è ampio, si deve presumere che si tratti di una decisione parzialmente automatizzata. Allo stesso modo, le direttive interne all'amministrazione, la formazione dei collaboratori e la possibilità per gli interessati di presentare le proprie argomentazioni possono costituire indizi della presenza di una decisione individuale parzialmente automatizzata. In entrambi i casi, l'art. 21 LPD non è applicabile. Se, invece, una decisione viene presa da terzi, può comunque trattarsi di una decisione individuale automatizzata ai sensi dell'art. 21 LPD.

90 Allo stesso modo, può risultare difficile tracciare una linea di demarcazione tra le decisioni che comportano un pregiudizio significativo e quelle che non lo comportano. I seguenti aspetti possono servire alla classificazione:

- *l'immediatezza dell'effetto della decisione sulla persona interessata;*
- *l'effetto temporaneo o definitivo della decisione;*
- *la potenziale influenza della decisione sul comportamento o sul processo decisionale della persona interessata;*

- *la questione della limitazione delle possibili fonti di reddito o di un'eventuale perdita finanziaria per la persona interessata.*

VIII. PROSPETTIVE

91 L'automazione dei processi e delle procedure decisionali sta avanzando rapidamente sia nel settore privato che in quello pubblico. Anche il Consiglio federale ritiene che in futuro le decisioni automatizzate saranno più frequenti. L'art. 21 LPD obbliga i responsabili del trattamento a informare gli interessati in merito alle decisioni individuali automatizzate e a garantire loro determinati diritti di tutela. Appare tuttavia critico il fatto che tali obblighi si applichino esclusivamente alle decisioni completamente automatizzate. Le decisioni parzialmente automatizzate (supporto o verifica decisionale) non rientrano nell'ambito di applicazione della norma. Ciò è problematico, poiché tali sistemi sono più diffusi nella pratica e – a seconda della complessità dell'algoritmo utilizzato – possono avere un'influenza considerevole sull'esito della decisione. Ciò crea lacune nella tutela, in particolare per quanto riguarda la trasparenza e la tutela dei diritti fondamentali. In questo contesto, è necessario estendere l'ambito di applicazione dell'art. 21 LPD alle decisioni parzialmente automatizzate. Questa questione è stata affrontata nel dibattito giuridico sull'uso dei sistemi automatizzati. Inoltre, la necessità di intervenire è stata presa in considerazione anche nel processo legislativo.

BIBLIOGRAFIA

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.

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 22 LPD

Un commentario di Rehana C. Harasgama / Dario Haux

CITAZIONE SUGGERITA

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

Breve citazione: OK-Harasgama/Haux, N. XXX zu Art. 22 DSG.

Art. 22 Valutazione d'impatto sulla protezione dei dati

[1] Il titolare del trattamento effettua previamente una valutazione d'impatto sulla protezione dei dati quando il trattamento dei dati personali può comportare un rischio elevato per la personalità o i diritti fondamentali della persona interessata. Se prevede più operazioni di trattamento simili può procedere a una valutazione d'impatto comune.

[2] Il rischio elevato, in particolare in caso di utilizzazione di nuove tecnologie, risulta dal tipo, dall'entità, dalle circostanze e dallo scopo del trattamento. Sussiste segnatamente nel caso di:

a. trattamento su grande scala di dati personali degni di particolare protezione;

b. sorveglianza sistematica di ampi spazi pubblici.

[3] La valutazione d'impatto sulla protezione dei dati contiene una descrizione del trattamento previsto, una valutazione dei rischi per la personalità o per i diritti fondamentali della persona interessata nonché i provvedimenti a loro tutela.

[4] Il titolare privato tenuto a effettuare il trattamento in virtù di un obbligo legale è esentato dall'obbligo di procedere a una valutazione d'impatto.

[5] Il titolare privato del trattamento può rinunciare a una valutazione d'impatto se si avvale di un sistema, un prodotto o un servizio che dispone di una certificazione secondo l'articolo 13 per l'impiego previsto o se rispetta un codice di condotta secondo l'articolo 11 che:

a. si basa su una valutazione d'impatto sulla protezione dei dati;

b. prevede misure a tutela della personalità e dei diritti fondamentali della persona interessata; e

c. è stato sottoposto all'IFPDT.

STRUTTURA

In breve 326
I. Generalità 326
A. Panoramica 326
B. Storia delle origini 327
C. Scopo della norma 329
II. Contenuto 331
A. Destinatari 331
B. Rischio elevato 332
C. Attuazione della DIA 335
1. Introduzione 335
2. Procedura 335
3. Esecuzione di una DIA congiunta 338
4. Organizzazione 338
D. Eccezioni 339
III. Violazione dell'obbligo di effettuare una DIA 340
IV. Sfide e rilevanza pratica 341
V. Confronto con il diritto dell'UE 342
Bibliografia 344
I Materiali 345

IN BREVE

L'art. 22 LPD disciplina i requisiti per l'esecuzione di una valutazione d'impatto sulla protezione dei dati (DPIA). L'articolo si basa sulle disposizioni dell'art. 35 septies del GDPR. DSGVO. Con l'aiuto dell'analisi dei rischi per la protezione dei dati, deve essere effettuata una valutazione di tali rischi prima di qualsiasi trattamento dei dati previsto che possa comportare rischi elevati per la personalità o i diritti fondamentali degli interessati. In questo modo, le misure appropriate per ridurre al minimo il rischio dovrebbero essere definite e adottate prima dell'inizio del trattamento dei dati. Secondo la legge, un rischio elevato sussiste in particolare nel caso di (i) trattamento esteso di dati che richiedono una protezione speciale (ad esempio, dati sanitari) o (ii) monitoraggio sistematico ed esteso di aree pubbliche (ad esempio, l'installazione di telecamere di sorveglianza in un parco). Tuttavia, l'elenco dei rischi elevati di cui all'art. 22 non è esaustivo. In genere, i rischi elevati derivano dall'uso di nuove tecnologie e processi, come i sistemi algoritmici ("intelligenza artificiale"), i sistemi DLT o l'analisi dei Big Data. Tuttavia, l'attività di trattamento prevista può essere classificata come ad alto rischio per la personalità o i diritti fondamentali degli interessati anche a causa di altri fattori, ad esempio perché sono coinvolti minori, vengono prese decisioni individuali automatizzate o i dati personali vengono trasmessi a una rete complessa di responsabili del trattamento. Tuttavia, la violazione dell'obbligo di cui all'art. 22 non è direttamente punibile.

I. GENERALITÀ

A. Panoramica

1 A differenza del GDPR, il DSGVO rivisto non prevede un obbligo generale di responsabilità. Tuttavia, è stato introdotto l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) per le operazioni di trattamento dei dati con rischi elevati, che costituisce di fatto un obbligo di responsabilità per determinate operazioni di trattamento dei dati. La DPIA non è sancita dalla legge solo a livello federale, ma anche in numerosi cantoni. A Zurigo, ad esempio, l'obbligo corrispondente si trova nel § 10 cpv. 1 IDG, in relazione al controllo preventivo (cfr. sulla procedura di consultazione preventiva a livello federale il commento all'art. 23).

Con la revisione, la DIA è ancorata alla Legge svizzera sulla protezione dei dati per tutti i responsabili del trattamento, sia per i responsabili privati che per gli organi federali. Per questo motivo, la formulazione della disposizione copre sia i rischi elevati per la personalità (per il trattamento dei dati da parte dei responsabili privati) sia i diritti fondamentali (per il trattamento dei dati da parte degli organi federali) degli interessati. La DIA serve a identificare e valutare i rischi potenziali di un trattamento di dati pianificato in una fase iniziale e a definire e attuare misure di riduzione del rischio. Queste misure devono essere adottate prima dell'inizio del trattamento dei dati previsto (si veda più avanti il paragrafo 8 e seguenti). L'applicazione dell'art. 22 è una conseguenza dell'approccio basato sul rischio della LPD, che è particolarmente evidente nell'attuazione degli artt. 22 e 23. 2

DIA viene attribuita un'importanza crescente. Ciò è giustificato soprattutto dalla crescente diffusione di sistemi algoritmici avanzati o di nuove tecnologie comparabili in tutti i settori della vita, come le tecnologie di distributed ledger o l'Internet degli oggetti. In molte delle suddette applicazioni sono coinvolti dati personali e non si può escludere che la personalità o i diritti fondamentali degli interessati siano esposti a rischi elevati quando si utilizzano queste tecnologie. In questi casi, è quindi necessaria una DPA. Il titolare del trattamento è incoraggiato ad analizzare in anticipo il trattamento dei dati previsto. Allo stesso tempo, va notato che alcuni processi sono difficilmente tracciabili, soprattutto nel caso di sistemi algoritmici, e il loro potenziale non può essere definito in modo definitivo (il cosiddetto problema della "scatola nera"). Di conseguenza, potrebbe non essere possibile definire e delimitare chiaramente i dati personali trattati e le finalità del trattamento nei singoli casi, soprattutto perché spesso nel trattamento dei dati sono coinvolti molti responsabili del trattamento e altre terze parti e le analisi dei big data alla base dei sistemi offrono un potenziale non ancora prevedibile. In questi casi, il DPAA può anche essere un'"impresa ambiziosa", ma la sua attuazione deve essere presa ancora più sul serio. Quanto meglio sarà fatto, tanto più sarà probabile che l'uso di queste tecnologie sia affidabile e trasparente. 3

B. Storia delle origini

Prima della revisione totale, la LPD svizzera non richiedeva esplicitamente ai responsabili del trattamento dei dati privati di effettuare una LPD. Tuttavia, gli organi federali erano già obbligati, ai sensi della vecchia LPD, a notificare al 4

responsabile interno della protezione dei dati o all'IFPDT i progetti che prevedevano il trattamento automatizzato di dati personali (art. 20 cpv. 2 LPD). Questa notifica era legata al fatto che le rispettive autorità federali dovevano elaborare un concetto di sicurezza delle informazioni e di protezione dei dati ("concetto ISDS") per il trattamento dei dati previsto. Secondo il messaggio, questa procedura è paragonabile al DSFA. Per i responsabili del trattamento dei dati privati, la DIA si basava in alcuni casi sull'art. 7 dell'aDSG. Inoltre, i principi del trattamento dei dati hanno sempre richiesto che si tenga conto delle conseguenze del trattamento dei dati. In passato, inoltre, l'IFPDT richiedeva agli incaricati del trattamento dei dati privati di presentare una DIA in determinati casi, soprattutto quando si trattava di un trattamento dei dati ad alto rischio. L'introduzione dell'obbligo di effettuare una DIA era dovuta, non da ultimo, ai requisiti a livello dell'UE ai sensi dell'art. 8bis del progetto di decreto 108 e dell'art. 27 septies della direttiva (UE) 2016/680. L'art. 35 septies del GDPR contiene disposizioni analoghe per i responsabili del trattamento dei dati privati. Il DSGVO contiene disposizioni analoghe per i responsabili del trattamento dei dati che rientrano nell'ambito di applicazione del DSGVO ma non obbligano direttamente la Svizzera nel contesto della legislazione.

5 A livello internazionale, lo strumento si basa su una lunga storia che risale agli anni Novanta. Durante questo periodo, le prime valutazioni d'impatto sulla privacy sono state sviluppate sia nella direttiva UE sulla protezione dei dati (art. 20, direttiva 95/46/CE), che è stata sostituita dal DSGVO, sia nel mondo anglosassone. Altri Stati membri dell'UE, come Francia e Germania, hanno emesso raccomandazioni corrispondenti basate sulla Direttiva 95/46/CE. Queste linee guida non vincolanti miravano a ridurre al minimo i possibili rischi fin dall'inizio o, se possibile, a escluderli, soprattutto perché un tale orientamento preventivo si è sempre dimostrato più semplice ed economico rispetto all'adattamento dei processi, ad esempio a posteriori, a un'indagine dell'autorità di vigilanza competente. Questi obiettivi dovrebbero essere raggiunti, tra l'altro, attraverso la descrizione dei "flussi di informazioni", l'inclusione e il dialogo con le "parti interessate" e la stesura di relazioni. Si possono citare come esempio anche i regolamenti della precedente legge federale sulla protezione dei dati (aBDSG) in Germania, che prevedevano una maggiore protezione per tipi speciali di dati nel § 3 cpv. 9 dell'aBDSG. Questi dati speciali erano, tra gli altri, quelli relativi alle opinioni politiche o alla salute. Prima di consentire il trattamento di questi dati da parte delle

organizzazioni, il responsabile della protezione dei dati doveva effettuare un cosiddetto "controllo preventivo" per garantire un trattamento adeguato (sezione 4d cpv. 5, aBDSG).

Il processo legislativo svizzero ha evidentemente recepito tutti questi sviluppi, prevedendo una LPD in tutte le versioni preliminari della LPD totalmente rivista. Nella bozza preliminare, l'art. 22 e l'associato art. 23 LPD sono stati riuniti in un articolo 16 VE-DSG. Tuttavia, l'art. 16 cpv. 3 LPD era formulato in modo più rigoroso rispetto alla disposizione attualmente in vigore. L'articolo prevedeva che ogni DIA dovesse comunicare all'FDPIC sia il risultato che le misure adottate. Nella LPD, la valutazione d'impatto è stata quindi suddivisa in due articoli e adattata alla struttura dell'art. 35 DSGVO. L'elenco delle operazioni di trattamento ad alto rischio, che richiedono pertanto una DIA, includeva nella bozza anche la profilazione (art. 20 cpv. 2 lett. b LPD). Nel testo finale della legge, tuttavia, questa procedura di trattamento è stata rimossa dall'elenco delle operazioni di trattamento dei dati ad alto rischio sulla base delle consultazioni parlamentari e in conformità con l'attuale sistema giuridico. Questo passo è da accogliere con favore, soprattutto perché in molti casi la profilazione non sarà classificata come particolarmente sensibile e una DIA non sarebbe quindi giustificata. 6

La DIA è ora standardizzata nell'articolo 22 della LPD ed è applicabile sia ai responsabili del trattamento dei dati privati che agli organi federali. La norma giuridica va quindi oltre l'obbligo precedentemente previsto per gli organi federali dall'art. 20 cpv. 2 della FADP e lo amplia. Nell'ambito della nuova norma introdotta con la revisione totale, mancano ulteriori disposizioni di attuazione - ad eccezione dell'art. 14 LPD sull'obbligo di conservazione dei dati per due anni - che potrebbero semplificare l'attuazione nella pratica. 7

C. Scopo della norma

Il rispetto dei requisiti dell'art. 22 serve a garantire che un trattamento dei dati pianificato non comporti una violazione della LPD. Il DPA ha lo scopo di sensibilizzare il titolare del trattamento al trattamento dei dati ad alto rischio, come l'uso di sistemi algoritmici ("intelligenza artificiale") o di big data analytics, l'uso di software di riconoscimento facciale, l'introduzione di una banca dati di pazienti o la profilazione ad alto rischio. Si tratta quindi di una "autovalutazione ai sensi della legge sulla protezione dei dati" nel caso di un trattamento dei dati particolarmente rischioso. L'art. 22 è una conseguenza 8

dei principi di protezione dei dati e del principio della protezione dei dati attraverso la tecnologia e le impostazioni predefinite favorevoli alla protezione dei dati (art. 7). L'obiettivo è identificare i rischi in una prima fase e valutarli analiticamente in una seconda fase. Il responsabile del trattamento deve formulare una prognosi sulle possibili conseguenze del trattamento dei dati previsto per gli interessati. Ciò che conta in questo caso è come e in che misura il trattamento dei dati previsto influirà sugli interessati. Infine, lo standard mira a sviluppare e implementare misure appropriate basate sui risultati dell'analisi effettuata al fine di (i) mitigare i rischi identificati del trattamento dei dati pianificato, (ii) trarne conclusioni a lungo termine e (iii) comportarsi complessivamente in modo conforme alla protezione dei dati. In caso di successo, la DPA offre anche la possibilità di dimostrare all'IFPDT la conformità alle disposizioni della legge sulla protezione dei dati e di risparmiare sui costi a lungo termine. In questo senso, l'art. 22 impone al titolare del trattamento di riflettere autonomamente ed esaminare i rischi derivanti dal trattamento dei dati previsto: il trattamento dei dati previsto è conforme alle disposizioni della legge sulla protezione dei dati? Vengono rispettati i principi generali di protezione dei dati? Il trattamento dei dati è proporzionato? La sicurezza dei dati è messa in pericolo dal trattamento previsto? Esistono altri rischi per la personalità o i diritti fondamentali delle persone interessate? Queste domande devono essere affrontate indipendentemente dal livello di rischio, per cui il legislatore si affida in larga misura a una "mentalità pratica". Ciò dovrebbe servire a ridurre i rischi associati al trattamento dei dati a un livello percepito come adeguato.

9 Gli obblighi di documentazione e conservazione di cui all'art. 14 DPA integrano l'obbligo di condurre una DIA per i trattamenti di dati ad alto rischio. Il titolare del trattamento è tenuto a documentare la DSFA effettuata e a conservarla per almeno due anni dopo la fine del trattamento dei dati. In questo modo, in caso di indagine da parte dell'IFPDT, il responsabile del trattamento è in grado di giustificare il trattamento dei dati ad alto rischio e di dimostrare come i rischi elevati sono stati contrastati. Questa disposizione dimostra il carattere della DIA come responsabilità supplementare sia nei confronti dell'IFPDT che degli interessati.

II. CONTENUTO

A. Destinatari

L'articolo 22 si rivolge in particolare a due soggetti: gli organi federali e i responsabili privati del trattamento dei dati, poiché riguarda sia la valutazione del rischio del trattamento dei dati in questione in relazione alla personalità e ai diritti fondamentali degli interessati. Gli organi federali avevano già un obbligo simile ai sensi dell'aDSG. I responsabili del trattamento dei dati privati, così come gli organi federali, sono interessati da questo obbligo se rientrano nell'ambito di applicazione della LPD ai sensi dell'articolo 3, paragrafo 1. Ciò significa che i responsabili del trattamento dei dati privati con sede in Italia sono tenuti a rispettare le disposizioni della LPD. Ciò significa che anche i responsabili del trattamento dei dati privati con sede all'estero sono soggetti a tale obbligo, a condizione che le loro attività di trattamento dei dati abbiano un impatto in Svizzera secondo il principio dell'impatto e che siano soddisfatti gli altri requisiti dell'art. 22 (cfr. il commento all'art. 3 per i dettagli sul principio dell'impatto). 10

Gli incaricati del trattamento contrattuali non sono giustamente coperti dall'obbligo di effettuare una DIA, soprattutto perché trattano i dati per conto di un responsabile del trattamento e il responsabile del trattamento decide fondamentalmente le finalità e i mezzi del trattamento dei dati. La valutazione del rischio non rientra quindi fondamentalmente nella loro sfera di competenza. Sebbene la LPD, a differenza dell'articolo 28, paragrafo 3, lettera f), del DSGVO, non preveda un obbligo di assistenza per gli incaricati del trattamento dei dati nei confronti dei responsabili del trattamento nell'esecuzione di una DIA, un obbligo di assistenza per gli incaricati del trattamento dei dati può anche essere nel loro interesse. In pratica, un obbligo corrispondente sarà spesso parte degli accordi contrattuali tra il responsabile del trattamento e l'incaricato del trattamento. Dai principi di protezione dei dati di cui all'art. 6, tuttavia, si può dedurre l'obbligo per gli incaricati del trattamento di garantire che il trattamento dei dati loro trasferito sia effettuato in conformità ai principi di protezione dei dati. In caso contrario, il titolare del trattamento deve essere informato che l'attività di trattamento dei dati deve essere adattata. Se necessario, si dovrebbe persino suggerire di effettuare una DPA. 11

B. Rischio elevato

12 Cpv. 2 prevede che la DIA debba essere effettuata in tutti i casi in cui si debba presumere un rischio elevato per la personalità o i diritti fondamentali dell'interessato. Di conseguenza, non è necessario effettuare una DIA per ogni operazione di trattamento dei dati. Ciò corrisponde all'approccio basato sul rischio della LPD, per cui in questo caso sono in primo piano i rischi per gli interessati e non quelli che si presentano per i responsabili del trattamento.

13 Il rischio elevato deriva dalla natura, dalla portata e dalle circostanze, nonché dalla finalità del trattamento dei dati. Questi criteri sono paragonabili ai rischi che devono essere presi in considerazione nella determinazione delle misure di sicurezza dei dati ai sensi dell'art. 1 cpv. 3 LPD. In questo senso, il rischio elevato è presente in particolare, ma non esclusivamente, quando vengono utilizzate nuove tecnologie. Quanto più estese e sensibili sono le azioni e gli archivi di dati, tanto più probabile è l'esistenza di un rischio elevato. Il trattamento dei dati previsto deve essere esaminato in relazione all'impatto sull'identità, l'autodeterminazione o la dignità della persona interessata. Non è necessario che il rischio elevato si manifesti effettivamente: Si tratta di identificare e valutare i rischi potenziali che potrebbero sorgere nel corso del trattamento dei dati.

14 In base alle lettere a e b, esiste un rischio elevato nel senso di una finzione se (i) i dati personali che richiedono una protezione speciale sono trattati in modo estensivo (ad esempio, quando le informazioni sul casellario giudiziario sono pubblicate in un registro pubblico, quando si utilizzano applicazioni sanitarie che valutano i dati e formulano diagnosi, o nelle sperimentazioni cliniche) o (ii) le aree pubbliche sono monitorate in modo estensivo e sistematico (ad esempio, il monitoraggio di un parco giochi o di un parco pubblico o il monitoraggio sistematico dell'uso di Internet da parte dei dipendenti). La legge non elenca altri trattamenti di dati per i quali è necessario effettuare una DPA. Al contrario, il DSGVO prevede, ad esempio, che le autorità di controllo pubblichino gli elenchi dei trattamenti di dati per i quali è obbligatoria una DIA.

15 Secondo la formulazione dell'articolo 22, paragrafo 2, né la profilazione ad alto rischio né il processo decisionale individuale automatizzato sono classificati come attività di trattamento dei dati che richiedono una DIA. A prima vista, ciò sembra sorprendente, soprattutto perché la profilazione ad

alto rischio comporta per definizione un rischio elevato per l'interessato e le decisioni individuali automatizzate comportano conseguenze giuridiche o altre conseguenze che riguardano in modo significativo l'interessato. In questo contesto, la profilazione ad alto rischio deve sempre essere oggetto di una DIA. Nel caso delle decisioni automatizzate, invece, la situazione è diversa e più complessa, soprattutto perché una DIA valuta il trattamento dei dati in sé, che non è necessariamente sensibile nel caso di queste decisioni individuali automatizzate. Ciò che è sensibile in questo caso è principalmente il risultato della decisione, che è disciplinato dall'art. 21. Una DIA deve comunque essere effettuata se il trattamento dei dati che porta alla decisione individuale automatizzata potrebbe di per sé comportare un rischio elevato per la personalità o i diritti fondamentali della persona interessata.

16 L'invio elenca ulteriori trattamenti di dati che potrebbero comportare un rischio elevato, in particolare in caso di trattamento di grandi quantità di dati, di trasferimento di dati a paesi terzi (in questo contesto, si fa riferimento alla cosiddetta valutazione d'impatto del trasferimento di dati; cfr. il commento all'art. 16 f.) o se un gran numero di persone può accedere ai dati. Nei singoli casi, tuttavia, occorre sempre verificare se esiste effettivamente un rischio elevato.

17 Né la LDA né la LPD contengono requisiti più precisi in merito alla determinazione del rischio elevato. Pertanto, occorre sempre verificare, sulla base dello specifico trattamento dei dati previsto, se è necessario effettuare una DIA. Le linee guida dell'UE, che forniscono nove criteri per il regolamento di cui all'art. 35 f. DPA, possono servire da guida. DSGVO, che forniscono nove criteri in base ai quali è possibile determinare un rischio elevato. Secondo le linee guida, non appena un'operazione di trattamento dei

dati pianificata soddisfa due di questi nove criteri, dovrebbe esserci l'obbligo di effettuare una DIA. I nove criteri sono i seguenti:

- Valutazione o classificazione di persone o aspetti della personalità con l'ausilio di dati;
- Processo decisionale automatizzato con effetti giuridici nei confronti di persone fisiche o effetti altrettanto significativi;
- Monitoraggio sistematico;
- Trattamento di dati riservati o altamente personali;
- Elaborazione di dati su larga scala;
- Corrispondenza o fusione di diverse serie di dati, a meno che non sia prevedibile;
- Trattamento dei dati di persone vulnerabili (ad esempio, bambini, dipendenti o pazienti);
- Uso o applicazione innovativa di nuove soluzioni tecnologiche o organizzative (ad esempio, intelligenza artificiale, big data analytics o tecnologie basate su blockchain), poiché spesso il loro rischio per la protezione dei dati non è ancora stato valutato con precisione; e
- casi in cui il trattamento dei dati impedisce agli interessati di esercitare un diritto, utilizzare un servizio o eseguire un contratto.

Sebbene le linee guida dell'UE non siano applicabili in Svizzera, possono essere utilizzate per condurre una DIA ai sensi della legge svizzera e dell'UE sulla protezione dei dati, a causa dei requisiti legali comparabili. Inoltre, non si può escludere che l'IFPDT pubblichi linee guida simili o applichi per analogia alla Svizzera gli elenchi delle operazioni di trattamento dei dati delle varie autorità di controllo dell'UE ai sensi dell'art. 35 (4) del DSGVO, che richiedono una DPA. Questa prassi garantirà una maggiore certezza giuridica per quanto riguarda la valutazione del rischio elevato.

C. Attuazione della DIA

1. Introduzione

L'articolo 22 specifica chiaramente in quali casi il responsabile del trattamento deve condurre una DSFA e cosa deve essere osservato nel condurla. Ciò include che la valutazione del rischio deve essere effettuata e documentata in modo strutturato. La documentazione deve anche essere sottoposta alla consultazione dell'IFPDT se, nonostante le misure attuate, il trattamento dei dati continua a comportare un rischio elevato per la personalità o i diritti fondamentali degli interessati (art. 23, par. 1; cfr. in dettaglio il commento all'art. 23). 18

2. Procedura

La DIA deve essere effettuata dal titolare del trattamento prima di avviare un'attività di trattamento dei dati nuova o aggiornata. Ciò serve a identificare in anticipo i rischi del trattamento dei dati previsto e ad attuare misure adeguate prima che si verifichino violazioni legali. La regola è: prima è, meglio è. Tuttavia, l'implementazione iniziale del DSFA non è sufficiente. Piuttosto, sono necessarie ulteriori prove nel corso del progetto, per verificare se le modifiche apportate al trattamento dei dati portino a una valutazione diversa e se quindi altre misure appaiano più appropriate o addirittura obsolete. 19

Per quanto riguarda il contenuto, il DSFA richiede tre fasi, definite nel cpv. 3. Si tratta, in primo luogo, della fase di preparazione, in cui il trattamento dei dati viene descritto nel modo più preciso possibile. In secondo luogo, nella fase di valutazione, si valutano i rischi e su questa base, in una terza fase, si adottano misure per affrontare o superare tali rischi. 20

Prima di eseguire queste tre fasi, tuttavia, i responsabili del trattamento dei dati privati devono verificare se sono legalmente obbligati a trattare i dati. Se esiste un obbligo legale di trattamento, sono esenti dall'obbligo di effettuare una DIA (art. 22 cpv. 4). Inoltre, l'autorità federale o il responsabile del trattamento privato deve innanzitutto effettuare una valutazione preliminare. Si tratta di una valutazione del rischio generale, piuttosto superficiale, per verificare se il trattamento dei dati previsto possa potenzialmente comportare un rischio elevato (cfr. sul rischio elevato N. 12 e segg.). In questo modo, è possibile chiarire in anticipo se sia necessaria una DIA. Se il responsabile del 21

trattamento giunge alla conclusione che il trattamento dei dati previsto non può comportare un rischio elevato, la DIA non è necessaria. Tuttavia, tale decisione deve essere documentata e conservata a fini probatori. Tuttavia, se il responsabile del trattamento conclude, sulla base di questa valutazione preliminare, che il trattamento dei dati in questione potrebbe comportare un rischio elevato, la DIA deve essere effettuata in linea di principio. Un'eccezione è prevista solo nei casi di cui all'art. 22(5).

22 La fase preparatoria comprende una descrizione dettagliata dell'attività di trattamento dei dati (prevista). La legge non specifica cosa debba includere questa descrizione, né quanto dettagliata debba essere. A seconda della complessità dell'attività di trattamento dei dati prevista, la DPA può essere più o meno lunga. Tuttavia, la descrizione deve almeno includere il tipo di dati trattati e le categorie di interessati, una spiegazione delle finalità perseguite, il periodo di conservazione, le operazioni di trattamento, i destinatari e il luogo di trattamento e conservazione. In caso contrario, non è possibile effettuare una valutazione completa del rischio. La descrizione deve indicare i motivi per cui i dati personali devono essere trattati e le modalità di trattamento. Nell'ambito di questa descrizione, devono essere affrontate le tecnologie e i sistemi sottostanti, nonché le basi giuridiche pertinenti, in modo da riconoscere e attuare tempestivamente l'eventuale necessità di un intervento legislativo.

23 Segue la fase di valutazione, durante la quale la necessità e la proporzionalità del trattamento dei dati vengono messe in relazione con i possibili rischi. Vengono valutate le conseguenze negative del trattamento dei dati per la personalità o i diritti fondamentali dell'interessato. I rischi elevati o gli effetti negativi del trattamento dei dati possono manifestarsi in modi diversi: Ad esempio, il trattamento dei dati può danneggiare la reputazione di una persona, oppure il trattamento di dati falsi può portare a prognosi o diagnosi errate in ambito medico. Sono anche ipotizzabili situazioni in cui una persona viene licenziata ingiustificatamente o si verifica una perdita di fiducia nelle autorità, nel responsabile privato o in amici e familiari. Inoltre, il trattamento dei dati può avere anche conseguenze finanziarie. Questi e altri rischi analoghi devono essere analizzati in base alla loro probabilità e gravità nella fase di valutazione.

24 Nella valutazione dei rischi, devono essere rispettati i principi della protezione dei dati, in particolare quelli della minimizzazione dei dati, della

protezione dei dati attraverso la tecnologia e delle impostazioni predefinite favorevoli alla protezione dei dati (cfr. n. 4). Anche l'autodeterminazione informativa dell'interessato è di particolare importanza, ma non gli interessi del responsabile del trattamento. Tuttavia, la ponderazione degli interessi in merito alle misure da adottare tra gli interessi dell'interessato (interesse alla protezione dei dati, interesse alla libertà di disporre dei propri dati) e del responsabile del trattamento (interesse al trattamento dei dati) può avvenire in una fase successiva. Sebbene i dati rilevanti per il DPA non debbano necessariamente essere "particolarmente sensibili", la "natura sensibile" dei dati deve essere presa in considerazione nel contesto del rispettivo DPA e delle misure da adottare. Di conseguenza, in questa fase si deve tenere conto sia del numero che della sensibilità dei dati. La fase di valutazione comprende la valutazione della gravità dei rischi e della probabilità che questi si verifichino. Anche se un rischio potenzialmente elevato deve essere identificato in questa fase, i rischi possono anche emergere solo dopo l'esecuzione del DSFA. In questo senso, le tre fasi citate non possono essere rigorosamente separate l'una dall'altra.

Dopo che la fase di valutazione ha stabilito se il trattamento dei dati comporta un rischio elevato per la personalità o i diritti fondamentali dell'interessato, nella terza fase vengono definite le misure per ridurre il rischio. In questa fase, il responsabile del trattamento non solo deve essere consapevole dei rischi esistenti, ma deve anche decidere come contrastarli. Le misure possono essere organizzative, tecniche, legali o contrattuali. Il responsabile del trattamento deve analizzare come l'attività di trattamento dei dati prevista possa essere adattata per ridurre il rischio elevato a un livello ragionevole. Tali misure possono essere, ad esempio, la restrizione delle categorie di dati, la limitazione dell'accesso ai dati, la crittografia dei dati, la modifica di un incaricato del trattamento coinvolto, la modifica del luogo di trattamento, l'inclusione di determinati obblighi nei contratti con terzi in relazione al trattamento dei dati, ecc. Tuttavia, le misure devono essere adatte a mitigare i rischi specificamente identificati e non possono essere applicate di default, cioè in generale a tutti i rischi delle attività di trattamento dei dati che richiedono una DPA. Esse devono essere definite caso per caso. 25

La LPD non specifica se la DIA debba essere effettuata una sola volta o su base regolare. Ciò dipende dall'attività di trattamento dei dati: Se si tratta di un'attività una tantum, è sufficiente una DIA effettuata una volta sola. Tuttavia, 26

se il trattamento dei dati viene effettuato per un periodo di tempo più lungo e sorgono rischi nuovi o più elevati a causa di circostanze mutate, la DIA deve essere ripetuta. In linea di principio, tuttavia, il DSFA dovrebbe essere ripetuto ogni tre anni circa. Resta da vedere se questa raccomandazione resisterà alla prova del tempo di fronte alle innovazioni tecnologiche in rapido progresso e sempre più complete, ma sembra piuttosto improbabile nella prospettiva attuale.

27 In termini di tempo, si deve tenere conto anche del periodo di conservazione. Ai sensi dell'art. 14 DPA, la documentazione richiesta per la DIA deve essere conservata per due anni. Il periodo inizia con la fine del trattamento dei dati.

3. Esecuzione di una DIA congiunta

28 Il responsabile del trattamento ha il diritto di condurre una DIA congiunta nel caso di diverse operazioni di trattamento dei dati comparabili. Tuttavia, ciò vale solo se i rischi e le contromisure sono simili. Questa possibilità serve a ridurre lo sforzo e i costi per il responsabile del trattamento. Tuttavia, non è certo che questo diritto porti effettivamente a una riduzione degli oneri per i responsabili del trattamento, a meno che una particolare piattaforma o applicazione di trattamento non venga utilizzata in diversi settori o progetti.

4. Organizzazione

29 L'esecuzione di un DSFA non è responsabilità di una sola persona, organo o dipartimento del responsabile del trattamento. Come qualsiasi altra analisi del rischio, si tratta di un processo in cui devono essere coinvolti diversi soggetti, organi e dipartimenti. All'interno di un'azienda, il DSFA coinvolge solitamente la direzione del progetto, il reparto IT e/o il Chief Information Security Officer, l'unità di protezione dei dati o il consulente per la protezione dei dati, il reparto legale, il reparto rischi e conformità e altre persone chiave. Ogni persona coinvolta è essenziale per alcune fasi del DSFA. Ad esempio, il project management è particolarmente importante per la fase di preparazione, perché può descrivere al meglio il trattamento dei dati (previsto). Il dipartimento legale e di protezione dei dati è responsabile della valutazione dei rischi in base alla protezione dei dati e alla legge applicabile. Altri dipartimenti sono particolarmente importanti nel determinare le misure di mitigazione del rischio. Anche gli incaricati del trattamento dei dati che saranno utilizzati nell'operazione di trattamento dei dati prevista dovrebbero

essere coinvolti nella DIA. Come per ogni progetto, è particolarmente importante che una persona, un ente o un dipartimento assuma la guida del DSFA e mantenga una visione d'insieme dell'intero processo. Questa leadership è solitamente fornita dal consulente per la protezione dei dati o dal responsabile del progetto a livello operativo. Gli incaricati del trattamento che vengono utilizzati nell'operazione di trattamento dei dati pianificata devono essere coinvolti nel DSFA.

Dal punto di vista del titolare del trattamento, è quindi opportuno definire un organismo o un dipartimento che abbia familiarità con i requisiti legali per un DSFA e che disponga delle competenze necessarie per condurre un DSFA. Di solito si tratta dell'ufficio o del dipartimento responsabile della protezione dei dati. A seconda dell'obiettivo o del modello aziendale delle parti responsabili, può essere utile creare un modello che includa le istruzioni per condurre un DSFA, da utilizzare nei singoli casi. In questo modo, si soddisfano i requisiti legali senza dimenticare alcuni aspetti. 30

D. Eccezioni

Oltre all'obbligo generale di condurre una DIA nei casi in cui il trattamento dei dati comporti un rischio elevato per gli interessati, i paragrafi 4 e 5 definiscono alcune eccezioni. 31

L'articolo 22 cpv. 4 prevede che i responsabili del trattamento dei dati privati possano essere esentati dall'obbligo di effettuare una DIA in singoli casi, a condizione che siano legalmente obbligati a trattare i dati. Nel processo legislativo, questa esenzione è stata giustificata dal fatto che i possibili rischi in questi casi sono già stati valutati e quindi non è più necessario condurre una DIA. Tuttavia, è stato giustamente sottolineato che l'eccezione riguarda esclusivamente la questione dell'ammissibilità del trattamento dei dati, non le modalità di trattamento dei dati. Il DSGVO è più rigoroso a questo proposito e richiede che l'analisi dei rischi effettuata nel contesto della legislazione si riferisca alla specifica attività di trattamento affinché l'eccezione sia applicabile (cfr. n. 40). Inoltre, devono essere presi in considerazione anche i casi in cui il trattamento dei dati non avviene esclusivamente per l'adempimento del rispettivo obbligo di legge. Gli obblighi legali di trattamento dei dati da parte di soggetti privati si trovano, ad esempio, nella Legge federale sulla lotta al riciclaggio di denaro e al finanziamento del terrorismo (art. 30 LRD) o nella divulgazione dei dati dei dipendenti da parte 32

di un datore di lavoro per adempiere agli obblighi di sicurezza sociale (art. 84 LAMal). È ovvio che le autorità federali non rientrano in questa esenzione: Esse possono trattare i dati solo sulla base di un fondamento giuridico.

33 L'art. 22 cpv. 5 prevede poi un'ulteriore eccezione. In base ad esso, i responsabili del trattamento dei dati privati possono esimersi dall'obbligo di predisporre la DIA se sono soddisfatte determinate condizioni relative alla certificazione di un'operazione di trattamento dei dati o al rispetto di codici di condotta approvati. Queste esenzioni non si applicano alle autorità federali. Da un lato, ciò avviene se il responsabile del trattamento utilizza un sistema, un prodotto o un servizio certificato per l'uso ai sensi dell'articolo 13 (si veda in dettaglio il commento all'articolo 13 LPD). D'altro canto, l'obbligo non si applica nel caso in cui il responsabile del trattamento si attenga a un codice di condotta ai sensi dell'art. 11, (i) che sia basato su una DPAA, (ii) che adotti misure specifiche per proteggere la personalità e i diritti fondamentali delle persone interessate e (iii) che sia stato sottoposto all'IFPDT. Attualmente in Svizzera non esistono codici di condotta di questo tipo. Tuttavia, tali codici sono ipotizzabili per i settori in cui gli operatori del settore lavorano a stretto contatto e sviluppano congiuntamente processi standardizzati, come ad esempio nelle banche e nelle compagnie assicurative, nelle aziende tecnologiche o dei media o nell'industria pubblicitaria. Nell'UE, lo sviluppo di codici di condotta o regolamenti analoghi è disciplinato dall'art. 40 del DSGVO, per cui è attualmente noto il Codice di condotta UE per il cloud, che funge da codice di condotta armonizzato per il settore del cloud all'interno dell'UE.

III. VIOLAZIONE DELL'OBBLIGO DI EFFETTUARE UNA DIA

34 Se un responsabile del trattamento non effettua una DSFA, sebbene esista un obbligo corrispondente ai sensi dell'art. 22, è necessario osservare l'art. 51 cpv. 3, lett. d. In base a questo articolo, l'IFPDT può ordinare al responsabile del trattamento di effettuare una DIA sotto pena di ammenda. Per contro, gli interessati non hanno il diritto di agire in giudizio per ottenere l'esecuzione di una DIA.

35 Se nel corso di un'indagine l'IFPDT stabilisce che un'operazione di trattamento dei dati comporta un rischio elevato, può ordinare che l'operazione di trattamento dei dati sia adattata, sospesa o interrotta del tutto fino all'esecuzione di una DIA (art. 51 cpv. 1 in combinato disposto con l'art. 49

f). Ciò può comportare notevoli ritardi per il responsabile del trattamento, che a sua volta comporta costi elevati e sforzi aggiuntivi per il responsabile del trattamento. Poiché i risultati di un'indagine possono anche essere pubblicati dall'IFPDT (art. 57 cpv. 2), vi sono anche notevoli rischi di reputazione per la persona responsabile.

La violazione dell'obbligo di condurre una DIA non è autonomamente soggetta a multa. Questa norma sembra avere senso alla luce del fatto che tale obbligo è principalmente un obbligo di diligenza (consistente in un obbligo di documentazione e di rendicontazione). Nell'UE, tuttavia, la questione è trattata in modo diverso (cfr. n. 40 e segg.). Tuttavia, si può presumere che i responsabili del trattamento dei dati rispetteranno comunque gli obblighi previsti dalla LPD. Da un lato, perché le autorità pubbliche dovevano già tenere conto di tale obbligo nell'ambito dell'aDSG. D'altro canto, anche i responsabili del trattamento dei dati privati, in particolare i gruppi aziendali, hanno effettuato DPA prima dell'entrata in vigore della DPA completamente rivista, ad esempio perché il trattamento dei dati in questione rientrava nella DPA o perché l'IFPDT lo aveva richiesto. 36

IV. SFIDE E RILEVANZA PRATICA

Con l'entrata in vigore dell'art. 22 rivisto, è evidente che i requisiti normativi per una LPD sono molto complessi. Ciò vale in particolare per l'attuazione da parte delle piccole e medie imprese (PMI), la cui importanza economica in Svizzera non va sottovalutata. Per loro, è probabile che l'esecuzione delle singole fasi previste dall'art. 22 si riveli impegnativa. Ciò vale in particolare per la fase preparatoria e per la fase delle misure (cfr. N. 18 e segg.), che richiedono molto tempo a causa della procedura analitica necessaria. Ciò può generare costi considerevoli nei singoli casi. Di conseguenza, si può presumere che la necessità di modelli, consulenza e assistenza da parte dell'IFPDT aumenterà notevolmente nel prossimo futuro. A questo proposito, l'obbligo delle autorità di vigilanza europee di pubblicare elenchi che definiscano quando una DFA è obbligatoria può essere visto come un passo in questa direzione (art. 35 cpv. 4 DSGVO; cfr. n. 43). 37

Con il crescente utilizzo di sistemi algoritmici e altre applicazioni (cfr. n. 2), anche la DPA diventerà più importante. I responsabili del trattamento devono valutare attentamente in ogni singolo caso quali rischi sembrano appropriati e se l'uso di tali sistemi è conveniente. Questo approccio analitico prima 38

dell'inizio effettivo del progetto non dovrebbe essere una novità, in particolare per le grandi aziende, soprattutto perché le corrispondenti valutazioni d'impatto sulla privacy sono già state effettuate prima della revisione totale (cfr. n. 4 s. e 35) e dovrebbero conoscere gli obblighi analoghi a livello UE attraverso il DSGVO.

39 Il DPA chiarisce inoltre che nell'ambito delle nuove tecnologie dirompenti, le varie aree del diritto si sovrappongono e si può osservare una crescente commistione tra le questioni legali e quelle relative alla tecnologia utilizzata. Un esempio di questo sviluppo è la discussione sulla legge sull'intelligenza artificiale ("AI Act"). Paragonabile alla DIA ai sensi dell'art. 22 LPD, l'ultimo testo discusso si basa su un approccio fortemente basato sul rischio, in base al quale viene operata una differenziazione tra rischio limitato, elevato e inaccettabile. Pertanto, soprattutto nel caso di applicazioni ad alto rischio, definite nell'Allegato III della Legge sull'AI, deve essere eseguita una procedura di valutazione della conformità ai sensi dell'Art. 43 della Legge sull'AI, che si basa, tra l'altro, sull'Allegato VI. Questi requisiti, come la DIA ai sensi della LPD, devono essere intesi come un processo preventivo e continuo che comprende sia aspetti legali che tecnici e, più in generale, serve a garantire la trasparenza e quindi la fiducia degli utenti.

V. CONFRONTO CON IL DIRITTO DELL'UE

40 In generale, l'attuazione del DSGVO ai sensi della LPD è paragonabile ai requisiti a livello UE del DSGVO. Allo stesso tempo, l'Art. 22 f. LPD sono meno severi dell'Art. 35 f. DSGVO. Nell'UE, ad esempio, la DPA deve essere effettuata anche se il trattamento dei dati può comportare un rischio elevato per i diritti e le libertà delle persone fisiche. A differenza dell'art. 22 del DPA, l'art. 35 cpv. 3 lett. a del DPA prevede esplicitamente una DPA anche per le decisioni individuali automatizzate.

41 Le lettere da a a d dell'art. 35 cpv. 7 regolano fasi comparabili a quelle dell'art. 22 LPD, che devono essere prese in considerazione quando si effettua una DIA. Pertanto, la fase preparatoria è paragonabile alla lettera a, la fase di valutazione alle lettere b e c e la fase di attuazione delle misure alla lettera d. Anche se in Svizzera si può presumere che una DIA possa essere effettuata nuovamente nel corso del trattamento dei dati a causa di circostanze mutate, l'art. 35 cpv. 11 DSGVO lo prevede esplicitamente in alcuni casi.

Mentre l'art. 35 cpv. 2 DSGVO prevede l'obbligo di consultare il responsabile della protezione dei dati, almeno se è stato nominato, l'art. 35 cpv. 9 DSGVO prevede addirittura che il responsabile del trattamento possa consultare gli interessati quando effettua la DIA. La LPD non contiene una disposizione di questo tipo. La consultazione del responsabile della protezione dei dati non ha alcuna influenza sul DSFA in termini di contenuto, soprattutto perché il ruolo del responsabile della protezione dei dati non è specificato. La consultazione degli interessati, invece, è finalizzata alla trasparenza da parte del responsabile del trattamento e all'autodeterminazione degli interessati. Queste consultazioni rafforzano il senso e lo scopo della LPD, dimostrando ancora una volta che i rischi da valutare sono quelli del trattamento dei dati per gli interessati e quindi non principalmente quelli per il responsabile del trattamento. 42

A differenza della Svizzera, l'art. 35 cpv. 4 DSGVO impone alle autorità di controllo di tenere un elenco delle operazioni di trattamento per le quali è necessario effettuare una DIA in ogni caso (i cosiddetti elenchi positivi). In sostanza, il legislatore europeo stabilisce un obbligo de facto di effettuare una DIA nei casi definiti dalle autorità di controllo. Inoltre, le autorità di controllo sono autorizzate a tenere facoltativamente elenchi di attività di trattamento dei dati per le quali non è richiesta una DIA (i cosiddetti elenchi negativi; art. 35 cpv. 5 DSGVO). Questi elenchi sono soggetti alla procedura di coerenza se includono "attività di trattamento connesse all'offerta di beni o servizi agli interessati o al monitoraggio del comportamento di tali interessati in diversi Stati membri o che potrebbero incidere in modo sostanziale sulla libera circolazione dei dati personali all'interno dell'Unione" (art. 35 cpv. 6 GDPR). La LPD non prevede l'obbligo di mantenere elenchi positivi o negativi, anche se ciò sarebbe utile per la certezza del diritto. 43

Mentre l'art. 22 cpv. 5 LPD afferma esplicitamente che non è necessario effettuare una DIA se viene rispettato un codice di condotta ai sensi dell'art. 11 LPD e vengono soddisfatti i requisiti aggiuntivi di cui al cpv. 5 ai sensi del DSGVO tali codici di condotta devono essere presi in considerazione nella DIA solo come parte della valutazione dell'impatto del trattamento dei dati in questione. Tuttavia, non esonerano il responsabile del trattamento dall'obbligo di condurre una DIA se questa è obbligatoria per legge. 44

Infine, analogamente all'art. 22 cpv. 4 del DPA, l'art. 35 cpv. 10 del DPA stabilisce che non è necessario effettuare una DIA se un'operazione di 45

trattamento dei dati si basa su una base legittima. Tuttavia, l'eccezione nel DSGVO è definita in modo più restrittivo: L'eccezione si applica solo se la DIA è stata effettuata nel contesto dell'emanazione della base giuridica e la base giuridica regola la specifica operazione o le specifiche operazioni di trattamento. L'importanza pratica è quindi probabilmente limitata. Inoltre, esiste un'eccezione ai sensi dell'art. 35(10) del DSGVO se il trattamento dei dati è effettuato per il soddisfacimento di interessi pubblici o nell'esercizio di pubblici poteri.

46 Il DSGVO prevede multe fino a 10 milioni di euro o fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente per le violazioni dell'obbligo di condurre una DPA (art. 83(4)(a) DSGVO). Questa multa è in contrasto con la LPD, che non prevede una multa per tale violazione (cfr. n. 35).

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 23 LPD

Un commentario di Rehana C. Harasgama / Dario Haux

CITAZIONE SUGGERITA

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

Breve citazione: OK-Harasgama/Haux, N. XXX zu Art. 23 DSG.

Art. 23 Consultazione dell'IFPDT

[1] Il titolare del trattamento chiede previamente il parere dell'IFPDT se dalla valutazione d'impatto sulla protezione dei dati emerge che, nonostante i provvedimenti previsti dal titolare, il trattamento previsto comporta un rischio elevato per la personalità o i diritti fondamentali della persona interessata.

[2] L'IFPDT comunica entro due mesi al titolare del trattamento le sue obiezioni contro il trattamento previsto. Il termine può essere prorogato di un mese se si tratta di un trattamento di dati complesso.

[3] Se ha obiezioni contro il trattamento previsto, l'IFPDT propone al titolare del trattamento provvedimenti appropriati.

[4] Il titolare privato del trattamento può rinunciare a consultare l'IFPDT se ha consultato il consulente per la protezione dei dati ai sensi dell'articolo 10.

STRUTTURA

In breve 350
I. Aspetti generali 350
A. Panoramica 350
B. Storia 350
C. Scopo della norma 351
II. Contenuto 352
A. Destinatari 352
B. Trattamento "pianificato 352
C. Consultazione 353
1. Introduzione 353
2. Informazioni da fornire 354
3. Procedura dell'IFPDT 355
4. Limite di tempo 357
D. Eccezioni 357
III. Violazione dell'obbligo di consultazione dell'IFPDT 358
IV. Sfide e rilevanza pratica 359
V. Confronto con il diritto dell'UE 360
Bibliografia 361
I Materiali 362

IN BREVE

L'art. 23 è il regolamento successivo all'art. 22. Se nel corso di una DIA il responsabile del trattamento stabilisce che esiste un rischio elevato per la personalità o i diritti fondamentali dell'interessato nonostante le misure di attenuazione del rischio adottate, è necessaria la consultazione dell'IFPDT. I requisiti, le scadenze e le conseguenze sono elencati e specificati. L'IFPD controlla il trattamento dei dati previsto in relazione alla conformità con la LPD. In caso di obiezioni al trattamento dei dati previsto, l'IFPDT emette un parere che contiene anche raccomandazioni sulle possibili misure da adottare. Il parere viene trasmesso al titolare del trattamento. L'IFPDT può anche esercitare i poteri di cui agli artt. 49 e 51 e segg. successivamente alla consultazione di cui all'art. 23. Tuttavia, la violazione dell'obbligo di cui all'art. 23 non è punibile.

I. ASPETTI GENERALI

A. Panoramica

1 L'art. 23 descrive i requisiti per la consultazione dell'IFPDT. Si tratta di una procedura strettamente correlata alla valutazione d'impatto sulla protezione dei dati (DIA) di cui all'art. 22. Se, nel corso di una valutazione d'impatto sulla protezione dei dati, il responsabile del trattamento stabilisce che, nonostante le misure adottate, sussiste ancora un rischio elevato per la personalità o i diritti fondamentali dell'interessato a seguito del trattamento dei dati previsto, è necessario consultare preventivamente l'IFPDT. In questo caso, l'IFPDT verifica la compatibilità del trattamento dei dati previsto con la legge sulla protezione dei dati e con i requisiti di sicurezza delle informazioni. Entro due o tre mesi, l'IFPDT informa il titolare del trattamento delle sue obiezioni con una dichiarazione. In tal modo, l'IFPDT è tenuto a proporre misure adeguate per contrastare i rischi individuati.

B. Storia

2 L'obbligo di effettuare una DIA e di consultare l'IFPD se il trattamento dei dati previsto comporta un rischio elevato per gli interessati nonostante le misure adottate non esisteva prima della revisione totale della LPD. L'obbligo non

esisteva nemmeno per le autorità federali, che dovevano effettuare una DPA ai sensi dell'art. 22 aDSG. Neanche la Convenzione europea sulla protezione dei dati (ETS 108+) richiede l'introduzione di questo obbligo. Tuttavia, l'obbligo era già previsto in alcune leggi cantonali sulla protezione dei dati, ad esempio nel Cantone di Zurigo all'art. 10 IDG o nel Cantone di Berna all'art. 17a KDSG.

Tuttavia, la possibilità o la necessità di consultazione si basa sui requisiti legali europei del 2008, in particolare sull'art. 20 della Direttiva 95/46/CE, secondo cui le operazioni di trattamento che comportano determinati rischi per le persone, in particolare per quanto riguarda i diritti e le libertà, devono essere esaminate preventivamente dal commissario per la protezione dei dati. Questa norma continua ad avere effetto oggi nell'art. 28 dell'attuale Direttiva 2016/680/UE, che ha dovuto essere attuata anche in Svizzera a causa dell'acquis di Schengen nel settore della prevenzione, indagine, accertamento o perseguimento transfrontaliero dei reati o dell'esecuzione delle sanzioni penali, nonché nell'art. 36 del DSGVO, che è stato attuato in modo analogo. 3

Il VE-DSG prevedeva all'art. 16 cpv. 3 del VE-DSG la notifica all'FDPIC dei risultati della DIA in ogni caso. In linea con l'attuale regolamento, l'IFPDT doveva notificare al responsabile del trattamento le sue obiezioni entro un certo periodo di tempo. L'obbligo di informare l'IFPDT dei risultati di una DIA in ogni caso è stato fortemente criticato nella consultazione pubblica. Il Consiglio federale ha quindi ammorbidito l'obbligo con l'articolo 21 cpv. 1 della LPD. Questa norma indebolita è stata adottata nell'attuale regolamento all'art. 23 cpv. 1, nel senso che l'IFPDT deve essere consultato solo se, nonostante le misure adottate, sussistono ancora rischi elevati per la personalità o i diritti fondamentali della persona interessata. 4

C. Scopo della norma

Secondo il messaggio, l'obbligo di consultazione è stato inserito nell'ambito della revisione totale del 2020 "perché consente al responsabile di agire in modo preventivo e consultivo". Questo è il modo più efficiente per il responsabile del trattamento, in quanto i potenziali problemi di protezione dei dati possono essere identificati e affrontati in una fase precoce. La consultazione consente all'IFPDT di ottenere e valutare le informazioni necessarie per valutare un'operazione di trattamento dei dati pianificata ad alto rischio. Ciò va anche a vantaggio del processo democratico. 5

6 Lo scopo dell'art. 23 è anche quello di sviluppare soluzioni prima dell'attuazione di un progetto che prevede tale trattamento di dati. Ciò serve a garantire un elevato standard di protezione dei dati e di sicurezza delle informazioni fin dall'inizio. Il legislatore mira quindi a un comportamento proattivo per ridurre al minimo le possibili violazioni legali fin dall'inizio o, idealmente, per escluderle del tutto. Inoltre, serve a proteggere il titolare del trattamento dei dati a posteriori - quando il trattamento dei dati è già iniziato - da sforzi e costi aggiuntivi. Ciò sembra avere senso anche alla luce del fatto che i danni e le violazioni successive sono spesso difficili da rimediare. Nel complesso, l'articolo si inserisce quindi nell'approccio basato sul rischio della LPD completamente rivista.

II. CONTENUTO

A. Destinatari

7 Come nell'art. 22, i destinatari dell'art. 23 sono le autorità federali e i responsabili privati del trattamento dei dati. Sono esclusi gli incaricati del trattamento. Per quanto riguarda il ruolo di questi incaricati del trattamento, si rimanda al corrispondente commento dell'art. 22.

8 Le autorità federali e i responsabili privati del trattamento dei dati sono quindi tenuti a consultare l'IFPDT se un trattamento dei dati pianificato comporta un rischio elevato per la personalità e i diritti fondamentali delle persone interessate, nonostante le misure attuate. L'IFPDT, dal canto suo, è tenuto a effettuare la consultazione in conformità con la LPD e a rispettare le scadenze applicabili (cfr. n. 25).

B. Trattamento "pianificato

9 Il testo dell'art. 23 prevede, al cpv. 1, che la consultazione dell'IFPDT debba essere effettuata in caso di trattamento pianificato che comporti un rischio elevato per la personalità o i diritti fondamentali dell'interessato. Questa disposizione si applica solo se il responsabile del trattamento ha già adottato misure per mitigare i rischi risultanti e il trattamento dei dati comporta comunque un rischio elevato.

10 Sebbene la formulazione suggerisca che ciò possa riguardare solo i trattamenti di dati nuovi e pianificati, essa copre anche le modifiche a trattamenti o

procedure già esistenti (cfr. il commento all'art. 69). Ciò significa che l'IFPDT deve essere consultato ogniqualvolta si verifichino cambiamenti nel processo di trattamento dei dati o mutate circostanze di fatto o giuridiche. Tuttavia, queste mutate circostanze devono suggerire o rendere evidente l'esistenza di un rischio elevato ai sensi dell'art. 22. Inoltre, le misure adottate nel contesto di una DIA rinnovata o ripetuta potrebbero non essere sufficienti a ridurre questo rischio elevato. Per quanto riguarda il concetto di rischio elevato, si rimanda alle spiegazioni sull'art. 22 (art. 22 n. 12 e segg.). La valutazione secondo cui l'IFPDT deve essere consultato anche in caso di modifiche alle attività di trattamento dei dati esistenti è supportata dal fatto che in un ambiente così dirompente, caratterizzato da rapidi cambiamenti, i responsabili del trattamento dei dati devono sempre includere i rischi nelle proprie considerazioni e nella pianificazione del trattamento dei dati, al fine di non mettere in pericolo o violare specificamente i diritti degli interessati (cfr. art. 7).

C. Consultazione

1. Introduzione

In primo luogo, l'art. 23 richiede che il responsabile del trattamento abbia effettuato una DIA in relazione a un trattamento dei dati pianificato o modificato ai sensi dell'art. 22. Se il responsabile del trattamento giunge alla conclusione che, nonostante le misure previste, il trattamento dei dati presenta un rischio elevato per la personalità o i diritti fondamentali dell'interessato, deve consultare l'IFPDT. Anche se la legge non prevede requisiti formali, questa consultazione deve avvenire per iscritto, se non altro per motivi di prova. Se questo rischio elevato non sussiste, il responsabile del trattamento può comunque presentare volontariamente la DIA all'IFPDT. Sebbene ciò sia utile per la sicurezza giuridica e dell'informazione, è probabile che i responsabili del trattamento privati si astengano dal farlo regolarmente (cfr. n. 34 e segg.). 11

La consultazione deve essere effettuata prima dell'inizio del trattamento dei dati in questione. Solo al termine della consultazione, ossia dopo che l'IFPDT ha emesso un parere, l'autorità federale o il responsabile del trattamento privato possono iniziare a trattare i dati. 12

13 Per quanto riguarda la consultazione, occorre tenere conto di tre punti:

- In primo luogo, la consultazione è soggetta a una tassa per i responsabili del trattamento privati (cfr. art. 59 cpv. 1 lett. c LPD; art. 44 LPD). I rispettivi costi dipendono dalle spese per il personale nel singolo caso. Per gli organi federali, invece, non sono previsti costi.
- In secondo luogo, l'IFPDT può a sua volta contattare il responsabile del trattamento e richiedere una valutazione dei rischi e una consultazione se viene a conoscenza di operazioni di trattamento pianificate.
- In terzo luogo, l'IFPDT può combinare questa richiesta con l'adozione di misure investigative (cfr. n. 23).

2. Informazioni da fornire

14 La disposizione dell'art. 23 precisa i casi in cui l'IFPDT deve essere consultato. Tuttavia, non definisce quali informazioni debbano essere presentate all'IFPDT per la sua valutazione. A causa di questa situazione iniziale, si può presumere, o è già stato annunciato, che lo stesso IFPDT emanerà delle linee guida corrispondenti poco dopo l'entrata in vigore, che il responsabile del trattamento potrà utilizzare come orientamento. Tuttavia, il responsabile del trattamento dovrebbe almeno assicurarsi che i documenti creati nel corso della DIA siano disponibili nella loro interezza, in modo che l'IFPDT possa emettere un parere corrispondente su questa base. Tali documenti devono quindi contenere, tra l'altro, informazioni sul trattamento previsto - compresa la finalità del trattamento, se applicabile - sui possibili rischi per la personalità o i diritti fondamentali dell'interessato e sulle misure tecniche e organizzative previste. Deve inoltre essere spiegato perché il rischio è ancora considerato elevato nonostante le misure descritte. Questo è importante, perché altrimenti non sarebbe necessaria alcuna consultazione.

15 Il DSGVO può servire da guida in questo senso, in quanto contiene un elenco delle informazioni da presentare (cfr. n. 39). Può essere utile anche procedere secondo il cosiddetto concetto ISDS. Questo prevede una descrizione del progetto il più precisa possibile, che includa una spiegazione della situazione giuridica e delle misure organizzative e tecniche. La descrizione del progetto deve includere informazioni sul titolare e sul responsabile del trattamento, sullo scopo e sul tipo di trattamento dei dati, nonché sui destinatari e sugli interessati. La descrizione degli aspetti organizzativi e tecnici richiede invece

una descrizione delle applicazioni, delle reti, delle tecnologie, nonché dei ruoli e dei concetti di autorizzazione. Va notato che in singoli casi possono essere richiesti concetti o piani d'azione più dettagliati.

Inoltre, i documenti presentati devono essere strutturati e includere il nome del richiedente e un indirizzo di contatto. Questo serve come mezzo di comunicazione con l'IFPDT nel caso in cui sorgano domande nei singoli casi o ci sia bisogno di altri chiarimenti. 16

3. Procedura dell'IFPDT

Una volta presentata la documentazione completa (cfr. n. 15 e segg.), l'IFPDT procede solitamente in tre fasi (i)-(iii): In una prima fase, le informazioni presentate vengono esaminate e si verifica se sono necessarie ulteriori informazioni, documenti o altri dettagli per il chiarimento. In tal caso, tali informazioni vengono richieste alla persona responsabile (i). Successivamente, i documenti vengono attentamente controllati e analizzati per verificarne la comprensibilità e la validità (ii). In una terza fase si conclude la procedura, con la comunicazione delle obiezioni, se necessario, e la proposta delle misure da adottare (iii). In queste tre fasi, l'IFPDT valuta se le misure proposte sono sufficienti a garantire la protezione della personalità e dei diritti fondamentali dell'interessato e a mitigare il rischio elevato. 17

Nella prima fase, l'IFPDT esamina le informazioni presentate dal titolare del trattamento e si assicura di comprendere l'operazione di trattamento dei dati. In particolare, l'attenzione si concentra sulla descrizione fattuale e tecnica del trattamento dei dati in questione. Se l'IFPDT necessita di ulteriori informazioni, le richiederà e, se necessario, chiederà una discussione orale del trattamento dei dati previsto con il responsabile del trattamento al fine di chiarire questioni specifiche. Va osservato che la formulazione della legge non chiarisce se il termine per la presentazione di osservazioni da parte dell'IFPDT inizi a decorrere solo dopo questa fase o direttamente dalla presentazione della richiesta di consultazione. Secondo il punto di vista qui adottato, tuttavia, il termine per presentare osservazioni inizia a decorrere solo dopo che tutte le informazioni richieste dall'IFPDT sono state presentate in modo completo. Ciò significa che la durata della consultazione può quindi essere superiore a questi due o tre mesi, a seconda delle informazioni e dei documenti supplementari che l'IFPDT continua a richiedere. 18

19 Su questa base, inizia la revisione vera e propria del trattamento dei dati in questione. In questa seconda fase, l'IFPDT esamina in particolare la valutazione dei rischi e le misure proposte dal titolare del trattamento. Questa valutazione comprende un esame dei requisiti legali, che include principalmente il rispetto dei principi di protezione dei dati. Oltre alla proporzionalità (parola chiave: economia dei dati ed evitamento dei dati), ciò include, tra l'altro, qualsiasi base legale o contrattuale o giustificazione per il trattamento dei dati, l'esternalizzazione del trattamento dei dati o la divulgazione dei dati all'estero, la sicurezza dei dati e la garanzia dei diritti degli interessati come, in particolare, il diritto all'informazione e il diritto alla correzione e alla cancellazione dei dati. Si deve tenere conto sia della sensibilità dei dati che delle parti coinvolte e delle loro responsabilità. Vengono inoltre esaminate le misure tecniche e organizzative. Ciò avviene in relazione alle tecnologie utilizzate e, se del caso, ai fornitori che le hanno adottate. Nell'era dei crescenti attacchi informatici e di hacker, questo serve alla sicurezza delle informazioni.

20 Dopo aver approfondito questi aspetti, in una terza fase l'IFPDT redige generalmente un parere all'attenzione della persona responsabile. In questo parere elenca le sue osservazioni sul trattamento dei dati previsto e offre una valutazione sia dal punto di vista legale che da quello tecnico-organizzativo. Se l'IFPDT giunge alla conclusione che il trattamento dei dati è conforme alla legge sulla protezione dei dati, non vi sono ulteriori requisiti per il responsabile del trattamento. In questo caso, l'IFPDT non formula alcuna raccomandazione. In tal caso, l'IFPDT può anche astenersi dal rilasciare una dichiarazione al responsabile del trattamento. Se l'IFPDT solleva obiezioni, le associa a proposte di misure concrete (cfr. misure art. 22 n. 26). Tali misure mirano a garantire il rispetto della protezione dei dati e della sicurezza delle informazioni. Di norma, l'IFPDT fissa un termine per l'attuazione di tali misure da parte del responsabile.

21 In questo contesto, va notato un caso particolare: Se, a seguito del trattamento dei dati effettuato, l'IFPDT giunge alla conclusione che le misure non erano sufficienti o che non esistono affatto misure per ridurre i rischi individuati, è autorizzato a svolgere un'indagine (art. 49). A tal fine, l'IFPDT dispone di tutte le misure amministrative di cui all'art. 51. L'indagine può quindi portare alla sospensione o addirittura al divieto di trattamento dei dati. Sebbene si possa presumere che l'IFPDT emetterà generalmente sentenze

formali solo in casi isolati, la legge gli lascia esplicitamente questa possibilità se i responsabili del trattamento dei dati non gestiscono i rischi in modo adeguato.

Va inoltre sottolineato che il parere dell'IFPDT è una raccomandazione non vincolante. Non ha il carattere di un ordine e non può quindi essere inteso in alcun modo come un'approvazione o addirittura un'autorizzazione a effettuare il trattamento dei dati previsto. 22

4. Limite di tempo

Se l'IFPDT è chiamato in causa per una consultazione, deve comunicare il suo parere al titolare del trattamento entro due mesi dalla presentazione completa all'IFPDT, ai sensi dell'articolo 23, paragrafo 2. L'IFPDT può prorogare il termine per l'invio del parere. L'IFPDT può prorogare il termine di un mese al massimo se il trattamento dei dati è complesso. Se il titolare del trattamento non riceve alcuna comunicazione dall'IFPDT entro questo termine, si può presumere che l'IFPDT non solleverà alcuna obiezione al trattamento dei dati previsto. 23

D. Eccezioni

L'articolo 23 prevede alcune eccezioni all'obbligo fondamentale di consultazione. Tali eccezioni sono disciplinate dal cpv. 4 e si applicano solo ai responsabili del trattamento dei dati privati. Le autorità federali sono quindi escluse dalle eccezioni. 24

Paragrafo 4 stabilisce che la consultazione non è necessaria se il titolare del trattamento consulta un consulente per la protezione dei dati in merito al trattamento dei dati previsto. A questo proposito, il messaggio afferma che il consulente per la protezione dei dati deve essere effettivamente coinvolto attivamente nella DPA. Deve quindi essere stato in grado di esprimersi in modo esauriente sulle misure e sui rischi. Alla luce di questa circostanza, sembra ragionevole regolamentare il processo di un DSFA, nonché le competenze e il coinvolgimento del consulente per la protezione dei dati in linee guida o direttive interne. 25

Secondo il messaggio, l'eccezione è volta a ridurre l'onere amministrativo per i responsabili del trattamento dei dati privati. Da un punto di vista economico, questa eccezione va accolta con favore. Ciò vale soprattutto perché, dal punto 26

di vista dei responsabili privati, si possono evitare ritardi, costi aggiuntivi e conseguenze potenzialmente negative dovute alla consultazione dell'IFPDT. Sebbene l'FDPIC si fosse espresso contro questa eccezione durante il processo di consultazione, alla fine è stata comunque integrata nel testo di legge.

27 L'eccezione deve essere interpretata anche come un incentivo per i responsabili del trattamento dei dati privati. Il regolamento offre loro un motivo molto specifico per nominare un consulente per la protezione dei dati. Questo incentivo è importante perché, a differenza dell'art. 37 DSGVO, la nomina di un consulente per la protezione dei dati è sempre volontaria ai sensi della LPD.

28 Tuttavia, l'eccezione si applica solo se sono soddisfatti i requisiti dell'art. 10(3). Di conseguenza, il consulente per la protezione dei dati deve essere professionalmente indipendente e non vincolato da istruzioni, deve essere esente da conflitti di interesse e deve possedere le competenze necessarie (per maggiori dettagli su questi requisiti si veda il commento all'art. 10). Il titolare del trattamento, invece, deve pubblicare i dati di contatto del consulente per la protezione dei dati e comunicarli all'IFPDT. Questa eccezione ricorda quella prevista dall'art. 11a cpv. 5 lett. e aDSG relativa all'obbligo di registrare le raccolte di dati, che è stata eliminata dalla LPD senza essere sostituita. I responsabili del trattamento dei dati privati hanno quindi già molta familiarità con questi requisiti.

29 I responsabili del trattamento privati che sviluppano o utilizzano modelli o tecnologie aziendali che potenzialmente comportano rischi elevati per gli interessati, sulla base dell'esperienza, nomineranno un consulente per la protezione dei dati e si avvarranno di questa eccezione. Ciò consentirà loro di evitare di consultare l'IFPDT. Ciò è tanto più probabile in quanto i responsabili del trattamento privati attivi a livello internazionale in tali settori sono già obbligati a nominare un responsabile della protezione dei dati ai sensi del DSGVO.

III. VIOLAZIONE DELL'OBBLIGO DI CONSULTAZIONE DELL'IFPDT

30 Nel caso in cui un responsabile del trattamento non consulti preventivamente l'IFPDT nonostante l'obbligo di cui all'art. 23, l'art. 51 cpv. 3 lett. e), prevede

che l'IFPDT possa ordinare al responsabile del trattamento di consultare preventivamente l'IFPDT sotto pena di ammenda. Per contro, gli interessati non hanno il diritto di agire in giudizio per ottenere la consultazione dell'IFPDT.

Se nel corso di un'indagine l'IFPDT stabilisce che un'operazione di trattamento dei dati comporta un rischio elevato, può ordinare che l'operazione di trattamento dei dati sia adattata, sospesa o completamente interrotta. Ciò vale fino a quando non sia stata effettuata una DIA e non sia stato consultato l'IFPDT (art. 51 cpv. 1 in combinato disposto con l'art. 49 f). Questa fase può comportare notevoli ritardi e quindi costi elevati e sforzi aggiuntivi per la persona responsabile. Inoltre, poiché i risultati di un'indagine possono essere pubblicati dall'IFPDT (art. 57 cpv. 2), in questi casi sono prevedibili rischi per la reputazione. 31

Tuttavia, la violazione dell'obbligo di consultazione dell'IFPDT non è autonomamente soggetta a una multa. Ciò sembra logico, soprattutto perché si tratta di un obbligo di diligenza e l'IFPDT ha le competenze corrispondenti (cfr. a questo proposito le spiegazioni dell'art. 22 n. 37). Nell'UE, in questi casi è prevista una multa. 32

IV. SFIDE E RILEVANZA PRATICA

La rilevanza pratica dell'art. 23 resta da vedere. Almeno i responsabili del trattamento dei dati privati cercheranno di evitare il più possibile l'obbligo adattando il trattamento dei dati previsto fino a quando non comporterà più un rischio elevato per gli interessati nell'ambito delle misure adottate. Si può quindi presumere che l'IFPDT sarà consultato solo in casi eccezionali. Vi sono altre ragioni per questo: Da un lato, i responsabili del trattamento dei dati privati non vorranno aspettare fino a tre mesi prima di ricevere una valutazione del loro trattamento dei dati e poter procedere con il loro progetto. Soprattutto perché si può presumere che questo periodo non inizierà prima che l'IFPDT abbia ricevuto tutte le informazioni che ritiene necessarie dal responsabile del trattamento. In singoli casi, ciò potrebbe comportare un'interruzione dei progetti molto più lunga. I progetti potrebbero poi riguardare anche processi e fatti rilevanti per l'azienda che, non appena presentati all'IFPDT, potrebbero diventare pubblici. Quest'ultimo, ad esempio, perché l'FDPIC deve riferire sulla DIA nel suo rapporto di attività o è obbligato a divulgare determinate informazioni sulla base di una richiesta 33

pubblica ai sensi di LTras. A ciò non si può sempre opporre il fatto che l'FDPIC si impegna a mantenere la riservatezza. Infine, la consultazione dell'IFPD ai sensi dell'art. 59 cpv. 1 lett. c LPD è soggetta a un onorario per i responsabili del trattamento dei dati privati in funzione del tempo impiegato dall'IFPD e si basa su una tariffa oraria di 150-250 franchi (art. 44 cpv. 2 LPD), che non deve essere un costo sottovalutato nel contesto di procedure di trattamento dei dati complesse. Gli onorari possono essere aumentati fino al doppio se la consultazione dell'IFPDT può essere ulteriormente utilizzata a fini commerciali (art. 44 cpv. 3 e 4 LADP). Questi costi si aggiungono ai costi propri che un DSFA comporta comunque per un responsabile del trattamento privato.

34 Nei casi in cui un'operazione di trattamento dei dati sia di dominio pubblico e l'IFPDT, a causa di questo o delle pressioni politiche che lo accompagnano, effettui un'indagine sul responsabile del trattamento o conduca un'inchiesta, i responsabili del trattamento privati possono essere obbligati a eseguire una DIA mediante un'ordinanza, come è avvenuto in passato (cfr. art. 51 cpv. 2 lett. d e art. 49). Tali ordini prevederanno presumibilmente anche l'obbligo di consultare l'IFPDT per quella particolare operazione di trattamento dei dati.

V. CONFRONTO CON IL DIRITTO DELL'UE

35 Il DSGVO prevede all'art. 36 cpv. 1 l'obbligo di consultare l'autorità di controllo competente se un trattamento di dati potrebbe comportare rischi elevati per gli interessati nonostante le misure adottate. A questo proposito, la disposizione è identica all'art. 23 cpv. 1 LPD.

36 Similmente all'art. 23 cpv. 2 DPA, l'autorità di controllo competente deve notificare al responsabile del trattamento e, se del caso, agli incaricati del trattamento coinvolti, eventuali obiezioni al trattamento dei dati previsto entro otto settimane ai sensi dell'art. 36 cpv. 2 DPA. Tali obiezioni possono sorgere perché l'autorità di controllo conclude che il responsabile del trattamento "non ha sufficientemente identificato o attenuato il rischio". Il termine, invece, può essere prorogato di sei settimane, e non solo di un mese, a partire dalla data di ricezione della richiesta. Tale proroga deve essere notificata alla persona responsabile entro un mese e deve essere accompagnata da una motivazione. L'autorità di controllo può sospendere questi termini fino a quando non avrà ricevuto le informazioni necessarie ai sensi dell'art. 36 cpv. 3 DSGVO. Le norme dell'UE sono più dettagliate rispetto

a quelle svizzere e sembrano avere senso, soprattutto perché regolano in modo più dettagliato il processo e anche gli obblighi delle autorità di controllo in relazione ai termini.

Se l'autorità di controllo ha obiezioni, deve inviare raccomandazioni scritte al responsabile del trattamento e, se del caso, agli incaricati del trattamento coinvolti, il che è molto simile alla normativa svizzera, dove in Svizzera il destinatario del parere è generalmente il responsabile del trattamento. L'autorità di controllo ha anche il diritto esplicito di esercitare gli altri poteri di cui all'art. 58 DSGVO. Ciò non è esplicitamente menzionato nella LPD. 37

Sebbene l'art. 23 DPA non contenga disposizioni più dettagliate sulle informazioni che il responsabile del trattamento deve fornire all'IFPDT nel contesto della consultazione, l'art. 36 cpv. 3 DPA contiene un elenco delle informazioni da fornire: Informazioni sulle responsabilità del responsabile del trattamento, dei contitolari del trattamento e, se del caso, dei responsabili del trattamento incaricati, le finalità e i mezzi del trattamento dei dati previsto, le misure e le garanzie previste per la protezione dei diritti e delle libertà degli interessati [ai sensi del DSGVO], i dati di contatto del responsabile della protezione dei dati, se del caso, la valutazione d'impatto sulla protezione dei dati stessa e qualsiasi altra informazione richiesta dall'autorità di controllo. 38

L'articolo 36 cpv. 4 e 5 del DSGVO disciplina poi alcuni diritti e obblighi degli Stati membri, nonché ulteriori requisiti che gli Stati membri possono prevedere nel loro diritto locale. 39

La violazione dell'obbligo di consultare l'autorità di controllo è punibile ai sensi del DSGVO, così come l'obbligo di condurre una DFA. Il DSGVO prevede multe fino a 10 milioni di euro o fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente per la violazione dell'obbligo di consultazione (art. 83 cpv. 4 lett. a DSGVO). Ciò è in contrasto con la LPD, che non prevede una multa in questi casi (cfr. n. 33). 40

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 25 LPD

Un commentario di Martin Steiger

CITAZIONE SUGGERITA

Martin Steiger, Kommentierung zu Art. 25 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Steiger, N. XXX zu Art. 25 DSG.

Capitolo 4: Diritti della persona interessata

Art. 25 Diritto d'accesso

[1] Chiunque può domandare al titolare del trattamento se dati personali che lo concernono sono oggetto di trattamento.

[2] Alla persona interessata sono fornite le informazioni necessarie affinché possa far valere i suoi diritti secondo la presente legge e sia garantito un trattamento trasparente dei dati. In ogni caso le sono fornite le informazioni seguenti:

a. l'identità e i dati di contatto del titolare del trattamento;

b. i dati personali trattati in quanto tali;

c. lo scopo del trattamento;

d. la durata di conservazione dei dati personali o, se ciò non è possibile, i criteri per stabilire tale durata;

e. le informazioni disponibili sulla provenienza dei dati personali che non sono stati raccolti presso la persona interessata;

f. se del caso, l'esistenza di una decisione individuale automatizzata e la logica su cui si fonda la decisione;

g. se del caso, i destinatari o le categorie di destinatari cui sono comunicati dati personali, nonché le informazioni di cui all'articolo 19 capoverso 4.

3 I dati personali concernenti la salute possono essere comunicati alla persona interessata per il tramite di un professionista della salute da lei designato; a tale scopo è necessario il consenso della persona interessata.

4 Il titolare del trattamento è tenuto a fornire le informazioni richieste anche se ha affidato il trattamento dei dati personali a un responsabile del trattamento.

5 Nessuno può rinunciare preventivamente al diritto d'accesso.

6 Il titolare del trattamento fornisce gratuitamente le informazioni. Il Consiglio federale può prevedere eccezioni alla gratuità, segnatamente se l'informazione richiede un onere sproporzionato.

7 Di norma l'informazione è fornita entro 30 giorni.

STRUTTURA

In breve 366
I. Generalità 366
A. Finalità 366
B. Storia delle origini 367
II. Diritto di accesso (cpv. 1) 368
III. Contenuto delle informazioni (cpv. 2) 370
IV. Casi speciali 372
A. Informazioni da parte di un professionista della salute (cpv. 3) 372
B. Trattamento da parte di incaricati del trattamento (cpv. 4) 373
V. Modalità 373
A. Nessuna rinuncia al diritto all'informazione (cpv. 5) 373
B. Fornitura gratuita di informazioni (cpv. 6) 373
C. Termine per fornire le informazioni (cpv. 7) 375
VI. Applicazione 375
Bibliografia 376

IN BREVE

L'art. 25 LPD disciplina il diritto all'informazione degli interessati come "pietra angolare della legge sulla protezione dei dati". Ogni interessato può chiedere al titolare del trattamento informazioni sull'eventuale trattamento di dati personali che lo riguardano. Il diritto all'informazione è altamente personale. Gli interessati non possono rinunciare in anticipo al diritto all'informazione. L'informativa deve contenere tutti i dettagli necessari per consentire all'interessato di far valere i propri diritti e di comprendere il trattamento dei dati. Il contenuto minimo dell'informativa è regolato dalla legge. Le informazioni devono essere fornite in forma comprensibile, gratuitamente ed entro 30 giorni. In caso di trattamento da parte di un incaricato, il responsabile del trattamento rimane obbligato a fornire informazioni. Gli interessati hanno diverse opzioni legali per far valere il loro diritto all'informazione.

I. GENERALITÀ

A. Finalità

1 Il capitolo 4, "Diritti degli interessati", comprende il diritto all'informazione (art. 25 e segg. LPD) e il diritto alla divulgazione o al trasferimento dei dati introdotto con la LPD (art. 28 e segg. LPD; anche: diritto alla portabilità dei dati). Il diritto all'informazione può essere ricavato dall'art. 13 della Cost. sulla "protezione della privacy" e dall'art. 8 della CEDU sul "diritto al rispetto della vita privata e familiare" ed è una "pietra miliare della legge sulla protezione dei dati". Il diritto di accesso deve quindi essere espressamente incluso anche nelle clausole di protezione dei dati in un contratto (art. 16 cpv. 2 lett. b LPD) e in garanzie specifiche (art. 16 cpv. 2 lett. c LPD) quando i dati personali vengono divulgati all'estero.

2 Il diritto di accesso è un diritto legale fondamentale per le persone interessate a scoprire - entro certi limiti - quali dati che le riguardano vengono trattati da chi e per quale scopo. In particolare, le persone interessate dovrebbero poter utilizzare il diritto di accesso per verificare se i loro dati sono trattati in conformità con i principi della legge sulla protezione dei dati (art. 6 e segg.

LPD). Il diritto all'informazione dovrebbe quindi avere una funzione di controllo e di prevenzione.

Il diritto all'informazione consente agli interessati di esercitare il loro diritto all'autodeterminazione informativa, se e nella misura in cui tale diritto è stato attuato nella LPD. Il diritto all'informazione e le informazioni fornite costituiscono spesso la base per l'esercizio di ulteriori diritti legali degli interessati, quali la rettifica e la cancellazione (artt. 32 e 41 LPD) o l'opposizione (art. 30 cpv. 2 lett. b LPD), in ultima analisi per far valere la protezione della personalità. 3

Il diritto all'informazione ai sensi degli artt. 25 e segg. LPD integra l'obbligo di informazione di cui agli artt. 19 e segg. e va oltre in termini di contenuto. Gli interessati possono ricevere informazioni che vanno al di là di quelle che il responsabile del trattamento è tenuto a comunicare loro, aumentando così la trasparenza. 4

I tre articoli sul diritto all'informazione sono strutturati come segue: L'art. 25 LPD stabilisce chi può richiedere informazioni e quali informazioni i responsabili del trattamento devono fornire e in quale ambito. L'art. 26 LPD chiarisce le condizioni in cui il diritto all'informazione può essere limitato. L'art. 27 LPD disciplina le condizioni in cui il diritto all'informazione può essere ulteriormente limitato in relazione ai media. Nell'ordinanza sulla protezione dei dati, gli artt. 16-19 LDP specificano il diritto all'informazione. 5

B. Storia delle origini

L'art. 25 si basa sul precedente art. 8 aDSG. Rispetto all'art. 8 LPD, le persone possono chiedere informazioni a tutti i responsabili del trattamento (art. 5 lett. j LPD) e non più solo al "responsabile di una raccolta di dati" (art. 3 lett. i i.V.m. art. 8 cpv. 1 LPD). Nel complesso, le precedenti disposizioni sul diritto all'informazione ai sensi dell'art. 8 aDSG e seguenti sono state mantenute e in parte integrate. 6

L'obbligo di informazione - dal punto di vista del responsabile del trattamento dei dati la controparte del diritto all'informazione degli interessati - non è più limitato a informazioni specifiche (come era ancora il caso in particolare nell'art. 8 cpv. 2 aDSG), ma devono essere fornite le informazioni necessarie per consentire all'interessato di far valere i propri diritti ai sensi della LPD e per garantire un trattamento trasparente dei dati (art. 25 cpv. 2 LPD). Allo 7

stesso tempo, si cerca di limitare "l'abuso abituale del diritto all'informazione per ottenere prove" ai sensi dell'aDSG. Nel dibattito parlamentare è stato aggiunto in particolare che devono essere fornite informazioni sui "dati personali trattati in quanto tali" (art. 25 cpv. 2 lett. b LPD).

II. DIRITTO DI ACCESSO (CPV. 1)

8 L'art. 25 cpv. 1 LPD stabilisce il diritto all'informazione in modo generale. Ogni persona fisica può chiedere che un responsabile del trattamento o un incaricato fornisca informazioni sull'eventuale trattamento di dati personali (art. 5 lett. a LPD) che la riguardano. I privati e gli organi federali responsabili sono tenuti a fornire informazioni (art. 5 lett. j LPD). In linea di principio, non è richiesta una giustificazione o un interesse legale per le informazioni richieste. Nel caso degli organi federali, la fornitura di informazioni è un ordine ai sensi dell'art. 5 PA, il che significa che sono necessarie una motivazione e istruzioni sulle modalità di ricorso ai sensi dell'art. 35 PA.

9 Il diritto all'informazione è di natura altamente personale ed è limitato all'accesso ai dati personali. Il diritto all'informazione non è trasferibile e non è ereditabile. Per le persone incapaci di giudizio, agisce il rappresentante legale (art. 19c cpv. 2 CC).

10 La persona interessata che richiede informazioni deve farsi identificare dal titolare del trattamento adottando misure ragionevoli e deve collaborare per dimostrare la propria identità (art. 16 cpv. 5 LDP). L'adeguatezza dell'identificazione con una copia di un documento d'identità ufficiale deve essere valutata caso per caso. L'obbligo di cui all'art. 1 cpv. 1 dell'AVDSG, secondo il quale l'interessato deve dimostrare la propria identità, non esiste più. A seconda dei dati disponibili su una persona, le informazioni contenute in una carta d'identità ufficiale possono non essere adatte all'identificazione. Nel caso delle piattaforme Internet, ad esempio, i responsabili spesso conoscono solo l'indirizzo e-mail o un numero di cellulare. In questo caso, l'identificazione può avvenire in questo modo. La richiesta generica di una copia di un documento d'identità, se necessario anche certificata, violerebbe i principi di necessità, proporzionalità e finalità della protezione dei dati (art. 6 cpv. 2, 3 e 4 LPD).

11 La richiesta dell'interessato di informazioni sul trattamento dei dati che lo riguardano deve, in linea di principio, essere formulata per iscritto (art. 16 cpv.

1 frase 1 LDP). Il responsabile del trattamento può anche autorizzare richieste di informazioni orali (art. 16 cpv. 1 frase 2 RPD). Il diritto all'informazione è quindi potenzialmente reso a bassa soglia. I mezzi elettronici sono equiparati ai mezzi scritti (Art. 16 (3) FADP). La forma scritta comprende qualsiasi forma che consenta una prova testuale.

Le informazioni sui dati trattati devono essere fornite per iscritto o nella forma in cui i dati sono disponibili (Art. 16 (2), prima frase, FADP). La forma elettronica equivale a quella scritta (art. 16 cpv. 3 LPD). Il responsabile del trattamento può offrire un'ispezione in loco, alla quale l'interessato non è tenuto ad acconsentire (art. 16, par. 2, seconda frase, LADP). Il responsabile del trattamento può anche fornire informazioni oralmente con il consenso dell'interessato (art. 16, par. 2, terza frase, LADP). In caso di ispezione in loco, esiste un diritto di copia. I dati personali dell'interessato devono essere protetti dall'accesso di terzi non autorizzati quando vengono fornite informazioni (art. 8 LPD). Il titolare del trattamento può rispondere nella stessa forma in cui l'interessato ha richiesto le informazioni, ad esempio tramite un messaggio di posta elettronica non criptato da capo a capo. La crittografia della posta elettronica è spesso impraticabile e non appropriata. Un'alternativa alla posta elettronica può essere la messaggistica istantanea con crittografia end-to-end standard, ad esempio con Signal, Threema o WhatsApp, a condizione che l'interessato che richiede le informazioni utilizzi un tale servizio di messaggistica istantanea. 12

Quando si utilizzano mezzi elettronici, in particolare la posta elettronica, occorre notare che una richiesta di informazioni o un'informazione fornita per via elettronica senza conferma di ricezione può non essere considerata consegnata. L'onere della prova spetta al mittente. Nel caso di piattaforme internet, può essere offerto di elaborare le richieste di informazioni e la fornitura di informazioni tramite la piattaforma. Tuttavia, gli interessati sono liberi di richiedere informazioni per iscritto. 13

Le informazioni devono essere fornite in una forma comprensibile per l'interessato (art. 16 cpv. 4 LADP). La comprensibilità, ad esempio nel caso di un formato insolito o non facilmente leggibile dei dati, può essere garantita da spiegazioni adeguate. Secondo la formulazione, la comprensibilità riguarda la forma e non il contenuto delle informazioni. 14

III. CONTENUTO DELLE INFORMAZIONI (CPV. 2)

15 Nel senso di una clausola generale ai sensi dell'art. 25 cpv. 2 LPD, l'informativa deve includere le informazioni necessarie per consentire alla persona interessata di far valere i propri diritti ai sensi della LPD e per garantire un trattamento trasparente dei dati. Se non sono disponibili dati personali, deve essere fornita un'informazione negativa.

16 Indipendentemente da ciò, l'art. 25 cpv. 2 LPD definisce un catalogo minimo di informazioni che devono essere fornite agli interessati: identità e dati di contatto del titolare del trattamento (lett. a, analoga all'art. 19 cpv. 2 lett. a LPD), dati personali trattati in quanto tali (lett. b), finalità del trattamento (lett. c, analoga all'art. 19 cpv. 2 lett. b LPD), periodo di conservazione o, se non è possibile, criteri per determinare il periodo di conservazione (lett. d), informazioni disponibili sull'origine dei dati personali (fonte), a meno che non siano state ottenute dall'interessato, poiché in questo caso l'interessato doveva già essere informato ai sensi dell'art. 19 lett. f. LPD (lett. e), l'esistenza e la logica di qualsiasi decisione individuale automatizzata ai sensi dell'art. 21 LPD (lett. f) e gli eventuali destinatari (lett. f, analoga all'art. 19 cpv. 2 lett. c LPD). È controverso se le informazioni non elencate debbano essere fornite dal responsabile del trattamento solo su richiesta o se si debba fare riferimento a tali informazioni fin dall'inizio.

17 Nel caso della persona responsabile ai sensi dell'art. 25 cpv. 2 lett. a, potrebbe non essere chiaro chi sia il responsabile, eventualmente insieme ad altri (art. 5 lett. j LPD). L'identità e i dati di contatto devono essere indicati o, se già noti, confermati. Chiunque riceva una richiesta di informazioni dovrà informare l'interessato - anche alla luce della clausola generale - se non esiste una responsabilità esclusiva o se non è possibile fornire informazioni per mancanza di responsabilità. In caso di responsabilità congiunta, la fornitura di informazioni deve essere coordinata tra i responsabili del trattamento, per cui gli interessati devono sempre poter richiedere informazioni a uno o più responsabili del trattamento in Svizzera, il che è particolarmente importante nel caso di altri responsabili del trattamento all'estero. Se vi sono più responsabili del trattamento, ogni singolo responsabile è tenuto a fornire informazioni (art. 17 cpv. 1 LADP). Se non esiste un responsabile del trattamento, in particolare nel caso di trattamento da parte di incaricati del trattamento (art. 8 LPD), la richiesta di informazioni deve essere inoltrata al responsabile del trattamento o, quanto meno, si deve fare riferimento al

responsabile del trattamento. L'onere di dimostrare che le informazioni indicate come complete sono effettivamente complete spetta al responsabile. I responsabili del trattamento di norma non vogliono dare l'impressione che le informazioni fornite siano complete e non sono obbligati a confermarlo.

Ai sensi dell'art. 25 par. 2 lett. b, devono essere forniti solo i dati personali trattati in quanto tali, vale a dire non, ad esempio, singoli documenti, e-mail, note o contratti nel loro complesso, ma solo i dati personali in essi contenuti. I documenti nel loro complesso possono essere forniti volontariamente, il che in pratica può essere più facile per il titolare del trattamento o il responsabile, a seconda dei dati. Il diritto di accesso può riguardare solo i dati personali trattati coperti dalla LPD (art. 2 cpv. 2 LPD), cioè, ad esempio, non i dati personali trattati da persone fisiche esclusivamente per uso personale (art. 2 cpv. 2 lett. a LPD e contrario). In caso di trattamento di grandi quantità di dati, il titolare del trattamento può chiedere all'interessato di specificare i dati. 18

Possono essere divulgati solo "i dati che esistono per iscritto o "fisicamente" e che quindi possono essere oggettivamente consultati a lungo termine [...], ma non i dati che possono essere semplicemente recuperati dalla memoria". "Il tipo di archiviazione o la denominazione" dei dati è irrilevante. 19

Il diritto di accesso ai dati di persone decedute ai sensi dell'art. 1 cpv. 7 LPD non è stato incorporato nella LDP o nella LPD. La disposizione è stata recentemente qualificata dalla giurisprudenza come contraria al diritto federale. 20

Ciò che costituisce un dato personale ai sensi del diritto all'informazione deve essere valutato caso per caso, soprattutto per quanto riguarda il criterio dell'identificabilità (art. 5 lett. a LPD). La norma e allo stesso tempo la restrizione è la clausola generale: "La legge sulla protezione dei dati ha il solo scopo di aiutare la persona interessata a far valere i propri diritti di protezione dei dati (almeno i diritti azionabili) e di garantire la trasparenza del trattamento dei dati (motivata dalla legge sulla protezione dei dati)". In particolare, il diritto di accesso non è inteso come mezzo per ottenere prove (cfr. n. 7 sopra). 21

Lo scopo del trattamento (art. 25 cpv. 2 lett. c) corrisponde a quello previsto dall'obbligo di informazione (art. 18 cpv. 2 lett. b LPD). 22

23 Il periodo di conservazione o, se non è possibile comunicare un periodo, i criteri per determinarlo (art. 25 cpv. 2 lett. d LPD) possono essere presi dai titolari del trattamento da qualsiasi elenco esistente di attività di trattamento (art. 12 cpv. 2 lett. e LPD). Come criterio, si dovrà almeno fare riferimento al principio di necessità (art. 6 cpv. 4 LPD).

24 In caso di origine, ai sensi dell'art. 25 cpv. 2 lett. e LPD, il responsabile del trattamento non può essere tenuto a chiarire l'origine dei dati.

25 Nel caso di una decisione individuale automatizzata, devono essere fornite informazioni su questo fatto, da un lato, e sulla logica su cui si basa la decisione, dall'altro, ai sensi dell'art. 25 cpv. 1 lett. f LPD. In linea di principio, l'esistenza stessa del dato dovrebbe essere già nota alla persona interessata in virtù dell'obbligo di informazione nel caso di una decisione individuale automatizzata (art. 21 cpv. 1 LPD; eccezioni ai sensi dell'art. 21 cpv. 3 LPD). La logica, ossia i criteri e i dati sottostanti, devono essere richiesti dall'interessato con riferimento al suo diritto all'informazione. Gli algoritmi possono essere protetti come segreti commerciali, ma i presupposti di base della logica dell'algoritmo devono essere dichiarati. Nel caso dell'"intelligenza artificiale", il diritto all'informazione ha i suoi limiti a questo riguardo, poiché il responsabile spesso non sa (e non può sapere) quali dati personali hanno portato al risultato visibile e perché.

26 Nel caso di eventuali destinatari ai sensi dell'art. 25 cpv. 2 lett. g, è sufficiente rivelare le categorie. Le categorie sono, ad esempio, le autorità o le società del gruppo, mentre i nomi non devono essere resi noti. Inoltre, devono essere fornite informazioni sulla divulgazione all'estero ai sensi dell'art. 19 cpv. 4 LPD.

IV. CASI SPECIALI

A. Informazioni da parte di un professionista della salute (cpv. 3)

27 Nel caso di dati personali relativi alla salute, l'art. 25 cpv. 3 LPD prevede che tali dati possano essere divulgati da un professionista della salute designato dalla persona interessata, previo consenso di quest'ultima. I dati sulla salute sono dati personali che richiedono una protezione speciale ai sensi dell'art. 5 lett. c n. 2 LPD.

La disposizione corrisponde in larga misura all'art. 8 cpv. 3 aDSG. Il consenso richiesto è stato aggiunto per consentire alla persona interessata di effettuare una scelta libera. Le informazioni non possono più essere fornite solo dai medici, ma da tutti gli operatori sanitari qualificati per il caso specifico. In particolare, devono essere considerati professionisti della salute i medici iscritti al Registro professionale medico (MedReg). 28

B. Trattamento da parte di incaricati del trattamento (cpv. 4)

In caso di trattamento di dati personali da parte di incaricati del trattamento (art. 9 LPD), il responsabile del trattamento rimane obbligato a fornire informazioni. La disposizione corrisponde alla prima frase del precedente art. 8 cpv. 4 aDSG, la cui seconda frase è stata eliminata senza sostituirla. 29

Un incaricato del trattamento a cui viene richiesto di fornire informazioni senza essere il responsabile del trattamento deve inoltrare la richiesta di informazioni al responsabile del trattamento o almeno fare riferimento al responsabile del trattamento. Ai sensi dell'art. 17 cpv. 2 della FADP, gli incaricati del trattamento devono assistere il responsabile del trattamento nel fornire informazioni se non sono stati incaricati di farlo. Il responsabile del trattamento dovrà disciplinare la fornitura di informazioni nel contratto con l'incaricato del trattamento (contratto di trattamento commissionato) (art. 9 cpv. 1 lett. a LPD). 30

V. MODALITÀ

A. Nessuna rinuncia al diritto all'informazione (cpv. 5)

Ai sensi dell'art. 25 cpv. 5 LPD, il diritto all'informazione non può essere rinunciato in anticipo. La disposizione corrisponde all'art. 8 cpv. 6 aDSG. 31

B. Fornitura gratuita di informazioni (cpv. 6)

Secondo l'art. 25 cpv. 6 LPD, in linea di principio le informazioni devono essere fornite gratuitamente. La corrispondente disposizione parziale dell'art. 8 cpv. 5 aDSG ("di norma [...] gratuitamente") è stata così ripresa. Il diritto all'informazione si basa sul presupposto che la fornitura di informazioni è generalmente possibile senza grandi sforzi se il trattamento dei dati è conforme alla legge e all'ordinanza. 32

33 Il Consiglio federale ha la facoltà di prevedere eccezioni al diritto all'informazione gratuita, "in particolare se lo sforzo richiesto è sproporzionato". Il Consiglio federale si è avvalso di questa competenza con l'art. 19 DPA.

34 In caso di sforzo sproporzionato, la fornitura di informazioni può eccezionalmente essere subordinata a un contributo ragionevole alle spese fino a 300 franchi (art. 19 cpv. 1 e 2 LDP).

35 Non sussiste uno sforzo sproporzionato se le informazioni devono essere fornite su una grande quantità di dati personali perché il titolare del trattamento raccoglie il maggior numero possibile di dati nel proprio interesse. Lo stesso vale se lo sforzo sproporzionato è il risultato di un'organizzazione inadeguata da parte del responsabile del trattamento. Nel caso delle richieste di informazioni alla fondazione meineimpfungen in seguito alla cessazione della piattaforma internet meineimpfungen.ch, l'IFPDT ha raccomandato di rimborsare agli interessati che avevano richiesto informazioni le spese per le copie certificate dei documenti di identità che la fondazione aveva richiesto.

36 Il responsabile del trattamento deve informare l'interessato che ha richiesto informazioni sull'importo della partecipazione ai costi prima di fornire le informazioni (art. 19 cpv. 3 frase 1 LDP). Se l'interessato non aderisce alle informazioni richieste entro dieci giorni, la richiesta di informazioni si considera ritirata senza spese (art. 19 cpv. 2 LADP). Il primo termine per fornire le informazioni ai sensi dell'articolo 18, paragrafo 1, della LADP è quindi prorogato di questo periodo di riflessione di dieci giorni (articolo 19, paragrafo 3, frase 2, della LADP).

37 In pratica, la partecipazione ai costi da parte dell'interessato è poco significativa. Nel caso di una contabilità dei costi completa, l'impegno della persona responsabile in relazione alla condivisione dei costi raggiunge spesso un massimo di 300 franchi svizzeri. Questo sforzo aumenta ulteriormente se l'interessato adegua la sua richiesta di informazioni a causa della condivisione dei costi richiesta, in modo che il responsabile non possa più rivendicare uno sforzo sproporzionato. Di solito è più facile per il responsabile chiedere una definizione più precisa delle informazioni richieste (cfr. n. 18 sopra).

C. Termine per fornire le informazioni (cpv. 7)

Per la fornitura di informazioni si applica un termine iniziale di 30 giorni dal ricevimento da parte del titolare del trattamento (art. 18 cpv. 1 LDP). Il responsabile del trattamento può prorogare il termine se le informazioni non possono essere fornite entro 30 giorni, e in tal caso deve informare l'interessato del nuovo termine (art. 18, par. 2, RPD). L'informazione deve essere fornita prima della scadenza del primo termine di 30 giorni, così come l'informazione sul rinvio, la restrizione o il rifiuto dell'informazione (art. 18 cpv. 3 LADP; cfr. art. 26 f. LADP sulle restrizioni all'accesso). LPD sulle limitazioni del diritto all'informazione). 38

VI. APPLICAZIONE

Il diritto all'informazione deve essere fatto valere con un'azione civile contro i privati responsabili, laddove il mancato adempimento non costituisce in linea di principio una violazione diretta dei diritti della personalità. Il mancato adempimento non può essere giustificato ai sensi dell'art. 31 LPD. Il foro competente per le azioni civili è il domicilio o la residenza di una delle parti (art. 20 lett. d CPC); non è previsto il pagamento di un anticipo sulle spese (art. 99 cpv. 3 lett. d CPC) e non vengono riconosciute le spese processuali (art. 113 cpv. 2 lett. g e 114 lett. g CPC). La procedura semplificata si applica alle azioni per far valere il diritto all'informazione (art. 243 cpv. 2 lett. d CPC). 39

Il diritto all'informazione nei confronti degli organi federali responsabili deve essere esercitato mediante ricorso. L'interessato che richiede informazioni ha diritto a una sentenza impugnabile. 40

L'IFPDT può ordinare la trasmissione di informazioni in un procedimento amministrativo ai sensi degli artt. 49 e segg. LPD e può comminare una sanzione (art. 51 cpv. 3 lett. g e 63 LPD). L'interessato non è parte in causa in questo procedimento (art. 52 cpv. 2 LPD e contrario). 41

La fornitura intenzionale di informazioni false o incomplete è punibile, su richiesta della persona interessata, con una multa fino a 250.000 franchi svizzeri (art. 60 cpv. 1 lett. a LPD). L'interessato ha il diritto di presentare un'istanza (art. 30 CP, in particolare art. 30 cpv. 1 CP). A differenza del DSGVO, la LPD non prevede sanzioni amministrative (art. 83 DSGVO), anche 42

se è possibile una sanzione pecuniaria per le imprese in via eccezionale (cfr. n. 44).

43 Chiunque, in qualità di responsabile o incaricato, non risponda a una richiesta di informazioni o dichiari falsamente di non essere obbligato a fornire informazioni non è perseguibile. Questa scappatoia di responsabilità penale esisteva già con l'art. 34 cpv. 1 lett. aDSG, che prevedeva una multa massima di 10.000 franchi svizzeri (art. 106 cpv. 1 CP).

44 La disposizione sanzionatoria è fondamentalmente limitata alle persone fisiche nel caso di privati responsabili. Il rischio di una multa è essenzialmente a carico delle singole persone fisiche che forniscono informazioni, che possono anche essere un soggetto subordinato. Le società possono essere punite solo in casi eccezionali; in questo caso la multa massima possibile è di 50.000 franchi svizzeri (art. 64 LPD). La responsabilità penale per la fornitura intenzionale di informazioni incomplete non si applica se non si dà l'impressione che le informazioni siano complete. Non esiste l'obbligo di rilasciare una dichiarazione di completezza. Per i dipendenti dell'Amministrazione federale e di altri organi federali sono previste solo sanzioni disciplinari.

BIBLIOGRAFIA

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 26 LPD

Un commentario di Martin Steiger

CITAZIONE SUGGERITA

Martin Steiger, Kommentierung zu Art. 26 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Steiger, N. XXX zu Art. 26 DSG.

Art. 26 Restrizione del diritto d'accesso

[1] Il titolare del trattamento può rifiutare, limitare o differire l'informazione se:

a. lo prevede una legge in senso formale, segnatamente per tutelare un segreto professionale;

b. lo esigono interessi preponderanti di terzi; o

c. la domanda d'accesso è manifestamente infondata, segnatamente se persegue uno scopo contrario alla protezione dei dati, o se è querulosa.

[2] Il titolare del trattamento può inoltre rifiutare, limitare o differire l'informazione se:

a. è un privato e:

lo esigono i suoi interessi preponderanti, e
non comunica i dati personali a terzi; o

b. è un organo federale e:

lo esige un interesse pubblico preponderante, in particolare la sicurezza interna o esterna della Svizzera, o
la fornitura delle informazioni rischia di compromettere un'indagine, un'istruzione o un procedimento giudiziario o amministrativo.

[3] Le imprese appartenenti al medesimo gruppo non sono considerate terzi ai sensi del capoverso 2 lettera a numero 2.

[4] Il titolare del trattamento indica il motivo per cui rifiuta, limita o differisce l'informazione.

STRUTTURA

In breve 382
I. Aspetti generali 382
II. Tipi di restrizione (cpv. 1 e 2) 382
III. Motivi di restrizione (cpv. 1-3) 384
A. Obblighi legali, in particolare il segreto professionale (cpv. 1 lett. a) 384
B. Interessi prevalenti di terzi (cpv. 1 lett. b) 384
C. Infondatezza evidente o querela evidente (cpv. 1 lett. c) 385
D. Interessi prevalenti dei responsabili del trattamento privati (cpv. 2 lett. a e cpv. 3) 386
E. Interessi preponderanti degli organi federali (cpv. 2 lett. b) 387
IV. Obbligo di motivazione (cpv. 4) 387
Bibliografia 388

IN BREVE

L'art. 26 LPD disciplina le possibili restrizioni al diritto all'informazione degli interessati. Il responsabile del trattamento può rinviare, limitare o rifiutare di fornire informazioni per vari motivi. In particolare, possono essere considerati motivi di restrizione gli obblighi di legge come il segreto professionale, gli interessi prevalenti di terzi e la manifesta infondatezza o l'evidente querelle. Le persone private in posizione di responsabilità possono invocare i propri interessi prevalenti, mentre gli organi federali possono invocare interessi pubblici prevalenti. Le restrizioni devono essere proporzionate, esaminate caso per caso e giustificate alla persona interessata.

I. ASPETTI GENERALI

1 Il diritto all'informazione degli interessati ai sensi dell'art. 25 LPD sussiste nei limiti dell'art. 26 f. LPD. LPD. L'informazione può essere rinviata, limitata o rifiutata dal responsabile del trattamento per vari motivi di restrizione (art. 26 LPD). I media possono invocare ulteriori motivi per limitare le informazioni (art. 27 LPD).

2 La disposizione "possono" dà l'impressione che i responsabili del trattamento siano liberi di decidere se limitare l'accesso. Tuttavia, non è così, perché i responsabili del trattamento dei dati possono spesso essere obbligati a limitare l'accesso. L'art. 26 cpv. 1 LPD elenca come motivi gli obblighi di legge (lett. a), gli interessi preponderanti di terzi (lett. b) e la manifesta infondatezza (lett. c). Altri motivi sono elencati nell'art. 26 cpv. 2 LPD a seconda che il responsabile sia un privato (lett. a) o un ente federale (lett. b) (cfr. n. 8 e segg.).

II. TIPI DI RESTRIZIONE (CPV. 1 E 2)

3 Le informazioni possono essere rinviate, limitate o rifiutate (art. 26 cpv. 1 e 2 LPD). La restrizione deve essere proporzionata, ossia necessaria, adeguata e appropriata o proporzionata in senso stretto, anche ai sensi dell'art. 6 cpv. 2 LPD e dell'art. 36 cpv. 3 Cost. In particolare, la restrizione deve essere idonea nella forma e nella portata, nonché in termini di tempo, a raggiungere l'obiettivo desiderato.

In caso di rifiuto, non sarà fornita alcuna informazione. L'interessato che richiede informazioni non riceverà alcuna informazione per un periodo di tempo illimitato. Il responsabile del trattamento non informa l'interessato se è in corso un trattamento di dati personali che lo riguardano (art. 25 cpv. 1 LPD). Se il rifiuto è limitato nel tempo, si tratta di un rinvio (cfr. n. 6). 4

Limitazione significa che vengono fornite solo informazioni parziali, ad esempio oscurando alcune informazioni. La restrizione può anche significare che le informazioni vengono fornite in tutto o in parte, ma che sono soggette a condizioni. Una condizione può essere che le informazioni fornite non siano rese accessibili a terzi e non siano pubblicate. Il responsabile del trattamento può richiedere all'interessato che richiede le informazioni di confermare in anticipo che rispetterà qualsiasi condizione, anche sotto forma di accordo di riservatezza. Un'ulteriore protezione, ad esempio mediante l'accordo su una sanzione contrattuale nel caso di un privato responsabile o mediante la minaccia di una sanzione ai sensi dell'art. 292 CP nel caso di un organo federale responsabile, dovrebbe essere consentita solo in casi eccezionali in considerazione della proporzionalità (cfr. n. 3 sopra). La fornitura ristretta di informazioni, comprese le eventuali condizioni, può essere limitata nel tempo. In questo caso, si tratta di un rinvio (cfr. n. 6). 5

In caso di differimento, l'informazione non viene fornita in tutto o in parte entro il termine (art. 25 cpv. 7 LPD), ma solo in un momento successivo. Nel caso di un organo federale responsabile, ad esempio, l'informazione può essere rinviata per non interferire con la libera formazione dell'opinione e della volontà. 6

A differenza dell'art. 9 cpv. 3 aDSG, l'art. 26 LPD non disciplina come procedere se i motivi di restrizione vengono meno. Ai sensi dell'art. 9 cpv. 3 aDSG, in questo caso un organo federale deve fornire le informazioni, a meno che la fornitura di informazioni sia impossibile o possibile solo con uno sforzo sproporzionato. Per gli organi federali responsabili, si può presumere che questo dovere fondamentale di riconsiderazione continuerà ad essere applicato. D'altro canto, l'obbligo di rispondere retroattivamente può essere ipotizzato solo con riserva nel caso di organi responsabili privati, ossia logicamente in caso di rinvio. 7

III. MOTIVI DI RESTRIZIONE (CPV. 1-3)

8 L'art. 26 cpv. 1-3 LPD elenca in modo conclusivo i possibili motivi di restrizione. Se non vi è alcun motivo di restrizione, l'informazione non può essere limitata in alcun modo (cfr. n. 3 e segg.). Se esiste più di un motivo di limitazione, i responsabili possono invocare tutti i motivi di limitazione. Tutti i responsabili del trattamento possono invocare i motivi di limitazione ai sensi dell'art. 26 cpv. 1 LPD. I motivi di limitazione di cui all'art. 26 cpv. 2 LPD distinguono tra responsabili del trattamento privati e organi federali. L'art. 26 cpv. 3 LPD riguarda solo le persone private. L'art. 5 lett. i LPD stabilisce se un responsabile è considerato un organismo federale.

A. Obblighi legali, in particolare il segreto professionale (cpv. 1 lett. a)

9 Secondo la formulazione, questo motivo di restrizione si applica esclusivamente agli obblighi di legge in senso formale. A parte la menzione ora esplicita del segreto professionale, questo motivo di restrizione è stato ripreso dall'art. 9 cpv. 1 lett. a aDSG. Al contrario, non sono sufficienti gli obblighi legali previsti da un'ordinanza. La possibilità di limitare le informazioni con riferimento al segreto d'ufficio generale deve essere esaminata in ogni singolo caso.

10 Inoltre, l'obbligo deve riguardare la restrizione delle informazioni alle persone interessate. Le disposizioni di legge che escludono in generale l'accesso ai dati personali non sono rilevanti. Un avvocato, ad esempio, può invocare il segreto professionale nei confronti di terzi ai sensi dell'art. 13 dell'AFC, ma non nei confronti di un cliente in quanto persona interessata.

B. Interessi prevalenti di terzi (cpv. 1 lett. b)

11 Non è necessario che i dati o le informazioni riguardino esclusivamente l'interessato che li richiede. Possono riguardare anche altre persone interessate (art. 5 lett. b LPD), ma anche altri soggetti terzi, come le persone giuridiche. Tra i terzi rientrano, ad esempio, i dipendenti del titolare del trattamento. Tale rapporto, e quindi gli eventuali interessi di terzi, sono possibili anche senza che i dati personali di tali terzi siano interessati. Pertanto, un terzo o una terza parte su cui il responsabile del trattamento non

tratta dati personali potrebbe comunque avere un interesse a che le informazioni fornite a una persona che richiede informazioni siano limitate.

Se vengono lesi gli interessi di terzi, il responsabile del trattamento deve esaminare se esistono interessi prevalenti e, in caso affermativo, se tali interessi prevalenti richiedono la limitazione delle informazioni. L'esame, compresa la ponderazione degli interessi, deve essere effettuato caso per caso. La necessità di interessi prevalenti dimostra che gli interessi dell'interessato che richiede le informazioni non sono di per sé prevalenti. Al contrario, gli interessi del terzo interessato alle informazioni riservate devono essere superiori agli interessi della persona interessata, vale a dire che si deve presumere una "certa rilevanza del pregiudizio della posizione del terzo". Il motivo della restrizione è stato ripreso senza modifiche dall'art. 9 cpv. 1 lett. b aDSG. L'eccezione si applica anche all'obbligo di informazione ai sensi dell'art. 20 cpv. 3 lett. a LPD. 12

C. Infondatezza evidente o querela evidente (cpv. 1 lett. c).

Ai sensi dell'art. 26 cpv. 1 lett. c LPD, le informazioni possono essere limitate se la richiesta di informazioni è manifestamente infondata, ossia se persegue uno scopo contrario alla protezione dei dati, o è manifestamente querula. Questi motivi di restrizione rappresentano un'innovazione rispetto ai motivi di restrizione previsti dall'art. 9 aDSG e sono stati aggiunti durante il dibattito parlamentare, supportati anche dalla giurisprudenza. Anche in questo caso si dovrebbero evitare richieste di informazioni abusive. 13

Questi motivi di restrizione devono essere interpretati in modo restrittivo. La persona responsabile non deve dare per scontato, senza ulteriori approfondimenti, che una richiesta di informazioni sia palesemente infondata o querula. In particolare, le richieste di informazioni sono considerate manifestamente querule se sono palesemente intese a "molestare o esercitare una persona responsabile (ad esempio con la ripetizione o con la consapevolezza dell'inutilità dell'informazione)". Una richiesta di informazioni è considerata manifestamente infondata se non tenta di rivendicare diritti di protezione dei dati o di creare trasparenza motivata dalla legge sulla protezione dei dati. 14

Se una richiesta di informazioni è effettivamente manifestamente infondata o manifestamente querula, si deve scegliere la soluzione più favorevole 15

all'interessato. La soluzione scelta, in particolare il rinvio o la restrizione piuttosto che il rifiuto, deve essere proporzionata (cfr. n. 3 sopra).

D. Interessi prevalenti dei responsabili del trattamento privati (cpv. 2 lett. a e cpv. 3)

16 I responsabili del trattamento privati possono limitare le informazioni al di là dei motivi di cui all'art. 26 cpv. 1 LPD se i loro interessi prevalgono su quelli dell'interessato che richiede le informazioni (cpv. 1) e se i dati in questione non vengono divulgati a terzi (cpv. 2). Questi requisiti si applicano cumulativamente. L'esame, compreso l'eventuale bilanciamento degli interessi, deve avvenire caso per caso (cfr. anche il precedente n. 12). La disposizione corrisponde nel contenuto all'art. 9 cpv. 4 aDSG ed esiste anche come eccezione per l'obbligo di informazione (art. 20 cpv. 3 lett. c LPD).

17 I dati che servono a proteggere da furti in un grande magazzino, la protezione di segreti di fabbricazione e commerciali o un elevato esborso finanziario sono esempi di possibili interessi prevalenti, per cui nel caso di questi ultimi la condivisione dei costi deve essere esaminata ai sensi dell'art. 26 cpv. 6 LPD.

18 I dati che non vengono comunicati a terzi o a terzi "reali", ossia i dati interni, sono in linea di principio dati che vengono comunicati solo a persone che appartengono alla stessa struttura organizzativa o aziendale, ossia non a un'altra struttura organizzativa o aziendale, e che con il trattamento dei dati possono perseguire finalità diverse da quelle del titolare del trattamento. Nel corso del dibattito parlamentare è stato creato un privilegio di gruppo con l'art. 26 cpv. 3 LPD, secondo il quale le società che appartengono allo stesso gruppo non sono considerate terzi ai sensi dell'art. 26 cpv. 2 lett. a n. 2 LPD (lo stesso vale per l'obbligo di informazione; art. 20 cpv. 3 lett. c n. 2 in combinato disposto con il cpv. 4 LPD). cpv. 4 LPD). L'aDSG non conosceva ancora tale privilegio e le società del gruppo erano considerate terze parti.

19 L'eccezione si applica anche alle società all'estero che appartengono allo stesso gruppo. In caso contrario, per la divulgazione di dati a società del gruppo all'estero si applicano gli obblighi previsti dalla legge sulla protezione dei dati, ad esempio per la divulgazione di dati personali all'estero (art. 16 f. LPD).

20 Gli appaltatori ai sensi dell'art. 5 lett. k LPD non sono considerati terzi (cfr. anche artt. 9 e 24 cpv. 4 LPD).

E. Interessi preponderanti degli organi federali (cpv. 2 lett. b)

Gli organi federali, in quanto responsabili del trattamento dei dati, possono limitare le informazioni al di là dei motivi di cui all'art. 26 cpv. 1 LPD se gli interessi pubblici prevalgono sugli interessi della persona che richiede le informazioni (cpv. 1) o se le informazioni mettono in pericolo un'indagine, un'inchiesta o un procedimento giudiziario (cpv. 2). La disposizione corrisponde essenzialmente all'art. 9 cpv. 2 aDSG ed esiste anche come eccezione all'obbligo di informazione (art. 20 cpv. 3 lett. d LPD). 21

Nummero 1 cita in particolare la sicurezza interna o esterna della Confederazione come possibile interesse pubblico prevalente, la cui tutela può richiedere una restrizione dell'informazione. L'elenco è esemplificativo, vale a dire che tutti gli interessi pubblici possono essere considerati motivi di restrizione, a condizione che siano prevalenti e che la restrizione sia necessaria per salvaguardare gli interessi corrispondenti. Altri interessi pubblici che entrano in gioco sono - sempre in base all'art. 7 cpv. 1 LTras - ad esempio la libera formazione dell'opinione e della volontà delle autorità, degli organi giudiziari e di altri enti pubblici, l'attuazione di misure ufficiali specifiche in conformità agli obiettivi, gli interessi di politica estera o le relazioni internazionali della Svizzera, le relazioni tra la Confederazione e i Cantoni o gli interessi di politica economica, monetaria e valutaria della Svizzera. 22

Nummer 2 cita come ulteriore motivo di restrizione l'eventuale messa in pericolo di un'indagine, di un'inchiesta o di un procedimento ufficiale o giudiziario. Questa restrizione si applica solo se e nella misura in cui la LPD è applicabile a tali indagini e procedimenti (art. 2 cpv. 3 LPD). In letteratura si sostiene che le indagini interne che precedono un procedimento disciplinare, ad esempio, potrebbero rientrare in questa disposizione. 23

Entrambi i motivi di restrizione devono essere esaminati caso per caso, compresa l'eventuale ponderazione degli interessi (cfr. anche i precedenti nn. 12 e 16). 24

IV. OBBLIGO DI MOTIVAZIONE (CPV. 4)

Il responsabile del trattamento deve giustificare la restrizione delle informazioni all'interessato, come già previsto dall'art. 9 cpv. 5 aDSG. La 25

giustificazione deve consentire all'interessato di comprendere il motivo o i motivi della restrizione e di esaminarne la legittimità. Nel caso degli organi federali competenti, la limitazione deve essere disposta almeno su richiesta dell'interessato sotto forma di ordinanza impugnabile (art. 5 PA). Non vi è alcun obbligo di conservare le motivazioni addotte, ma per motivi di prova è ovvio che il responsabile conservi la relativa comunicazione con l'interessato.

26 L'onere della prova dei motivi della restrizione spetta alla persona responsabile, anche per quanto riguarda la proporzionalità. Nel caso di richieste abusive di informazioni ai sensi dell'art. 26, par. 1, lett. c) LPD, è sufficiente dimostrare che una richiesta di informazioni "serve ovviamente in modo rilevante a uno scopo che non riguarda la protezione dei dati", il che costituisce una facilitazione della prova.

BIBLIOGRAFIA

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 27 LPD

Un commentario di Martin Steiger

CITAZIONE SUGGERITA

Martin Steiger, Kommentierung zu Art. 27 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Steiger, N. XXX zu Art. 27 DSG.

Art. 27 Restrizioni del diritto d'accesso nei confronti dei mezzi di comunicazione di massa

[1] Se i dati personali sono trattati esclusivamente in vista della pubblicazione nella parte redazionale di un mezzo di comunicazione di massa con carattere periodico, il titolare del trattamento può rifiutare, limitare o differire l'informazione se:

a. i dati forniscono indicazioni sulle fonti;

b. l'informazione permette di accedere a progetti di pubblicazioni; o

c. la libera formazione dell'opinione del pubblico rischia di essere compromessa.

[2] I giornalisti possono inoltre rifiutare, limitare o differire l'informazione qualora i dati personali servano loro esclusivamente a titolo di strumento personale di lavoro.

STRUTTURA

In breve 392
I. Aspetti generali 392
II. Prerequisiti per il privilegio dei media 392
III. Motivi di restrizione 393
A. Protezione delle fonti (cpv. 1 lett. a) 393
B. Protezione delle bozze (cpv. 1 lett. b) 394
C. Protezione della libertà di opinione del pubblico (cpv. 1 lett. c) 394
D. Strumenti di lavoro personali dei professionisti dei media (cpv. 2) 394
Bibliografia 395

IN BREVE

L'art. 27 LPD disciplina il privilegio dei media. A determinate condizioni, i media e i professionisti dei media possono limitare il diritto all'informazione degli interessati al di là dei motivi generali di restrizione. Il privilegio dei media si applica solo ai dati personali per le pubblicazioni editoriali nei media periodici. Il privilegio dei media serve a proteggere la libertà dei media.

I. ASPETTI GENERALI

1 È indubbio che la LPD si applica anche ai media. A causa del ruolo speciale dei media, soprattutto nel contesto della libertà dei media, compreso il segreto editoriale (art. 17 BV), l'art. 10 aDSG conosceva già un privilegio per i media (restrizioni al diritto all'informazione per i professionisti dei media). Questo privilegio dei media è stato ripreso sostanzialmente invariato, così come la relativa giustificazione (art. 31 cpv. 2 lett. d LPD, sebbene con adeguamenti rispetto all'art. 13 cpv. 2 lett. d aDSG). Il titolo ora menziona i media e non più i professionisti dei media, sebbene la disposizione riguardi ancora i media e i professionisti dei media.

2 Al privilegio dei media si applicano i tipi generali di restrizioni (art. 26 cpv. 1 e 2 LPD) e lo stesso obbligo di motivazione (art. 26 cpv. 4 LPD). Allo stesso modo, le restrizioni devono essere proporzionate e devono essere esaminate caso per caso.

II. PREREQUISITI PER IL PRIVILEGIO DEI MEDIA

3 I responsabili del trattamento che desiderano limitare le informazioni in riferimento al privilegio dei media devono soddisfare cumulativamente i seguenti requisiti: I dati personali in questione possono essere trattati esclusivamente per la pubblicazione nella sezione editoriale di un mezzo di comunicazione periodico (cpv. 1).

4 Trattamento esclusivo: i dati personali in questione non possono essere trattati per scopi diversi dalla pubblicazione nella sezione editoriale di un mezzo di comunicazione periodico. Qualsiasi altra finalità non obbligatoria per legge, come il segreto professionale (cfr. art. 26 n. 9 e segg.), significa che le informazioni non possono essere limitate in base al privilegio dei media. I

dati personali contenuti negli archivi dei media accessibili al pubblico non sono coperti dal privilegio dei media.

Uso editoriale: Articoli, rapporti, serie fotografiche, interviste, commenti e opinioni sono considerati editoriali. Anche i commenti dei lettori, tradizionalmente sotto forma di lettere al direttore, sono considerati editoriali. Non sono considerati editoriali gli scopi interni e altri scopi non editoriali, in particolare il marketing e la pubblicità dei lettori o le possibilità di comunicazione per il pubblico senza riferimenti editoriali, come le chat room. Non sono considerati editoriali nemmeno i commenti dei lettori che non vengono vagliati prima della pubblicazione. 5

Pubblicazione: i dati personali in questione devono essere trattati con l'obiettivo di pubblicare tali dati personali o almeno di contribuire a una pubblicazione. La dicitura "trattati per la pubblicazione [...]" significa che le informazioni riservate non si limitano al trattamento prima della pubblicazione, ma dipendono dallo scopo del trattamento, indipendentemente dal momento. 6

Mezzo di comunicazione pubblicato periodicamente: per mezzi di comunicazione ai sensi dell'art. 27 cpv. 1 LPD si intendono tutti i mezzi di diffusione delle informazioni, compresi i mezzi digitali quali newsletter via e-mail, canali di social media e newsletter. Il termine "mezzo" è deliberatamente formulato in modo aperto e tecnologicamente neutrale. La pubblicazione deve essere periodica, cioè ripetuta, senza che l'intervallo o il periodo debba essere sempre lo stesso. Un sito web pubblicato una sola volta con contributi editoriali o una rivista pubblicata una sola volta con contenuti giornalistici non sono pertanto considerati mezzi di pubblicazione periodica. 7

III. MOTIVI DI RESTRIZIONE

A. Protezione delle fonti (cpv. 1 lett. a)

Qualsiasi deduzione dai dati personali in questione a fonti di informazione di qualsiasi tipo è considerata un motivo di restrizione. Il motivo di restrizione va oltre la protezione delle fonti di cui all'art. 28a CP, ma allo stesso tempo richiede che i dati "forniscano effettivamente informazioni" e non solo che vi sia una possibilità corrispondente. Nel caso della sola protezione delle fonti, va notato che questa non garantisce la protezione delle fonti, ma consente ai 8

media e ai professionisti dei media di proteggere le loro fonti a determinate condizioni.

B. Protezione delle bozze (cpv. 1 lett. b)

9 Questo motivo di restrizione è volto a prevenire la precensura, anche se la protezione delle fonti (cpv. 1 lett. a) è garantita. Si parla anche di protezione della pubblicazione: la possibilità di un controllo preventivo attraverso il diritto di accesso potrebbe indurre i media e i professionisti dei media a non pubblicare i contenuti come previsto o a non pubblicarli affatto. Il motivo della restrizione può quindi anche prevenire un "effetto di raffreddamento".

C. Protezione della libertà di opinione del pubblico (cpv. 1 lett. c)

10 La libertà di opinione e di informazione comprende, tra l'altro, il diritto di ogni persona di formarsi liberamente un'opinione (art. 16 cpv. 2 Cost.), tra l'altro sulla base dei contenuti dei media e dei professionisti dei media (art. 16 cpv. 3 Cost.). La relativa giustificazione è volta a proteggere un panorama mediatico ben funzionante.

D. Strumenti di lavoro personali dei professionisti dei media (cpv. 2)

11 Questo motivo di restrizione riguarda i dati personali che non sono già esclusi dall'ambito di applicazione della LPD in quanto dati personali trattati da una persona fisica esclusivamente per uso personale (art. 2 cpv. 2 lett. a LPD) e che sono trattati da professionisti dei media.

12 Le raccolte di informazioni personali o gli appunti non rientrano nell'eccezione dell'art. 2 cpv. 2 lett. a LPD se vengono divulgati a terzi dai professionisti dei media. Spesso i professionisti dei media ne hanno bisogno, ad esempio nei contatti con le fonti e nelle ricerche.

13 I professionisti dei media sono tutte le persone fisiche che lavorano per i media, come definiti nel cpv. 1, con mansioni giornalistiche, artistiche o editoriali, su base permanente o come freelance o lavoratori autonomi, retribuiti o non retribuiti. Nel 2008, Rosenthal/Jöhri richiedeva ancora una certa attività professionale ed escludeva i "giornalisti per hobby", il che non può più essere applicato alla luce dell'attuale panorama mediatico.

BIBLIOGRAFIA

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 28 LPD

Un commentario di Samuel Mätzler

CITAZIONE SUGGERITA

Samuel Mätzler, Commentario all'art. 28 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Mätzler, art. 28 LPD N. XXX.

Art. 28 Diritto di farsi consegnare dati o di esigerne la trasmissione a terzi

[1] Chiunque può esigere che i dati personali che lo concernono e che ha comunicato al titolare del trattamento gli siano consegnati in un formato elettronico usuale, se:

a. il titolare tratta i dati personali in modo automatizzato; e

b. il trattamento è effettuato con il consenso della persona interessata oppure in relazione diretta con la conclusione o l'esecuzione di un contratto tra il titolare e la persona interessata.

[2] La persona interessata può inoltre esigere che il titolare del trattamento trasmetta a un altro titolare del trattamento i dati personali che la concernono se sono soddisfatte le condizioni di cui al capoverso 1 e la trasmissione non richiede un onere sproporzionato.

[3] Il titolare del trattamento consegna o trasmette gratuitamente i dati personali. Il Consiglio federale può prevedere eccezioni alla gratuità, segnatamente se la consegna o la trasmissione dei dati personali richiede un onere sproporzionato.

STRUTTURA

In breve 400
I. Osservazioni preliminari 400
II. Considerazioni generali 400
A. Finalità normativa 400
B. Genesi 403
C. Riferimenti di diritto comparato 404
III. Presupposti 404
A. Dati personali degli interessati 404
B. Dati comunicati 405
C. Trattamento automatizzato 407
D. Consenso o nesso diretto con il contratto 407
IV. Conseguenza giuridica: portabilità 409
A. All'interessato (consegna dei dati; comma 1) 409
B. A un responsabile del trattamento (trasferimento dei dati; cpv. 2) 409
C. Formato dei dati 410
1. Diffuso 411
2. In formato elettronico 411
3. Nessun requisito di interoperabilità 412
V. Modalità (cpv. 3 e OPDDa) 413
A. Forma e termine 413
B. Competenza 414
C. Gratuità 415
Bibliografia 415
I materiali 418

IN BREVE

Il diritto alla consegna o al trasferimento dei dati è, insieme al diritto di accesso, il secondo diritto dell'interessato previsto dalla normativa sulla protezione dei dati. Viene spesso definito anche diritto alla portabilità dei dati. Tale diritto consente all'interessato di richiedere la consegna di determinati dati forniti attivamente al titolare del trattamento o da questi raccolti, oppure di farli trasferire direttamente a terzi. I dati devono essere trasferiti in un formato elettronico comunemente utilizzato. Ciò dovrebbe consentire un riutilizzo diretto da parte dell'interessato o di un altro fornitore. Il nuovo diritto alla portabilità dei dati è stato ripreso dal GDPR e si colloca a metà strada tra il diritto alla protezione dei dati e il diritto della concorrenza. Esso mira a fornire all'interessato, nell'ambito dell'economia dei dati, la possibilità di disporre in modo autonomo dei «propri» dati.

I. OSSERVAZIONI PRELIMINARI

1 L'art. 28 della LPD sancisce il diritto dell'interessato alla consegna (cpv. 1) o al trasferimento (cpv. 2) di determinati dati che lo riguardano. Tale diritto è anche denominato **diritto alla portabilità dei dati** e costituisce – insieme al diritto di accesso – il secondo diritto dell'interessato nell'ambito della LPD. L'articolo 29 LPD, che segue, va letto congiuntamente all'articolo 28 LPD e prevede possibili motivi di limitazione.

2 Per l'esercizio dell'art. 28 LPD è **legittimata attivamente** la persona fisica richiedente i cui dati sono trattati da un responsabile del trattamento. È **legittimato passivamente** il responsabile del trattamento che tratta i dati della persona richiedente oggetto del diritto alla portabilità o che ne affida il trattamento a un incaricato. Rientrano in questa categoria i privati e, in rari casi, anche gli organi federali.

II. CONSIDERAZIONI GENERALI

A. Finalità normativa

3 La finalità normativa dell'art. 28 LPD è ancora oggi oggetto di controversia. Mentre, ad esempio, il Consiglio federale vede nel diritto alla portabilità dei

dati la realizzazione di obiettivi di diritto della concorrenza (cfr. N. 10), secondo altre voci della dottrina sono in primo piano obiettivi di tutela dei consumatori o di protezione dei dati. A complicare l'individuazione della finalità normativa si aggiunge il fatto che, durante l'elaborazione della norma, le Camere si sono concentrate sui social network, senza tuttavia prevedere nel diritto alla portabilità dei dati una corrispondente limitazione a tali reti. L'art. 28 LPD può quindi **trovare applicazione in numerose contesti e settori** – ad esempio nel settore della mobilità, in quello sanitario, nelle piattaforme Internet, nei servizi cloud o nella gestione delle risorse umane. L'unico elemento comune a tutti i casi di applicazione è che essi sono riconducibili a cambiamenti fondamentali nel trattamento moderno dei dati (cfr. anche N. 23 e segg.). Solo l'emergere, in tempi recenti, dell'**economia dei dati** ha reso necessario il diritto alla portabilità dei dati. Ciò deve essere preso in considerazione nella finalità della norma.

Dal punto di vista della normativa sulla protezione dei dati, il diritto alla portabilità dell'interessato deve consentire una **gestione autonoma dei dati**. Esso mira a superare la possibilità di esclusione di fatto di cui godrebbe il titolare del trattamento in assenza del diritto alla portabilità e a far sì che la persona, finora degradata a oggetto dei dati, assuma il ruolo di soggetto dei dati, potendo così partecipare alle decisioni relative all'utilizzo dei dati. In questo modo si affrontano gli squilibri tra gli attori generati dall'economia dei dati. L'interessato riceve per la prima volta uno strumento giuridico per intervenire autonomamente nell'economia dei dati e poter partecipare al potenziale dei dati. 4

A ciò sono tuttavia strettamente legate anche **considerazioni di diritto della concorrenza**. A questo proposito, il diritto alla portabilità mira a promuovere la concorrenza in generale e a favorire il libero flusso dei dati. Altri obiettivi spesso citati in letteratura, come la riduzione dei costi di passaggio o delle barriere all'ingresso sul mercato e la prevenzione degli effetti di lock-in, possono invece, secondo l'opinione qui sostenuta, svolgere solo un ruolo secondario: l'art. 28 LPD non si limita ai casi in cui esista o possa semplicemente esistere un effetto di lock-in, e non è necessario dimostrare l'esistenza di barriere all'ingresso nel mercato né la loro riduzione. Inoltre, il responsabile del trattamento non deve necessariamente detenere una posizione di mercato particolare né operare affatto su un mercato. 5

6 In tal modo, gli obiettivi di diritto della concorrenza si discostano da una concezione classica del diritto antitrust e si avvicinano a un «diritto regolamentare» che agisce *ex ante*. A questi obiettivi si fonda inoltre l'idealismo del cosiddetto **Open Web**. Questo movimento, emerso alla fine degli anni 2000, affonda le sue radici nella scena informatica americana e si basa sull'idea che solo la libera collegabilità dei contenuti su Internet (e in particolare nel World Wide Web), nonché l'accesso agli stessi, abbiano reso possibile l'innovazione e abbiano permesso la creazione delle offerte oggi esistenti. Questo Open Web è tuttavia minacciato dai monopoli e dai silos di dati (i cosiddetti «walled gardens»), poiché le grandi piattaforme Internet, in particolare, si isolano sempre più le une dalle altre. Il diritto alla portabilità dei dati va quindi visto, anche a un livello molto più fondamentale, come una reazione a un Internet costituito da «walled gardens». L'economia dei dati – nella sua forma prevalente nel World Wide Web – deve essere liberata dai silos di dati proprietari e gli interessati devono poter cambiare fornitore senza ostacoli che distorcano la concorrenza.

7 Data l'ampiezza dei possibili casi d'uso, gli obiettivi citati, talvolta molto diversi tra loro, non sono sempre facilmente conciliabili. Alla luce di quanto detto, il diritto alla portabilità dei dati persegue tuttavia obiettivi sia in materia di protezione dei dati che di diritto della concorrenza. Tuttavia, esso va **considerato principalmente come uno strumento di protezione dei dati** che persegue *anche* obiettivi di diritto della concorrenza. Ciò deriva sistematicamente dal fatto che il diritto alla portabilità riguarda solo i dati personali e può essere esercitato esclusivamente dagli interessati (ai sensi della normativa sulla protezione dei dati). Di conseguenza, è evidente il nesso con la personalità dell'interessato e la sua autodeterminazione informativa. Viceversa, non è necessario che siano soddisfatti requisiti di diritto della concorrenza affinché il diritto possa essere esercitato. Non è nemmeno necessario che il responsabile del trattamento operi su un mercato o in modo rilevante ai fini della concorrenza.

8 Di conseguenza, il diritto alla portabilità dei dati nel diritto sulla protezione dei dati **non è** (come talvolta sostenuto) **estraneo al sistema, bensì «costruttrice del sistema»**. È espressione di una decisione di principio del legislatore, secondo cui l'interessato deve avere la possibilità di partecipare alle decisioni relative ai dati che lo riguardano. Con il suo inserimento nella

LPD, il legislatore ha chiarito che in futuro l'attenzione dovrà essere posta sull'interessato.

Proprio alla luce della storia della sua genesi in Svizzera, non proprio lineare (ne parleremo tra poco), il diritto alla portabilità dei dati va inteso anche in un contesto più ampio: si tratta di uno strumento della **politica svizzera in materia di dati** per eccellenza e non «solo» di uno strumento di diritto della protezione dei dati. Il diritto alla portabilità deriva da considerazioni di fondo relative alla politica in materia di dati e mira a consentire un libero flusso di dati nell'era dell'economia dei dati. In questo senso, pur potendo essere – come ora è avvenuto – disciplinato dal diritto sulla protezione dei dati, non deve necessariamente avere uno stretto legame con la LPD. Già all'inizio delle deliberazioni sulla revisione della LPD, la portavoce della commissione competente aveva infatti giustamente osservato: «Non si tratta semplicemente di protezione dei dati, ma anche di altre questioni relative alla politica dei dati, come la portabilità ecc., di cui dobbiamo [...] occuparci.» 9

B. Genesi

L'art. 28 della LPD non ha alcun corrispondente nell'aDSG precedente. Si tratta di una vera e propria novità della revisione, ripresa dal DSGVO (cfr. N. 12) . La sua **introduzione, tuttavia, è rimasta incerta fino all'ultimo**: il Consiglio federale riteneva «problematica» una normativa in tal senso e ha rinunciato a inserire un diritto alla portabilità dei dati nel (pre)progetto. Ha motivato questa scelta sostenendo che un tale diritto fosse finalizzato più a consentire agli interessati il riutilizzo dei propri dati, per favorire la concorrenza, che a tutelare la loro personalità. Inoltre, temeva costi elevati e nutriva dubbi sul successo dell'attuazione, poiché sarebbe stato necessario un accordo tra i responsabili in merito ai supporti dati e agli standard informatici. Il Consiglio federale intendeva invece valutare l'introduzione di diritti di portabilità specifici per settore. 10

Nelle **deliberazioni parlamentari**, tuttavia, la Commissione delle istituzioni politiche del Consiglio nazionale (CIP-N) ha comunque inserito nel progetto un diritto generale alla portabilità dei dati. Ciò avrebbe dovuto aprire nuovi spazi economici e modificare l'equilibrio di potere tra piattaforme piccole e grandi. Una minoranza ha inoltre chiesto di ampliare ulteriormente la portata di tale diritto, sottoponendo alla portabilità tutti i dati relativi a una persona. La maggioranza del Consiglio nazionale e anche il Consiglio federale 11

ritenevano tuttavia che un tale diritto sarebbe andato troppo oltre, in considerazione dei possibili problemi relativi ai segreti d'affari. Infine, le Camere hanno deciso di sancire il diritto alla portabilità nella sua forma attuale, «sempre tenendo presente ciò che ne comprometterà l'adeguatezza e ciò che invece non lo farà».

C. Riferimenti di diritto comparato

12 Il diritto alla portabilità dei dati è stato **ripreso dalla DSGVO** praticamente senza modifiche, motivo per cui la normativa ivi contenuta nell'art. 20 della DSGVO può essere presa come riferimento per l'interpretazione svizzera. Esistono tuttavia alcune differenze specifiche nella formulazione, sulle quali – ove pertinente – occorre soffermarsi in relazione ai singoli presupposti.

III. PRESUPPOSTI

A. Dati personali degli interessati

13 L'art. 28 cpv. 1 LPD prevede innanzitutto che l'interessato possa richiedere al responsabile del trattamento la consegna dei «propri dati personali». Ne consegue che solo i dati che si riferiscono a una **persona fisica** sono portabili (art. 2 cpv. 1 e art. 5 lett. a LPD). Pertanto, i dati privi di riferimento all'interessato non rientrano nell'ambito di applicazione, a meno che il titolare del trattamento non sia in grado di collegarli a quest'ultimo. Si possono citare, ad esempio, le metriche di prestazione anonime relative al software, quali i dati sul carico della CPU o sul consumo di memoria sul dispositivo di un'utente. È quindi richiesta una stretta correlazione tra i dati e la personalità dell'interessato.

14 Di conseguenza, i dati relativi a persone giuridiche non sono soggetti al diritto alla portabilità. Non rientrano nell'ambito di applicazione nemmeno i dati che un responsabile del trattamento **anonimizza a posteriori**. Se si tratta di dati pseudonimizzati, questi devono essere considerati dati personali qualora il responsabile del trattamento possa collegarli all'interessato.

15 Come evidenziano le versioni in lingua latina, i dati devono riferirsi alla persona che presenta la richiesta. Non è invece possibile trarre alcuna conclusione dalla formulazione ambigua della versione in lingua tedesca («i suoi dati personali»), che consentirebbe anche un'interpretazione diversa e

più ampia. Ne consegue che **i dati puramente relativi a terzi**, ovvero i dati che si riferiscono esclusivamente a terzi, non sono soggetti al diritto alla portabilità.

È tuttavia controverso come si debba procedere nel caso di dati che si riferiscono *anche* a terzi, ad esempio foto in cui sono ritratte più persone. Poiché i motivi di limitazione del diritto alla portabilità dei dati di cui all'art. 29 cpv. 1 in combinato disposto con l'art. 26 cpv. 1 lett. b LPD fanno riferimento a interessi prevalenti di terzi, si deve presumere che i dati personali che si riferiscono anche a terzi possano essere soggetti al diritto alla portabilità. Rientrano quindi anche i **dati con un «doppio riferimento»**, che presentano una certa vicinanza alla persona interessata, anche se i dati non si riferiscono (solo) a quest'ultima. Ciò vale, ad esempio, per intere cronologie di chat o e-mail o per transazioni bancarie archiviate (comprese le informazioni sui debitori o sui beneficiari). Solo in presenza di interessi prevalenti di terzi (o qualora si tratti di dati che riguardano esclusivamente terzi) i dati non sono soggetti al diritto alla portabilità dei dati. Se così non fosse, l'art. 28 LPD risulterebbe privo di effetto proprio in molti dei casi previsti dallo scopo della norma. 16

Pertanto, per determinare se determinati dati siano soggetti al diritto alla portabilità, occorre procedere come segue: in una prima fase, il responsabile del trattamento deve verificare se, in generale, siano soddisfatti i requisiti di cui all'art. 28 LPD, in particolare se i dati personali in questione siano stati comunicati dall'interessato. Se i dati riguardano *anche* terzi (ma non *solo* terzi) e presentano un doppio riferimento, in una seconda fase occorre valutare, nel senso di un «correttivo restrittivo», se interessi prevalenti di terzi rendano necessaria una limitazione. In assenza di interessi prevalenti del terzo, i dati possono essere trasferiti. 17

B. Dati comunicati

Il diritto alla portabilità dei dati è limitato ai dati che l'interessato ha «comunicato» al responsabile del trattamento. Il concetto di comunicazione **non va inteso ai sensi della definizione giuridica di cui all'art. 5 lett. e LPD**. Ciò non è tuttavia necessario ai fini della sua interpretazione: già durante l'iter legislativo è stato precisato, nei materiali preparatori, a quali dati ci si riferisse. Il Consiglio federale ha poi definito il contenuto di tale caratteristica nell'OPDa. Inoltre, l'Ufficio federale di giustizia (UFG) si è 18

espresso in merito a tale contenuto nelle sue note esplicative. Per questo motivo, il requisito della comunicazione in Svizzera (a differenza di quanto previsto dalla DSGVO) è, almeno in teoria, ampiamente indiscusso. Nella pratica, tuttavia, possono sorgere difficili questioni di delimitazione.

19 Ai sensi dell'art. 20 cpv. 1 lett. a OPDDa, sono considerati comunicati innanzitutto i dati che un interessato mette a disposizione del responsabile del trattamento consapevolmente e volontariamente (**i cosiddetti dati anagrafici; anche «provided data**»). Sono inclusi tutti i dati comunicati direttamente e consapevolmente, ad esempio i dati di indirizzo inseriti nell'ambito di un ordine online o i dati che devono essere forniti in occasione di una registrazione su una piattaforma o su un questionario anamnestico in ospedale. Le password o le chiavi private non rientrano in questa categoria, a condizione che – come dovrebbe essere la norma – siano crittografate e non possano essere associate dall'amministratore all'interessato.

20 Inoltre, i dati si considerano comunicati quando un amministratore li ha raccolti sull'interessato e sul suo comportamento nell'ambito dell'utilizzo di un servizio o di un dispositivo (art. 20 cpv. 1 lett. b OPDa) . Tali **dati osservati (anche «observed data»)** vengono generati – consapevolmente o inconsapevolmente – dall'interessato in modo indiretto durante l'utilizzo di un servizio o di un dispositivo. Rientrano in questa categoria, ad esempio, i valori di un'app di fitness su uno smartwatch, generati in base alla prestazione sportiva, i brani musicali ascoltati su un servizio di streaming o i dati relativi al consumo e alla posizione di un veicolo intelligente.

21 Non rientrano in questa categoria i **dati derivati (anche «derived data»)**, ovvero i dati che il titolare del trattamento genera attraverso la propria valutazione dei dati (art. 20 cpv. 2 OPDDa). Poiché questi rappresentano una prestazione autonoma del titolare del trattamento, sono esclusi dal diritto alla portabilità. In questo caso, il legislatore ha attribuito maggiore importanza alla tutela dell'attività autonoma e dei propri investimenti rispetto al diritto dell'interessato di consentire un riutilizzo dei «propri» dati personali.

22 La distinzione tra dati osservati e dati derivati va effettuata caso per caso e potrebbe non essere sempre semplice. Ad esempio, nel settore sanitario «osservare» significa per lo più anche «misurare», e dietro una semplice misurazione si cela spesso una tecnologia complessa che opera secondo

metodi scientifici. In questi casi, il passaggio dalla pura osservazione alla derivazione può essere fluido e difficile da individuare.

C. Trattamento automatizzato

Un'ulteriore limitazione consiste nel fatto che solo i dati trattati in modo automatizzato dal responsabile del trattamento sono soggetti al diritto alla portabilità dei dati (art. 28 cpv. 1 lett. a LPD). Ciò mira principalmente a escludere i dati **conservati in formato cartaceo**. Si pensi, ad esempio, ai moduli cartacei di anamnesi presenti in uno studio medico, purché questi non vengano successivamente trasferiti in una cartella clinica elettronica. 23

Sono contemplati solo i **dati trattati elettronicamente**. Infatti, nonostante la neutralità tecnologica intrinseca della LPD, il diritto alla portabilità dei dati è finalizzato al traffico digitale e trova applicazione in particolare al traffico di dati su Internet. Tuttavia, tale presupposto oggi **non rappresenta quasi più una limitazione**, poiché la maggior parte dei trattamenti dei dati avviene presumibilmente in modo automatizzato. 24

Il titolare del trattamento non ha l'obbligo di digitalizzare i dati conservati in formato cartaceo o in altra forma analogica. Tuttavia, se i dati vengono trattati **solo parzialmente in modo automatizzato**, il titolare del trattamento può essere obbligato, in singoli casi, a trasferire tali dati, poiché la limitazione non fa riferimento a un trattamento esclusivamente automatizzato. Poiché in questo caso deve fornire o trasmettere i dati in un formato elettronico comunemente utilizzato, possono sussistere ulteriori obblighi a suo carico. 25

D. Consenso o nesso diretto con il contratto

Come ulteriore presupposto, l'art. 28 LPD prevede una limitazione ai dati trattati con il consenso dell'interessato o in nesso diretto con la stipula o l'esecuzione di un contratto tra il responsabile del trattamento e l'interessato (cpv. 1, lett. b). Tale presupposto fa riferimento ai **motivi giustificativi per il trattamento dei dati di cui all'art. 31 LPD** ed è stato ripreso *tel quel* dalla DSGVO. 26

Tuttavia, la DSGVO si basa sul principio del divieto con riserva di autorizzazione. In Svizzera, invece, il trattamento dei dati da parte di privati è in linea di principio consentito, purché non vi sia una violazione illecita della personalità dell'interessato (autorizzazione con riserva di divieto). Di 27

conseguenza, ai sensi della LPD non è richiesto in ogni caso un motivo giustificativo ai sensi dell'art. 31 LPD per il trattamento dei dati da parte di privati. Piuttosto, un trattamento dei dati non può **nemmeno ledere illecitamente** la personalità dell'interessato, ad esempio perché avviene in conformità con i principi di protezione dei dati (art. 30 cpv. 1 e cpv. 2 lett. a LPD *e contrario*). Ciò tuttavia non tiene conto del presupposto di cui all'art. 28 cpv. 1 lett. b LPD.

28 Un'interpretazione letterale comporterebbe quindi che solo i trattamenti di dati siano soggetti al diritto alla portabilità qualora possano fondarsi sui motivi giustificativi del consenso (art. 31 cpv. 1 variante 1 LPD) o dell'interesse prevalente in ragione di un nesso diretto con un contratto (art. 31 cpv. 2 lett. a LPD). Ciò garantirebbe certamente che i trattamenti di dati basati su un obbligo legale non rientrino nel diritto alla portabilità dei dati. Tuttavia, non si ravvisa alcun motivo per cui **i trattamenti di dati che non necessitano di una base giustificativa** dovrebbero essere esclusi dalla portabilità.

29 Nella dottrina si ipotizza quindi una negligenza legislativa e, alla luce della finalità della norma, si sostiene un'interpretazione più ampia. Si dovrebbe quindi fare riferimento alla **volontarietà del trattamento dei dati**. Di conseguenza, l'iniziativa per il trattamento concreto dei dati deve provenire almeno (anche) dall'interessato. Il trattamento dei dati non deve avvenire in modo completamente slegato dalla volontà degli interessati. Se ciò avviene, il presupposto di cui all'art. 28 cpv. 1 lett. b LPD deve essere considerato soddisfatto, indipendentemente dal fatto che venga invocato un motivo giustificativo ai sensi dell'art. 31 LPD.

30 A contrario, ciò significa che i trattamenti di dati che si basano su un altro motivo giustificativo non sono soggetti al diritto alla portabilità dei dati. Ciò è rilevante in particolare quando esiste una base legale per il trattamento dei dati (art. 31 cpv. 1 variante 3 LPD). Mentre la DSGVO prevede un'esplicita esclusione dei trattamenti nell'esercizio di funzioni pubbliche (art. 20 cpv. 3, seconda frase, DSGVO), ciò non avviene ai sensi della LPD. Tuttavia, già la limitazione di cui all'art. 28 cpv. 1 lett. b LPD chiarisce che i trattamenti di dati basati su una **base giuridica** sono in linea di principio esclusi. Di conseguenza, i trattamenti di dati effettuati da organi federali, vincolati al principio di legalità, non rientrano di norma nel diritto alla portabilità dei dati.

IV. CONSEGUENZA GIURIDICA: PORTABILITÀ

Se i presupposti di cui al punto III sono soddisfatti cumulativamente, l'interessato può richiedere la consegna dei dati a sé stesso (cpv. 1) o il trasferimento a un altro titolare del trattamento (cpv. 2). Sia la consegna che il trasferimento dei dati devono avvenire in un formato elettronico comunemente utilizzato (cfr. N. 38 e segg.). 31

L'esercizio del diritto alla portabilità non modifica il **rapporto giuridico** dell'interessato con il titolare del trattamento. Il consenso già prestato non si considera revocato, né subisce modifiche l'eventuale rapporto contrattuale tra le parti. Il titolare del trattamento può continuare a far valere motivi di giustificazione. Di conseguenza, non è tenuto a cancellare i dati trasferiti. 32

A. All'interessato (consegna dei dati; comma 1)

Ai sensi dell'art. 28 cpv. 1 LPD, il responsabile del trattamento consegna i dati **all'interessato**. Quest'ultimo può quindi utilizzare i dati per uso puramente personale (ad esempio salvando una raccolta di foto sul proprio computer) oppure trasmetterli autonomamente a un terzo di sua scelta. Quest'ultima operazione, tuttavia, non si basa sull'art. 28 LPD. 33

B. A un responsabile del trattamento (trasferimento dei dati; cpv. 2)

Ai sensi dell'art. 28 cpv. 2 LPD, su richiesta dell'interessato è possibile anche un **trasferimento diretto a terzi** (definiti nell'art. 28 come «altro responsabile del trattamento»). A tal fine devono innanzitutto essere soddisfatti tutti i requisiti di cui al cpv. 1. Inoltre, il trasferimento non deve comportare uno sforzo sproporzionato. Il cpv. 2 è soddisfatto se il terzo può ottenere i dati direttamente dal titolare del trattamento passivamente legittimato, ad esempio perché quest'ultimo gli concede l'accesso tramite un'interfaccia di programmazione (API). Non sussiste tuttavia alcun diritto in tal senso. 34

L'art. 21 cpv. 3 OPD precisa che sussiste un onere sproporzionato qualora il **trasferimento non sia tecnicamente possibile**. Tale impossibilità, tuttavia, difficilmente si verificherebbe, poiché la consegna dei dati all'interessato non è, dal punto di vista tecnico, né più semplice né più complessa del 35

trasferimento dei dati a un altro responsabile del trattamento. Poiché il responsabile del trattamento è tenuto per legge a consegnare i dati ai sensi del cpv. 1, anche un trasferimento dei dati ai sensi del cpv. 2 dovrebbe essere regolarmente possibile (senza un onere sproporzionato). Ciò vale a maggior ragione in quanto il responsabile del trattamento deve progettare i propri sistemi sin dall'inizio in modo tale da poter adempiere ai propri obblighi di legge (art. 7 LPD).

36 Naturalmente, un terzo non è tenuto a ricevere i dati né a garantire la fattibilità tecnica del trasferimento. A lui non spetta **alcun ruolo ai sensi della normativa sulla protezione dei dati** fintantoché non abbia ricevuto dati personali e, di conseguenza, non li tratti. In tal senso, la denominazione di «altro titolare del trattamento» nella legge è fuorviante, tanto più che l'art. 28 LPD – a differenza dell'art. 20 DSGVO – non prevede un divieto di ostacolo che imporrebbe all'«altro titolare del trattamento» un obbligo in relazione al diritto alla portabilità dei dati. Ai sensi della normativa UE si sostiene pertanto che la fattibilità tecnica debba riferirsi al rapporto tra il responsabile del trattamento e il terzo. Un trasferimento sarebbe sempre sproporzionato qualora i sistemi di trattamento dei dati del responsabile del trattamento e del terzo non fossero compatibili. Il presupposto si riferisce quindi a una caratteristica del terzo, senza attribuirgli alcun obbligo.

37 Dai costi sostenuti dal titolare del trattamento non si può dedurre alcun onere sproporzionato. Il diritto alla portabilità dei dati è un diritto dell'interessato che deve essere garantito a prescindere da eventuali costi di implementazione. I costi sostenuti per il trasferimento a un terzo non possono quindi essere addotti come argomentazione, soprattutto poiché non è chiaro in che misura tale trasferimento debba comportare costi superiori rispetto alla consegna all'interessato.

C. Formato dei dati

38 L'art. 28 LPD prevede la consegna o il trasferimento in un **formato elettronico comunemente utilizzato**. Si tratta di formati che consentono di trasferire i dati con un onere proporzionato e di riutilizzarli da parte dell'interessato o di un altro responsabile del trattamento (cfr. art. 21 cpv. 1 OPDa).

Poiché questa precisazione è di scarsa utilità, **occorre fare riferimento alla disposizione dell'art. 20 della DSGVO**, anche se la formulazione svizzera si è orientata piuttosto a quella relativa al diritto di accesso di cui all'art. 15 cpv. 3 della DSGVO. L'art. 20 della DSGVO parla di un «formato strutturato, comunemente utilizzato e leggibile da dispositivo automatico». 39

1. Diffuso

Un formato è diffuso se è ampiamente utilizzato nel settore di riferimento per il tipo di dati in questione e nell'area geografica pertinente. Tuttavia, non occorre attribuire un'importanza eccessiva all'area geografica. Nell'economia globalizzata dei dati, la Svizzera non è un'isola tecnologica e il requisito della diffusione risulterebbe così inutilmente elevato. La diffusione non corrisponde nemmeno allo stato dell'arte. Ciò che conta non è quale formato appaia «migliore», ma quale **sia il più diffuso** e si sia quindi dimostrato efficace nella pratica. Di conseguenza, un formato è considerato diffuso quando si è affermato come standard. Occorre quindi fare riferimento principalmente agli standard e alle consuetudini del settore. 40

Fanno eccezione, tuttavia, i **formati proprietari**, che pur essendo eventualmente diffusi, possono essere concessi in licenza solo a costi elevati. Essi non sono da considerarsi diffusi, così come i formati utilizzati esclusivamente a livello interno. Viceversa, **i formati aperti non sono di per sé diffusi**, ma devono essere di uso comune e ampiamente diffusi. Se in un determinato settore non esistono (ancora) formati diffusi, il responsabile dovrebbe ricorrere a formati aperti di uso comune, quali XML, JSON o CSV. 41

La diffusione va valutata dal **punto di vista del responsabile con legittimazione passiva**: un file DICOM (acronimo di Digital Imaging and Communications in Medicine, con estensione .dcm) può risultare insolito per una paziente, ma è diffuso in radiologia. Ciò vale anche se il responsabile opera in un settore diverso da quello del terzo a cui devono essere trasferiti i dati. Ciò può tuttavia rappresentare un ostacolo concreto al trasferimento intersettoriale. 42

2. In formato elettronico

Un formato elettronico corrisponde, in sostanza, alla leggibilità automatica ai sensi della DSGVO. In tale contesto, la leggibilità automatica è considerata un vero e proprio «requisito formale» per la società digitale, poiché solo essa 43

consente il trattamento automatizzato delle informazioni tramite computer. Poiché il diritto alla portabilità dei dati è finalizzato all'economia dei dati, il formato deve garantire l'importazione automatica dei dati in un sistema informatico in forma strutturata. I dati devono quindi essere **elaborabili elettronicamente** e poter essere ulteriormente trattati in modo automatizzato.

44 In alcuni casi specifici, tuttavia, la normativa svizzera può essere più restrittiva rispetto al concetto di leggibilità automatica. Mentre nell'ambito della DSGVO si discute talvolta se le stampe cartacee debbano essere considerate leggibili automaticamente in virtù della possibilità tecnica del riconoscimento ottico dei caratteri (cosiddetto optical character recognition; OCR), ai sensi della LPD queste non sono chiaramente classificabili come formato elettronico.

3. Nessun requisito di interoperabilità

45 Dalle disposizioni relative al formato dei dati non deriva alcun requisito di interoperabilità. L'interoperabilità non si riferisce comunque ai dati (o ai loro formati), bensì ai sistemi che sono coinvolti in uno scambio bidirezionale. A tal fine sarebbe quindi necessario non solo lo scambio di dati, ma anche l'**interazione tra sistemi diversi**. Ad esempio, un social network potrebbe consentire a un'utente di trasferire le proprie foto su un'altra piattaforma. L'interoperabilità tra due social network sarebbe invece raggiunta solo se, ad esempio, un commento sotto una foto potesse essere visualizzato su un altro social network e fosse possibile interagire con esso (ad esempio tramite un nuovo commento). I diversi sistemi devono quindi non solo essere in grado di scambiare dati, ma anche concordare quali condizioni si applicano a tali dati.

46 L'art. 21 cpv. 2 dell'OPDa chiarisce in tal senso che il diritto alla portabilità **non comporta alcun obbligo** per il responsabile del trattamento di adottare o mantenere sistemi di trattamento dei dati tecnicamente compatibili. Tale obbligo non sussiste ovviamente nemmeno per i terzi, che non sono tenuti a ricevere i dati trasferiti. Neppure dalle disposizioni della LPD e dell'OPDa deriva l'obbligo di garantire l'interoperabilità tra i sistemi.

47 Nelle sue note esplicative, l'UFJ suggerisce inoltre che le informazioni trasmesse debbano essere descritte in modo preciso in formati interoperabili con metadati adeguati e comprensibili, affinché possano essere trasferite in modo sensato in un nuovo sistema. I metadati devono essere sufficientemente

esaustivi da consentire l'utilizzo e il riutilizzo dei dati senza rivelare segreti d'affari. Ciò suggerisce un obbligo di elaborazione di (nuovi) metadati, che non va seguito. L'art. 28 LPD sancisce semplicemente, e proprio anche alla luce dell'art. 21 cpv. 2 OPDDa, un**diritto ai dati** *«as is».* Ciò comprende anche eventuali metadati che consentono, ad esempio, di strutturare un insieme di dati più ampio. Da ciò non si può tuttavia dedurre un obbligo di integrare i metadati (talvolta con dati di cui il responsabile del trattamento potrebbe non aver affatto bisogno nel proprio sistema). Ciò soprattutto perché la normativa svizzera, a differenza dell'art. 20 della DSGVO, non menziona espressamente la strutturazione come requisito. Inoltre, a seconda del formato (comune) utilizzato, può variare quali metadati possano tecnicamente essere contenuti in un formato. Devono quindi essere forniti solo quei metadati degli interessati che sono contenuti in un formato elettronico comune ai sensi dell'art. 28 LPD.

V. MODALITÀ (CPV. 3 E OPDDA)

L'art. 28 cpv. 3 LPD prevede che il responsabile del trattamento debba, in linea di principio, trasferire i dati personali a titolo gratuito. Inoltre, l'art. 22 OPDa precisa i termini, la competenza e ulteriori modalità. L'art. 22 OPDa si limita tuttavia a fare riferimento, per analogia, alle **modalità del diritto di accesso**, senza affrontare nel merito il diritto alla portabilità dei dati. In linea di principio è quindi possibile fare riferimento alle considerazioni relative al diritto di accesso. 48

A. Forma e termine

L'art. 22 in combinato disposto con l'art. 16 cpv. 1 OPD richiede all'interessato una **richiesta scritta**. In essa l'interessato deve identificarsi (art. 22 in combinato disposto con l'art. 16 cpv. 5 OPD). Ciò è possibile, ad esempio, allegando alla richiesta una copia del documento d'identità. Più frequentemente, tuttavia, l'identificazione dovrebbe avvenire quando l'interessato presenta la richiesta **direttamente dal proprio account (dopo aver effettuato l'accesso)** presso il titolare del trattamento. In questi casi, tuttavia, il titolare del trattamento dovrebbe adottare misure particolari in considerazione dei requisiti in materia di sicurezza dei dati (ad esempio implementando meccanismi per il rilevamento di tentativi di accesso insoliti da indirizzi IP estranei). Previo consenso del responsabile del trattamento, la 49

richiesta può essere presentata anche verbalmente, cosa che tuttavia dovrebbe verificarsi raramente.

50 Il trasferimento deve avvenire **entro 30 giorni dal ricevimento della richiesta** (art. 22 in combinato disposto con l'art. 18 cpv. 1 OPD). Se il trasferimento non può avvenire entro tale termine, il responsabile del trattamento deve informarne l'interessato e comunicargli entro quale termine potrà avvenire il trasferimento (art. 22 in combinato disposto con l'art. 18 cpv. 2 OPDDa). Anche un'eventuale limitazione deve essere comunicata entro lo stesso termine (art. 22 in combinato disposto con l'art. 18 cpv. 3 OPDDa).

51 Non è dovuto un flusso di dati continuo o periodico. Il responsabile del trattamento non è tenuto a garantire nemmeno un accesso illimitato ai dati da parte dell'interessato o dell'altro responsabile del trattamento (ad esempio tramite l'accesso a un'interfaccia). Il diritto alla portabilità dei dati è concepito come **meccanismo di trasferimento statico** e fornisce quindi solo un'«istantanea».

52 Come il diritto di accesso, anche il diritto alla portabilità dei dati può quindi essere garantito, in linea di principio, **in qualsiasi forma**. È possibile, ad esempio, l'invio postale di una chiavetta USB o l'invio elettronico tramite e-mail. È inoltre possibile, soprattutto nel caso di insiemi di dati di grandi dimensioni, che il titolare del trattamento offra un collegamento a un'API o la possibilità di scaricare i dati direttamente dai propri server (ad esempio da un server SFTP, da un'interfaccia web sicura o da un portale web).

B. Competenza

53 Il diritto alla portabilità dei dati è rivolto **al titolare del trattamento**, anche se i dati sono conservati presso un responsabile del trattamento. In caso di pluralità di titolari, l'interessato può far valere il proprio diritto nei confronti di ciascuno di essi (art. 22 in combinato disposto con l'art. 17 cpv. 1 OPDDa). I titolari del trattamento sono tenuti a trattare la richiesta e non semplicemente a inoltrarla. I responsabili del trattamento devono assistere il titolare del trattamento nel rispondere alla richiesta oppure rispondere essi stessi, per conto del titolare del trattamento (art. 22 in combinato disposto con l'art. 17 cpv. 2 OPDa). Il responsabile del trattamento deve quindi fornire al titolare del trattamento i dati rilevanti ai fini della portabilità, qualora quest'ultimo non ne disponga direttamente.

C. Gratuità

Il titolare del trattamento deve consegnare o trasferire i dati **gratuitamente** (art. 28 cpv. 3 LPD). In via eccezionale è **ammesso un contributo fino a CHF 300**, qualora il trasferimento comporti un onere sproporzionato (art. 22 in combinato disposto con l'art. 19 cpv. 1 e 2 OPDDa). Ciò può verificarsi, ad esempio, nel (raro) caso in cui sia necessaria una complessa selezione tra i dati di terzi e quelli dell'interessato. L'importo del contributo deve essere comunicato preventivamente dal responsabile del trattamento all'interessato (art. 22 in combinato disposto con l'art. 19 cpv. 3 OPDDa). 54

Nota:

La struttura e il contenuto del presente commento si basano sulla tesi di dottorato dell'autore sul diritto alla portabilità dei dati. Nelle note a piè di pagina si fa riferimento specifico a tale tesi solo quando vi si trovano approfondimenti in merito.

BIBLIOGRAFIA

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.

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 29 LPD

Un commentario di Samuel Mätzler

CITAZIONE SUGGERITA

Samuel Mätzler, Commentario all'art. 29 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Mätzler, art. 29 LPD N. XXX.

Art. 29 Restrizioni del diritto di farsi consegnare dati o di esigerne la trasmissione a terzi

[1] Il titolare del trattamento può rifiutare, limitare o differire la consegna o la trasmissione dei dati personali per i motivi di cui all'articolo 26 capoversi 1 e 2.

[2] Il titolare del trattamento indica il motivo per cui rifiuta, limita o differisce la consegna o la trasmissione.

STRUTTURA

In breve 423
I. Considerazioni generali 423
A. Finalità normativa e contesto 423
B. Riferimenti di diritto comparato 424
II. Motivi di limitazione (cpv. 1 in combinato disposto con l'art. 26) 424
A. Base giuridica, in particolare il segreto professionale (art. 26, cpv. 1, lett. a) 424
B. Interessi prevalenti di terzi (art. 26 cpv. 1 lett. b) 425
C. Manifesta infondatezza (art. 26 cpv. 1 lett. c) 425
D. Ulteriori motivi di limitazione (art. 26 cpv. 2) 426
III. Conseguenze giuridiche 427
IV. Obbligo di motivazione (cpv. 2) 427
Bibliografia 428
I materiali 429

IN BREVE

L'art. 29 della LPD illustra i possibili motivi di limitazione del diritto alla consegna o al trasferimento dei dati ai sensi dell'art. 28 della LPD. A tal proposito si fa riferimento ai motivi di limitazione del diritto di accesso. Ciò ha lo scopo di impedire che l'interessato possa, avvalendosi del diritto alla portabilità dei dati, ottenere dati che non sono soggetti al diritto di accesso. Tuttavia, il riferimento generico al diritto di accesso non tiene sufficientemente conto delle caratteristiche del diritto alla portabilità dei dati, il che può portare a incongruenze in diversi casi.

I. CONSIDERAZIONI GENERALI

A. Finalità normativa e contesto

L'art. 29 della LPD stabilisce per quali motivi un responsabile del trattamento possa limitare la consegna o il trasferimento dei dati ai sensi dell'art. 28 della LPD (denominato anche diritto alla portabilità dei dati). La disposizione, tuttavia, non elenca tali motivi in modo autonomo, ma rimanda ai **motivi di limitazione del diritto di accesso** di cui all'art. 26, cpv. 1 e 2, LPD. Per questo motivo, le considerazioni ivi contenute possono essere in gran parte applicate al diritto alla portabilità. 1

Il rinvio generico ai motivi di limitazione del diritto di accesso non è privo di controversie, poiché i due diritti degli interessati **perseguono obiettivi diversi** e i motivi di limitazione non sempre si adattano ai **diversi casi di applicazione**. Tuttavia, tale rinvio consente almeno di impedire che le limitazioni del diritto di accesso possano essere aggirate avvalendosi del diritto alla portabilità dei dati. 2

Insieme al diritto alla portabilità dei dati, l'art. 29 LPD è stato inserito in occasione della revisione della LPD solo nel corso della **discussione parlamentare**. La disposizione non è stata oggetto di discussione separata ed era incontestata. 3

B. Riferimenti di diritto comparato

4 L'art. 29 LPD è stato ripreso **per analogia dalla DSGVO**. Tuttavia, la DSGVO non prevede una disposizione specifica. Al contrario, la DSGVO limita il diritto alla portabilità dei dati in diversi punti. Ai sensi dell'art. 12, cpv. 5, comma 1 della DSGVO, il titolare del trattamento può subordinare il trasferimento dei dati al pagamento di un corrispettivo adeguato in caso di richieste manifestamente infondate o eccessive (lett. a) oppure rifiutarlo del tutto (lett. b). A tal fine, spetta a lui fornire la prova del carattere abusivo della richiesta (art. 12, cpv. 5, comma 2 della DSGVO).

5 Ai sensi dell'art. 20, cpv. 4 della DSGVO, il diritto alla portabilità non deve pregiudicare i **diritti e le libertà di altre persone**. Secondo l'opinione prevalente, ciò riguarda anche il titolare del trattamento. Pertanto, il diritto alla portabilità ai sensi della DSGVO può essere limitato da segreti aziendali e commerciali o dalla proprietà intellettuale, come ad esempio i diritti d'autore.

6 Inoltre, la DSGVO contiene, all'art. 20, cpv. 3, seconda frase, un **esplicito esclusione** per i trattamenti che sono nell'interesse pubblico o effettuati nell'esercizio di pubblici poteri. Inoltre, alle condizioni di cui all'art. 23 della DSGVO, nel diritto dell'Unione o in quello di uno Stato membro possono essere previste ulteriori limitazioni. In conformità con l'art. 85, cpv. 2, e l'art. 89, cpv. 3, della DSGVO, sono inoltre possibili ulteriori deroghe che possono limitare il diritto alla portabilità dei dati in determinate circostanze.

II. MOTIVI DI LIMITAZIONE (CPV. 1 IN COMBINATO DISPOSTO CON L'ART. 26)

A. Base giuridica, in particolare il segreto professionale (art. 26, cpv. 1, lett. a)

7 Una limitazione del diritto alla portabilità dei dati è ammessa se prevista da una legge in senso formale (art. 29 cpv. 1 in combinato disposto con l'art. 26 cpv. 1 lett. a LPD). Tale base legale deve riferirsi al diritto alla portabilità dei dati e andrebbe **valutata caso per caso**. Finora, tuttavia, non esistono basi legali corrispondenti.

8 La disposizione relativa al diritto di accesso cita a titolo esemplificativo la tutela del segreto professionale. Ciò evidenzia che il riferimento al diritto di

accesso **non è molto convincente**, poiché il diritto alla portabilità riguarda solo i dati che si riferiscono all'interessato e che sono stati da lui stesso comunicati al titolare del trattamento. I segreti professionali, invece, hanno lo scopo primario di proteggere proprio l'interessato. Poiché l'interessato esercita sempre il proprio diritto alla portabilità di propria iniziativa e, di conseguenza, sussiste il consenso, il segreto professionale non viene violato (cfr. art. 321 n. 2 CP).

B. Interessi prevalenti di terzi (art. 26 cpv. 1 lett. b)

Il titolare del trattamento può limitare il diritto alla portabilità qualora ciò sia necessario in ragione di interessi prevalenti di terzi (art. 29 cpv. 1 in combinato disposto con l'art. 26 cpv. 1 lett. b LPD). In questo contesto è in primo piano il **doppio o il triplo riferimento** dei dati, ma sono ipotizzabili anche segreti d'affari o diritti di proprietà intellettuale di terzi. Le limitazioni basate sugli interessi del titolare del trattamento devono invece essere valutate ai sensi dell'art. 26 cpv. 2 LPD. 9

Per quanto riguarda gli interessi di terzi, è necessario effettuare una **valutazione comparativa degli interessi**. Non si dovrebbe presumere a cuor leggero che gli interessi di terzi prevalgano: i dati in questione sono sempre quelli che si riferiscono (almeno in parte) all'interessato e che sono stati comunque comunicati da quest'ultimo al titolare del trattamento. Alla luce della scelta del legislatore di consentire all'interessato, tramite il diritto alla portabilità dei dati, di disporre dei «propri» dati, il motivo di limitazione non deve quindi essere **interpretato in modo troppo ampio**. Tuttavia, è anche vero che, in caso di dubbio, il titolare del trattamento dovrebbe preferire una possibile violazione del diritto alla portabilità dei dati – che ai sensi della LPD non è soggetta a sanzioni – piuttosto che la violazione dei diritti di terzi. 10

C. Manifesta infondatezza (art. 26 cpv. 1 lett. c)

Se una richiesta è manifestamente infondata, il responsabile del trattamento può altresì limitare il diritto alla portabilità dei dati (art. 29 cpv. 1 in combinato disposto con l'art. 26 cpv. 1 lett. c LPD). A titolo esemplificativo, l'art. 26 LPD, che si riferisce specificatamente al diritto di accesso, cita i casi in cui una richiesta persegue una **finalità contraria alla protezione dei dati** o è **manifestamente vessatoria**. La possibilità di limitare la portabilità in caso di 11

finalità contraria alla protezione dei dati è tuttavia difficilmente conciliabile con il diritto alla portabilità, alla luce degli obiettivi della normativa in materia di protezione dei dati e di concorrenza. Il diritto alla portabilità dei dati mira, tra l'altro, a garantire la libera circolazione dei dati, motivo per cui una richiesta **non dovrebbe essere considerata a cuor leggero come manifestamente infondata**. Anche questo riferimento al diritto di accesso risulta quindi insoddisfacente. Il diritto alla portabilità dei dati dovrebbe consentire di trasferire i dati tra diversi soggetti nel modo più standardizzato possibile e senza ricorrere a valutazioni caso per caso. Di conseguenza, non è chiaro in quali casi il titolare del trattamento possa rifiutare una richiesta a questo titolo.

12 Si può tuttavia presumere che una richiesta sia infondata, ad esempio, quando il diritto alla portabilità viene esercitato **in modo abusivo**. Viene inoltre menzionato il caso di una **raccolta di prove** a carico del titolare del trattamento in un procedimento civile.

D. Ulteriori motivi di limitazione (art. 26 cpv. 2)

13 L'art. 29 cpv. 1 LPD rimanda inoltre all'art. 26 cpv. 2 LPD. In tale disposizione sono previsti ulteriori motivi di limitazione per i privati (lett. a) e per gli organi federali (lett. b). Poiché questi ultimi sono raramente legittimati passivamente in materia di diritto alla portabilità dei dati, ai motivi di limitazione **per gli organi federali** non può essere attribuita, a priori, quasi alcuna rilevanza.

14 È invece ipotizzabile che un **titolare del trattamento privato** intenda limitare la portabilità dei dati perché i suoi interessi prevalenti lo richiedono (lett. a, n. 1). Un titolare del trattamento può quindi invocare, ai sensi dell'art. 29 cpv. 1 in combinato disposto con l'art. 26 cpv. 2 lett. a LPD, i propri **segreti d'affari e diritti di proprietà intellettuale** come motivo di limitazione. Nel complesso, tuttavia, ciò dovrebbe verificarsi solo raramente, poiché il diritto alla portabilità dei dati riguarda esclusivamente i dati comunicati dall'interessato, mentre i dati derivati, ovvero quelli basati su una prestazione del titolare del trattamento, sono esclusi dal campo di applicazione. Il legislatore ha già, in linea di principio, subordinato gli interessi del titolare del trattamento a quelli dell'interessato e della concorrenza con l'introduzione del diritto alla portabilità dei dati, motivo per cui quest'ultimo dovrebbe poter invocare i segreti commerciali solo in casi rari.

Qualora il responsabile del trattamento intenda limitare la portabilità in base ai propri interessi prevalenti, l'art. 26 cpv. 2 lett. a LPD enuncia un ulteriore presupposto che deve essere soddisfatto. Al responsabile del trattamento non deve essere consentito di **comunicare i dati personali a terzi** (lett. a n. 2). Tale presupposto, tuttavia, non è compatibile con il diritto al trasferimento dei dati ai sensi dell'art. 28 cpv. 2 LPD e, secondo il presente parere, è pertanto **irrilevante** come presupposto di limitazione. È altresì possibile dedurre che il responsabile del trattamento non possa affatto avvalersi dell'art. 26 cpv. 2 lett. a LPD qualora l'interessato richieda il trasferimento dei dati. 15

III. CONSEGUENZE GIURIDICHE

Qualora sussista un motivo di limitazione ammissibile, il responsabile del trattamento può **rifiutare, limitare o rinviare** la portabilità. In tal caso, il responsabile del trattamento deve rispettare il principio di proporzionalità e garantire il diritto alla portabilità dei dati **il più ampiamente possibile**. Pertanto, prima di un rifiuto, occorre sempre valutare la possibilità di un rinvio o di una limitazione. 16

IV. OBBLIGO DI MOTIVAZIONE (CPV. 2)

Ai sensi dell'art. 29, cpv. 2, della LPD, il responsabile del trattamento deve indicare i motivi per cui rifiuta, limita o rinvia la portabilità. Ciò corrisponde all'obbligo a cui il responsabile del trattamento deve ottemperare anche nell'ambito del diritto di accesso (cfr. art. 26, cpv. 4, della LPD). Il titolare del trattamento deve **comunicare all'**interessato *che* la portabilità viene negata, limitata o rinviata e **motivare** tale decisione in modo adeguato. Anche in questo caso si applica un **termine di 30 giorni** dal ricevimento della richiesta (art. 22 in combinato disposto con l'art. 18 cpv. 3 OPD). Per ulteriori dettagli si rimanda al commento all'art. 25 LPD. 17

Nota:

La struttura e il contenuto del presente commento si basano sulla tesi di dottorato dell'autore sul diritto alla portabilità dei dati. Nelle note a piè di pagina si fa riferimento specifico a tale tesi solo qualora vi si trovino approfondimenti in merito.

BIBLIOGRAFIA

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. ...).

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 31 cpv. 2 lit. e LPD

Un commentario di Philipp do Canto

CITAZIONE SUGGERITA

Philipp do Canto, Commentario all'art. 31 cpv. 2 lit. e LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-do Canto, art. 31 cpv. 2 lit. e LPD N. XXX.

Art. 31 Motivi giustificativi

[1] [...]

[2] Un interesse preponderante del titolare del trattamento può in particolare sussistere se questi:

a. [...]

b. [...]

c. [...]

d. [...]

e. tratta dati personali per scopi impersonali, in particolare nei settori della ricerca, della pianificazione o della statistica, e:

rende anonimi i dati non appena lo scopo del trattamento lo permette; se ciò non è possibile o richiede un onere sproporzionato, prende misure adeguate per impedire che le persone interessate possano essere identificate,
comunica a terzi i dati personali degni di particolare protezione soltanto in una forma che non permetta d'identificare le persone interessate; se ciò non è possibile, prende misure per garantire che i terzi possano trattare i dati soltanto per scopi impersonali, e
i risultati sono pubblicati soltanto in una forma che non permetta d'identificare le persone interessate; o

f. [...]

STRUTTURA

In breve 434
I. Generalità 434
II. cpv. 1, consenso, interesse preponderante, motivi legali di giustificazione 434
III. cpv. 2 434
A. Informazioni generali / fasi di verifica 434
1. lit. a - d 434
2 lit. e, Trattamento per finalità non personali 434
a) Finalità non personali come reato base 435
b) Cifra 1, anonimizzazione o pseudonimizzazione (crittografia) 436
c) Cifra 2, divulgazione a terzi 437
d) Cifra 3, Pubblicazione dei risultati 438
Bibliografia 439
I Materiali 440

IN BREVE

[Nell'introduzione all'articolo 31, a cura di altri redattori].

I. GENERALITÀ

[In generale all'articolo 31; preambolo e contesto, a cura di altri redattori].

II. CPV. 1, CONSENSO, INTERESSE PREPONDERANTE, MOTIVI LEGALI DI GIUSTIFICAZIONE

[sull'art. 31, cpv. 1; a cura di altri redattori].

III. CPV. 2

A. Informazioni generali / fasi di verifica

[In generale al cpv. 2; da parte di altri incaricati del trattamento].

B. Elenco dei casi giuridici

1. lit. a - d

[Da parte di altri incaricati del trattamento].

2 lit. e, Trattamento per finalità non personali

1 L'elaborazione per scopi non personali è la disposizione sugli interessi prevalenti che è stata maggiormente ampliata rispetto alla precedente disposizione dell'art. 13 cpv. 2 lett. e aDSG. Oltre alla precedente disposizione sulla pubblicazione dei risultati (nuova nel cpv. 3 della disposizione, si veda il n. 15 qui di seguito), vi è ora l'obbligo di anonimizzare o pseudonimizzare il più presto possibile (cpv. 1) e, come reato qualificato, l'obbligo di comunicare a terzi i dati personali particolarmente sensibili (cpv. 2). L'autorità di regolamentazione non inizia più con la pubblicazione dei risultati, ma interviene direttamente nella gestione del processo interno durante l'elaborazione. Da un lato, la maggiore densità normativa è il risultato di una concretizzazione giuridica dei principi esistenti; dall'altro, comporta un

inasprimento dei requisiti per i responsabili del trattamento in caso di trattamento per finalità non personali.

a) Finalità non personali come reato base

L'elemento centrale della disposizione è il trattamento per finalità non personali. Le finalità non personali sono finalità per le quali l'identità dell'interessato è irrilevante. In altre parole, lo scopo dell'attività è soddisfatto anche se vengono trattati dati anonimizzati o criptati. Le finalità di trattamento che possono rientrare in questa giustificazione sono molteplici. Non si tratta solo di un gran numero di persone, ma il trattamento dei dati di una singola persona o di un gruppo può servire anche a scopi non personali, purché riguardi solo le caratteristiche e non l'identità. L'identità dell'interessato può tuttavia avere un'importanza pratica per gli stessi responsabili del trattamento, ad esempio nel settore degli studi longitudinali in cui le informazioni vengono raccolte dagli interessati a intervalli regolari. 2

La legge stessa non definisce il termine "finalità non personalizzata", ma cita come esempi la ricerca privata, la statistica e la pianificazione. Il regolamento viene quindi definito anche come "privilegio di ricerca" ai sensi della legge sulla protezione dei dati. La pianificazione della popolazione, del territorio e dei trasporti sono citati come esempi di pianificazione. Lo status privilegiato di queste aree è giustificato dal fatto che non solo forniscono una base importante per il processo decisionale economico, ma soddisfano anche una serie di esigenze sociali e pubbliche. L'elenco delle aree non è esaustivo. In particolare, si dovrebbe prendere in considerazione la valutazione dei dati di utilizzo di Internet e delle app o l'uso di modelli di intelligenza artificiale nel contesto delle analisi dei big data, in cui qualsiasi interesse per l'individuo viene eliminato in anticipo. D'altra parte, la menzione esplicita nella legge non significa che il trattamento dei dati nei settori della ricerca, della statistica e della pianificazione abbia sempre finalità non personali. Un esempio di finalità personalizzata è la medicina di precisione, in cui i risultati positivi degli studi dovrebbero andare a beneficio anche delle persone interessate. Tra le attività con finalità diverse vi sono le ricerche storiche e genealogiche, che non sono coperte dal privilegio se si riferiscono a persone o gruppi specifici. 3

La disposizione regola il trattamento dei dati da parte di privati. Ciò include, ad esempio, la ricerca farmaceutica privata, gli studi clinici privati o gli studi condotti da organizzazioni private, le ricerche di mercato e la pianificazione 4

nelle aziende. In base all'art. 40 LPD, la disposizione copre anche le attività degli organi federali di diritto privato. L'art. 39 LPD, che contiene una disposizione analoga sul trattamento dei dati per scopi non personali da parte degli organi federali, si applica alle attività governative.

5 Vi saranno anche finalità di trattamento che hanno componenti sia personali che non personali, in particolare nella ricerca. Per tali attività, si pone il problema di stabilire in quale misura si possa invocare il motivo di giustificazione. Per gli organi federali, l'art. 35 LPD stabilisce che le eccezioni di cui all'art. 39 cpv. 2 LPD si applicano solo al trattamento per finalità non personali. Una normativa analoga per i responsabili del trattamento privati è quindi comprensibile; essa porta a considerare separatamente la legge sui dati per i diversi aspetti di un'attività specifica.

6 Per quanto riguarda le tre aree menzionate nella legge e altre aree, si deve poi tenere conto della legislazione speciale che, a seconda dell'emanazione, va dalla norma generale di riferimento a regolamenti dettagliati. Di particolare importanza è la legge sulla ricerca umana (attualmente in fase di revisione) con l'LRMT e le leggi correlate, come la legge sulla registrazione dei tumori, che contengono disposizioni proprie sulla pseudonimizzazione e disposizioni di triage relative all'applicazione dell'LRMT e della LPD (ad es. art. 28 LRMT). Nel settore della fornitura di energia elettrica, l'art. 17c cpv. 1 StromVG fa riferimento alla LPD per quanto riguarda i contatori intelligenti. Nel settore statistico, la legislazione speciale della Legge federale sulla statistica (BStatG) si applica nella misura in cui riguarda organizzazioni private (art. 2 cpv. 3 BStatG, cfr. anche i principi di cui all'art. 4 BStatG).

7 Se il trattamento viene effettuato per scopi non personalizzati, si applicano le varie disposizioni delle sezioni da 1 a 3. Le disposizioni in dettaglio:

b) Cifra 1, anonimizzazione o pseudonimizzazione (crittografia)

8 I responsabili del trattamento devono anonimizzare i dati non appena lo scopo del trattamento lo consente. La disposizione riprende quindi il principio dell'art. 6 cpv. 4 LPD e allo stesso tempo lo relativizza con un'eccezione. Secondo questa disposizione, i responsabili del trattamento possono adottare altre misure appropriate per impedire l'identificazione della persona se l'anonimizzazione è tecnicamente impossibile o comporta uno sforzo sproporzionato. Grazie allo sviluppo dei software di riconoscimento

biometrico, ad esempio, oggi è di fatto impossibile anonimizzare i ritratti delle persone, mentre in passato era sufficiente una barra nera nella zona degli occhi. In considerazione dello scopo della norma, l'eccezione deve essere applicata con un senso di proporzione nonostante le conseguenze tecniche e finanziarie e richiede una ponderazione degli interessi nei singoli casi, che bilanci gli interessi delle persone interessate rispetto alla volontà di privilegiare le attività in questione.

Le misure appropriate includono, in particolare, la pseudonimizzazione, la crittografia o la codifica. La pseudonimizzazione svolge un ruolo importante nella pratica e allo stesso tempo rappresenta una sfida tecnica. Soprattutto per quanto riguarda i dati ottenuti da materiale biologico (biocampioni), cioè da parti del corpo umano come tessuti o campioni di sangue, i requisiti tecnici per la pseudonimizzazione sono aumentati. La tecnologia di laboratorio, soprattutto l'analisi del DNA, facilita l'identificazione, eventualmente in combinazione con le caratteristiche di altri campioni. La legge sulla ricerca umana prevede disposizioni corrispondenti per il trattamento del materiale biologico e dei dati genetici (art. 32 e segg. LRUm). 9

Per quanto riguarda le misure per impedire l'identificazione, occorre fare riferimento all'ampio catalogo di misure tecniche e organizzative di cui all'art. 3 DPA, in particolare alle norme sulla riservatezza e sull'integrità. Esistono inoltre diverse linee guida sulla crittografia, come le linee guida vincolanti per il collegamento scientifico dell'Ufficio federale di statistica o le linee guida intersettoriali dell'Agenzia europea per la sicurezza informatica (Enisa). Le linee guida contengono, tra l'altro, requisiti per la gestione dei codici e per la de-pseudonimizzazione. 10

c) Cifra 2, divulgazione a terzi

Il secondo requisito riguarda il trattamento di dati particolarmente sensibili (per il termine, si veda il commento all'art. 5 lett. c LPD). La disposizione fa riferimento all'art. 30 cpv. 2 lett. c LPD, secondo cui la divulgazione di tali dati a terzi costituisce una violazione dei diritti della personalità. Come già nel paragrafo 1, viene stabilito un principio, mitigato da un'eccezione. L'eccezione non era ancora stata inserita nel disegno di legge ed è stata introdotta nel Consiglio nazionale. 11

12 Se è soddisfatto il criterio aggiuntivo dei dati particolarmente sensibili, si applica il principio secondo cui tali dati possono essere trasmessi a terzi solo in modo tale che la persona interessata non possa essere identificata. Pertanto, i dati possono essere trasferiti solo in forma anonima o criptata. Il trasferimento di dati a terzi non è quindi inizialmente trattato in modo diverso dalla pubblicazione (punto 3). Il punto 2 mira a impedire che la divulgazione di dati personali non anonimizzati particolarmente meritevoli di protezione sia giustificata dal fatto che vengono elaborati a fini di ricerca, pianificazione o statistica.

13 L'eccezione si applica se non è possibile adottare misure per impedire l'identificazione, come nel caso dei dati genetici estesi di una persona. Secondo la formulazione, la sproporzione della misura non è considerata una giustificazione (cfr. par. 1). In caso di impossibilità, si deve garantire che i terzi trattino i dati solo per scopi non personalizzati. La disposizione non richiede che lo scopo del trattamento da parte di terzi sia lo stesso del responsabile del trattamento, il che è comprensibile alla luce delle diverse aree di responsabilità nella ricerca, nella statistica e nella pianificazione. L'obbligo di garanzia si applica principalmente al responsabile del trattamento, mentre il paragrafo 2 non contiene alcun requisito metodologico per garantire (contrattualmente) la limitazione delle finalità non personalizzate nei confronti di terzi.

14 Il dispaccio sull'aDSG fa poi riferimento alle disposizioni di legge in materia di riservatezza. Quando queste vietano la divulgazione dei dati a terzi, hanno la precedenza su norme speciali, come il segreto professionale protetto dal diritto penale (ad esempio il segreto medico). Di conseguenza, i dipartimenti di statistica o i ricercatori non possono giustificare la divulgazione di dati segreti sulla base del paragrafo 2. Lo stesso vale per i contratti o le clausole di altro tipo. Lo stesso vale per gli obblighi di riservatezza contrattuali o altrimenti stipulati.

d) Cifra 3, Pubblicazione dei risultati

15 Il cpv. 3 riprende la precedente disposizione secondo cui le persone interessate non devono essere identificabili al momento della pubblicazione dei risultati (art. 13 cpv. 2 lett. e aDSG). In altre parole, non vi è ancora alcun obbligo di anonimizzazione al momento della pubblicazione dei risultati. In dottrina si osserva che la pubblicazione di studi con un numero ridotto di

persone colpite può comportare il rischio di trarre conclusioni sull'individuo, ad esempio nel caso di studi su malattie rare o sulla pianificazione di piccole aree geografiche. Tuttavia, quando si pubblicano risultati basati su dati relativi a un numero elevato di persone affette, questo sembra essere un problema minore, in quanto l'identificazione della persona da parte di un essere umano è più difficile. I sistemi di riconoscimento automatico menzionati in precedenza, invece, funzionano indipendentemente da restrizioni geografiche o numeriche, il che significa che, in ultima analisi, è il progresso tecnico ad aumentare costantemente i requisiti per la pubblicazione dei risultati.

BIBLIOGRAFIA

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).

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 33 LPD

Un commentario di Sandra Husi-Stämpfli

CITAZIONE SUGGERITA

Sandra Husi-Stämpfli, Kommentierung zu Art. 33 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Husi-Stämpfli, N. XXX zu Art. 33 DSG.

Capitolo 6:
Disposizioni speciali per il trattamento di dati personali da parte di organi federali

Art. 33 Controllo e responsabilità in caso di trattamento congiunto di dati personali

Il Consiglio federale disciplina le procedure di controllo e la responsabilità in materia di protezione dei dati nei casi in cui un organo federale tratta dati personali congiuntamente ad altri organi federali, a organi cantonali o a privati.

STRUTTURA

In breve 443
I. Aspetti generali 443
A. Storia 443
B. Scopo della norma 443
II. Nessun vuoto di responsabilità 444
III. Responsabilità condivisa 444
IV. Procedura di controllo 444
V. Regime normativo 445
VI. Questioni di responsabilità 445
Bibliografia 445

IN BREVE

Poiché sempre più spesso il trattamento dei dati personali viene effettuato non solo congiuntamente da diversi uffici federali, ma anche da enti cantonali o comunali o addirittura da privati, è necessario regolamentare in modo chiaro le responsabilità. L'art. 33 LPD autorizza il Consiglio federale a definire le responsabilità in queste costellazioni.

I. ASPETTI GENERALI

A. Storia

La disposizione precedente all'art. 16 aDSG è stata scissa con la revisione della protezione dei dati. L'art. 16 cpv. 1 aDSG, che disciplinava la responsabilità generale, è stato trasferito all'art. 5 lett. j. L'art. 16 cpv. 2 aDSG, che disciplinava la responsabilità in caso di coinvolgimento di più responsabili del trattamento, è stato trasferito all'art. 33 LPD. 1

B. Scopo della norma

L'art. 5 lett. j LPD definisce chi deve essere considerato "responsabile del trattamento dei dati" (cfr. OK-Hofmann sull'art. 5 lett. j LPD): il fattore di collegamento è l'autorità decisionale sulle finalità e sui mezzi del trattamento dei dati. L'organo federale che detiene tale potere decisionale è determinato dalle rispettive leggi speciali che fungono da base giuridica per il trattamento dei dati. 2

Poiché sempre più spesso il trattamento dei dati personali non solo viene effettuato congiuntamente da diversi enti federali, ma le operazioni di trattamento dei dati che attraversano i livelli federali fanno anche parte della vita quotidiana e anche i privati possono accedere a stock di informazioni comuni, è necessario regolamentare chiaramente le responsabilità. Altrimenti, c'è il rischio che molte agenzie trattino i dati personali in questione, ma nessuno si senta responsabile. 3

II. NESSUN VUOTO DI RESPONSABILITÀ

4 L'art. 33 LPD autorizza il Consiglio federale a disciplinare le responsabilità per il rispetto dei requisiti in materia di protezione dei dati e i relativi controlli nel caso in cui più organi federali o organi federali e terzi cantonali o privati siano coinvolti congiuntamente in operazioni di trattamento dei dati. Questa regolamentazione non avviene nella LPD, ma nella rispettiva legislazione speciale o nelle relative ordinanze di attuazione. L'art. 33 LPD, ad esempio, stabilisce esplicitamente che il Consiglio federale regola le procedure di controllo e la responsabilità per il trattamento congiunto dei dati personali.

III. RESPONSABILITÀ CONDIVISA

5 Per il trattamento congiunto dei dati personali sono ipotizzabili tre costellazioni:

- Una legge speciale o un'ordinanza del Consiglio federale può attribuire la responsabilità esclusiva del trattamento comune dei dati a un organo federale (art. 5 lett. j LPD).
- Da una legge speciale o da un'ordinanza si può evincere un rapporto di superiorità o di subordinazione nel trattamento congiunto dei dati, che si traduce in una responsabilità primaria e secondaria. Ne è un esempio il trattamento dei dati su commissione (art. 5 lett. k LPD).
- Una legge o un'ordinanza speciale può determinare una responsabilità parallela per l'elaborazione congiunta dei dati (art. 33 LADP), che deve essere differenziata da una chiara divisione dei compiti nella legge o nell'ordinanza speciale.

IV. PROCEDURA DI CONTROLLO

6 Il concetto di procedura di controllo va inteso come supervisione del trattamento dei dati. Nella prima costellazione di responsabilità esclusiva, così come nel caso di chiara responsabilità principale e secondaria, vi è un controllo unilaterale del responsabile unico o del responsabile principale nei confronti di coloro che partecipano al trattamento congiunto dei dati. Nella seconda costellazione di responsabilità parallele per il trattamento congiunto dei dati, devono naturalmente essere stabilite procedure di controllo reciproche. I dettagli relativi alla portata, alle modalità e alla regolarità delle

procedure di controllo devono essere disciplinati nella legge o nell'ordinanza speciale.

V. REGIME NORMATIVO

Al trattamento congiunto di dati da parte di organi federali con organi cantonali e privati si applicano regimi normativi diversi. Agli organi federali si applicano le disposizioni speciali sul trattamento dei dati ai sensi degli artt. 33 e segg. Agli organi federali si applicano le disposizioni speciali di cui agli artt. 30 e segg. della LPD. LPD e agli organi cantonali si applica il diritto cantonale. Anche in caso di trattamento congiunto dei dati, occorre sempre distinguere chiaramente quale attore è tenuto a rispettare gli obblighi. 7

VI. QUESTIONI DI RESPONSABILITÀ

La responsabilità degli organi federali, degli organi cantonali e dei privati è disciplinata da norme diverse: Per gli organi federali secondo la legge sulla responsabilità civile (VGG), per gli organi cantonali secondo le leggi cantonali sulla responsabilità civile e per i privati secondo il diritto civile. Non è chiaro in che misura una parte responsabile possa rispondere all'esterno per l'intero danno causato dal trattamento congiunto dei dati (cfr. responsabilità solidale). Inoltre, non è chiaro in che misura le violazioni di obblighi da parte di terzi possano essere imputate a un responsabile del trattamento sulla base dell'obbligo di controllo. 8

L'autrice fornisce la sua personale valutazione in questo commento.

BIBLIOGRAFIA

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

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 34 LPD

Un commentario di Esther Zysset

CITAZIONE SUGGERITA

Esther Zysset, Kommentierung zu Art. 34 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Zysset, N. XXX zu Art. 34 DSG.

Art. 34 Basi legali

[1] Gli organi federali hanno il diritto di trattare dati personali soltanto se lo prevede una base legale.

[2] La base legale deve figurare in una legge in senso formale nei casi seguenti:

a. sono trattati dati personali degni di particolare protezione;

b. è effettuata una profilazione;

c. lo scopo del trattamento o il tipo di trattamento può comportare una grave ingerenza nei diritti fondamentali della persona interessata.

[3] Per il trattamento di dati personali secondo il capoverso 2 lettere a e b è sufficiente una base legale figurante in una legge in senso materiale se:

a. il trattamento è indispensabile per l'adempimento di un compito stabilito in una legge in senso formale; e

b. lo scopo del trattamento non comporta rischi particolari per i diritti fondamentali della persona interessata.

[4] In deroga ai capoversi 1–3, gli organi federali possono trattare dati personali se:

a. il Consiglio federale ha autorizzato il trattamento poiché non ritiene pregiudicati i diritti delle persone interessate;

b. la persona interessata ha dato, nel caso specifico, il suo consenso al trattamento oppure ha reso i suoi dati personali accessibili a chiunque e non si è opposta espressamente al trattamento; o

c. il trattamento è necessario per proteggere la vita o l'integrità fisica della persona interessata o di un terzo e non è possibile ottenere il consenso della persona interessata entro un termine ragionevole.

STRUTTURA

In breve 450
I. Aspetti generali 450
A. Osservazioni preliminari 450
B. Scopo normativo e contesto 451
C. Storia delle origini 451
II. Il principio di legalità nella protezione dei dati personali 451
A. Ruolo e funzioni del principio di legalità in generale 451
1. Base giuridica come presupposto per la violazione dei diritti fondamentali e principio dell'azione statale 451
2. Livello e densità delle norme 452
B. Requisiti del principio giuridico ai sensi dell'art. 34 LPD 454
1. Principio fondamentale cpv. 1 454
2. Forma giuridica per i casi di cui al cpv. 2 456
3. Base giuridica sostanziale per i casi di cui al cpv. 3 457
a. Indispensabilità per un compito descritto dalla legge (lett. a) 457
b. La finalità del trattamento non comporta rischi particolari per i diritti fondamentali dell'interessato (lett. b). 458
4. Paragrafo 4: punto di raccolta per le eccezioni ai requisiti dei paragrafi 1-3. . 459
a. Autorizzazione del Consiglio federale (lett. a) 459
b. Consenso (lett. b) 460
c. Clausola di polizia ai sensi della legge sulla protezione dei dati (lit. c) 460
5. Casistica sull'intensità dell'intervento e sui requisiti della norma 461
6. Excursus: consenso "in singoli casi" (cpv. 4 lett. b) 462
Bibliografia 463
I Materiali 464

IN BREVE

Il requisito di un principio giuridico è la chiave di volta del trattamento dei dati da parte degli organi statali.

L'art. 34 LPD illustra per il trattamento dei dati da parte degli organi federali sia l'art. 5 Cost. secondo cui ogni azione statale richiede una base giuridica, sia l'art. 36 Cost. che stabilisce i presupposti per l'ingerenza nei diritti fondamentali in generale; la disposizione costituisce quindi diritto costituzionale concretizzato. Il trattamento dei dati personali da parte di enti pubblici costituisce una violazione del diritto fondamentale alla tutela dell'autodeterminazione informativa ai sensi dell'art. 13 cpv. 2 Cost. L'art. 34 LPD è schematico per quanto riguarda il livello richiesto della norma.

La nuova disposizione sulla base giuridica, che è stata scorporata rispetto alla versione precedente della stessa norma, riflette l'accresciuta importanza del corretto supporto giuridico del trattamento dei dati da parte degli organismi statali nell'era del trattamento digitale di grandi quantità di dati.

I. ASPETTI GENERALI

A. Osservazioni preliminari

1 La base giuridica è una norma generale astratta emanata da un organo statale competente. La legge applicabile determina in dettaglio i requisiti che una base giuridica deve soddisfare. A livello federale, i requisiti si trovano nella Costituzione federale (art. 164 Cost.) o nel diritto parlamentare (ad es. art. 22 ParlG). La norma che funge da base giuridica nel singolo caso può provenire dal diritto nazionale o internazionale.

2 La terminologia utilizzata in relazione al principio di legalità presenta una certa eterogeneità. Di seguito, il termine generale principio di legalità viene utilizzato anche per il requisito di una norma generale-astratta, indicato all'art. 34 DPA come "base giuridica". Inoltre, la legge emanata dal legislatore è descritta con il termine "forma di legge" o "legge in senso formale". Le leggi di livello inferiore sono invece considerate "leggi in senso sostanziale", come indicato nell'art. 34 cpv. 3 LPD.

B. Scopo normativo e contesto

L'art. 34 LPD specifica per il diritto della protezione dei dati ciò che vale in ogni caso per l'azione statale: oltre al principio generale di legalità dell'art. 5 cpv. 1 Cost. secondo cui la legge costituisce la base e la barriera dell'azione statale, l'art. 36 cpv. 1 Cost. richiede una base giuridica per le violazioni dei diritti fondamentali. L'art. 34 LPD fornisce linee guida schematiche a livello normativo per vari tipi di trattamento dei dati - e quindi per varie violazioni dei diritti fondamentali, prima fra tutte la violazione del diritto fondamentale all'autodeterminazione informativa (art. 13 cpv. 2 Cost.). 3

C. Storia delle origini

Il progetto del Consiglio federale della prima legge federale sulla protezione dei dati del 1988 conteneva già una disposizione simile a quella qui commentata; in particolare, si distingueva già tra il trattamento dei dati personali ordinari e quello dei dati che richiedono un livello di protezione più elevato, sotto forma di dati personali che richiedono una protezione speciale e profili della personalità. La disposizione precedente, l'art. 17 aDSG, che nel frattempo è stato modificato, prevedeva il principio fondamentale della base giuridica e stabiliva anche delle eccezioni, la cui portata non era molto chiara e di conseguenza ha dato adito a critiche. 4

La nuova disposizione opera una separazione strutturale; oltre al principio di base invariato (cpv. 1), distingue chiaramente tra il requisito della forma giuridica (cpv. 2), le situazioni con un livello normativo ridotto (cpv. 3) e le situazioni in cui è possibile derogare completamente al requisito di un principio giuridico (cpv. 4). 5

II. IL PRINCIPIO DI LEGALITÀ NELLA PROTEZIONE DEI DATI PERSONALI

A. Ruolo e funzioni del principio di legalità in generale

1. Base giuridica come presupposto per la violazione dei diritti fondamentali e principio dell'azione statale

Il trattamento dei dati personali da parte delle autorità statali comporta un'interferenza con posizioni protette dai diritti fondamentali: Si tratta 6

innanzitutto dell'art. 13 della Cost. e in particolare del cpv. 2 (diritto fondamentale all'"autodeterminazione informativa"), nonché dell'art. 8 della CEDU e dell'art. 17 del Patto ONU II. Contrariamente alla formulazione dell'art. 13 cpv. 2 della Cost. non viene tutelata solo la protezione dall'uso improprio dei dati personali, ma anche la sfera privata, nella misura in cui comprende anche i dati della rispettiva persona. Inoltre, può essere colpita un'ampia gamma di altri diritti fondamentali, tra cui il diritto alla libertà personale (art. 10 cpv. 2 Cost.) o alla libertà di espressione (art. 16 Cost.), soprattutto con la crescente digitalizzazione, in cui ogni attività statale è accompagnata dal trattamento dei dati.

7 Nell'art. 36 cpv. 1, la Costituzione federale stabilisce che le limitazioni dei diritti fondamentali richiedono una base legale; le limitazioni gravi devono essere previste dalla legge, a meno che non vi sia un caso di "pericolo grave, imminente e inevitabile". Inoltre, le limitazioni ai diritti fondamentali devono servire all'attuazione di un interesse pubblico ed essere proporzionate; il contenuto essenziale del diritto fondamentale deve essere preservato (cfr. criteri dell'art. 36 Cost.).

8 Nel suo ruolo di principio dell'azione statale, l'art. 5 cpv. 1 Cost. stabilisce che l'azione statale richiede una base giuridica e che, allo stesso tempo, è la legge a porre dei limiti a tutta l'azione statale ("barriere", secondo le parole del legislatore costituzionale). L'amministrazione - nella terminologia della LPD l'"organo federale" - può quindi agire solo se esiste una base giuridica e può spingersi solo fino a dove l'azione è coperta dalla base corrispondente. Questo vale indipendentemente dalla natura giuridica dell'azione dello Stato, anche se i requisiti del principio di legalità assumono forme diverse a seconda della situazione e del rischio.

2. Livello e densità delle norme

9 L'art. 36 cpv. 1 della Cost. indica già che il principio giuridico richiesto deve soddisfare requisiti maggiori in caso di gravi restrizioni dei diritti fondamentali. Quanto più grave è la violazione dei diritti fondamentali, tanto più elevati sono i requisiti per il livello e la densità della norma. Le restrizioni gravi devono essere previste dalla legge stessa, cioè da una legge in senso formale (livello della norma) e devono tenere sufficientemente conto del requisito della certezza (densità della norma). Come minimo, le norme giuridiche devono essere "formulate in modo così preciso da consentire a

coloro che sono soggetti alla legge di orientare la propria condotta di conseguenza e di riconoscere le conseguenze di un determinato comportamento con un grado di certezza adeguato alle circostanze". In quale caso la qualità della norma giuridica sia sufficiente spesso non è facile rispondere e dipende fortemente dal singolo caso. Nelle parole di Tschannen/Müller/Kern: il principio di legalità è "di una sgradevole assenza di sponde". Per quanto riguarda il diritto federale, l'art. 164 della Cost. fornisce almeno un elenco esemplare di argomenti per i quali le disposizioni di base sono considerate importanti disposizioni legislative e devono quindi essere disciplinate in una legge in senso formale; si tratta di:

- Esercizio dei diritti politici;
- Limitazioni dei diritti costituzionali;
- Diritti e doveri delle persone;
- il gruppo di persone soggette a tributi, nonché l'oggetto e la valutazione dei tributi;
- Doveri e servizi della Confederazione;
- Obblighi dei Cantoni nell'attuazione e nell'applicazione del diritto federale;
- Organizzazione e procedure delle autorità federali.

Da parte sua, la dottrina propone i seguenti criteri per circoscrivere l'importanza di un oggetto di regolamentazione: 10

- intensità dell'interferenza
- numero di persone interessate da una regolamentazione o dalle circostanze di vita regolamentate;
- importanza finanziaria;
- l'importanza per la formazione della volontà politica, per l'organizzazione delle istituzioni statali o per la procedura e per l'efficacia o l'accettabilità del regolamento.
- l'esplosività o l'accettabilità della questione.

11 Al contrario, la necessità di flessibilità e di un rapido adattamento o la presenza di competenze specifiche tendono a favorire le regolamentazioni a un livello normativo inferiore.

12 Questi requisiti generali della Costituzione federale devono essere tenuti in considerazione nella redazione delle basi giuridiche ai sensi dell'art. 34 LPD. L'art. 34 LPD specifica il livello normativo richiesto per alcune situazioni tipiche di protezione dei dati, ma non la densità normativa (cfr. sulla densità normativa infra N. 18-19). Nel contesto della protezione dei dati che interessa in questa sede, l'attenzione si concentra, tra l'altro, sulla restrizione dei diritti costituzionali o sull'intensità delle violazioni dei diritti fondamentali, nonché sulle disposizioni relative ai "diritti e doveri delle persone" contenute nei cataloghi citati in precedenza. Con la crescente digitalizzazione, tuttavia, anche la natura esplosiva degli argomenti gioca sempre più un ruolo come criterio per la forma della legge, come è attualmente evidente, ad esempio, nell'uso dell'intelligenza artificiale o, più specificamente, del riconoscimento facciale negli spazi pubblici.

13 Se i poteri legislativi devono essere delegati dal legislatore all'esecutivo, i requisiti generali della delega legislativa sviluppati dalla giurisprudenza e dalla dottrina entrano in gioco anche nella protezione dei dati. Ad esempio, la delega dei poteri legislativi non può essere esclusa dalla legge pertinente (cfr. art. 164 cpv. 1 Cost.); la norma di delega deve essere contenuta in un atto a livello legislativo; la delega deve essere limitata a una materia specifica e le caratteristiche principali di questa materia devono essere già elencate nella legge.

B. Requisiti del principio giuridico ai sensi dell'art. 34 LPD

1. Principio fondamentale cpv. 1

14 Con il requisito fondamentale di un principio giuridico, il trattamento dei dati da parte degli organi federali è soggetto a un divieto con riserva di autorizzazione, a differenza del trattamento dei dati da parte di privati. Il requisito si applica indipendentemente dal tipo di trattamento dei dati (si veda la definizione giuridica di trattamento all'art. 5 lett. d LPD; per il caso particolare della divulgazione, si veda l'art. 36 LPD). L'art. 34 LPD si limita a fornire il principio di base e non può essere utilizzato come base giuridica

diretta. Inoltre, il cpv. 1 non indica il livello di applicazione del principio giuridico o la densità della norma che deve avere.

Inoltre, dalla sistematica della LPD si evince che le restanti disposizioni generali della legge, in particolare i principi di trattamento dei dati di cui all'art. 6 LPD e le disposizioni sulla sicurezza di cui all'art. 8 LPD, si applicano cumulativamente. Pertanto, l'esistenza di una base giuridica non esime dall'obbligo di osservare il principio di proporzionalità e di trattare solo i dati effettivamente necessari per l'adempimento della funzione pubblica. 15

Il testo giuridico dell'art. 34 LPD si riferisce al trattamento dei dati personali da parte degli organi federali. Per quanto riguarda la definizione di organismo federale, l'art. 5 lett. i LPD stabilisce che non si tratta solo delle unità organizzative dell'amministrazione e delle istituzioni pubbliche della Confederazione, ma anche di persone private, nella misura in cui sono incaricate dell'adempimento di compiti pubblici della Confederazione (cfr. qui). 16

Nonostante le indicazioni sul livello normativo di cui ai cpv. 2-4, nella pratica legislativa spesso non è del tutto chiaro quale debba essere la densità normativa della base giuridica. Questo problema si manifesta, ad esempio, nella questione se sia sufficiente una base giuridica generale ("L'Ufficio X svolge il compito legale Y") o se sia necessaria una base giuridica specifica per un determinato trattamento di dati ("Per elaborare le domande di sovvenzione, l'Ufficio X tratta i seguenti dati personali: ...", ecc.) 17

Per quanto riguarda la natura della base giuridica, l'Ufficio federale di giustizia ha redatto una guida legislativa che fornisce linee guida specifiche per le basi giuridiche nel settore della protezione dei dati. Sullo sfondo delle funzioni del principio di legalità (cfr. infra n. 43 e segg.) e del postulato secondo cui il 18

cittadino deve essere in grado di comportarsi in conformità con la norma pertinente, devono essere disciplinati i seguenti elementi:

- Quale autorità (chi)
- tratta quali categorie di dati personali (cosa),
- per quale scopo (perché) e
- in che modo (come)?
- a chi vengono comunicati i dati personali (a chi) e in che modo (come)?
- in che modo (come)?

19 In particolare, è necessario indicare se vengono trattati anche dati personali che richiedono una protezione particolare e, in caso affermativo, quali categorie (cfr. art. 5 lett. c LPD), mentre le caratteristiche esatte possono essere specificate in un'ordinanza se la legge è sufficientemente densa. Quanto più grave è la violazione dei diritti fondamentali, tanto più dettagliata e precisa deve essere la formulazione della base giuridica, anche se, in considerazione del rapido sviluppo delle tecnologie dell'informazione e della comunicazione, si dovrà talvolta accettare una certa flessibilità nella formulazione e una conseguente vaghezza. Il trattamento comprende anche informazioni sul periodo di conservazione e sulla cancellazione dei dati personali.

20 Nella misura in cui ciò crea la trasparenza richiesta dalla legge nei confronti degli interessati, l'obbligo di fornire informazioni ai sensi dell'art. 19 LPD non si applica (cfr. art. 20 cpv. 1 lett. b LPD).

21 Nel rispettivo diritto sostanziale possono essere previste norme speciali, che prevalgono sulle disposizioni della LPD come lex specialis e possono, almeno teoricamente, discostarsene. Il Tribunale federale e la dottrina partono dal presupposto che in questi casi vadano comunque rispettati i principi generali della legge sulla protezione dei dati.

2. Forma giuridica per i casi di cui al cpv. 2

22 Il secondo paragrafo richiede la forma di legge (legge in senso formale) per i casi in cui il trattamento dei dati può comportare una grave violazione dei diritti fondamentali delle persone interessate. Se il trattamento dei dati

personali che richiedono una protezione speciale (lett. a) e la profilazione (lett. b) sono concetti e termini definiti nella LPD, il cpv. 2 prevede anche una clausola generale che si applica se la finalità del trattamento o le modalità di trattamento dei dati possono comportare una grave violazione dei diritti fondamentali degli interessati (lett. c). Tuttavia, il requisito per cui il trattamento dei dati di grande rilevanza per i diritti fondamentali deve avere la forma di una legge deriva già dall'articolo 36 cpv. 1 della Cost.

I due parametri dell'obiettivo e delle modalità di trattamento di cui alla lettera c sono gli elementi principali che vengono utilizzati per valutare la violazione del diritto fondamentale corrispondente. In considerazione del contesto dei diritti fondamentali, non sono esaustivi. 23

Se non è possibile basare il trattamento dei dati su una base giuridica sufficientemente precisa e dettagliata, la giurisprudenza conferma che una gestione particolarmente rigorosa del test di proporzionalità, ad esempio, può avere un certo effetto compensativo. 24

3. Base giuridica sostanziale per i casi di cui al cpv. 3

cpv. 3 prevede la possibilità di un livello standard ridotto per il trattamento di dati personali particolarmente sensibili e per la profilazione, a condizione che siano soddisfatte cumulativamente due condizioni: Il trattamento è indispensabile per un compito formalmente definito dalla legge; e la finalità del trattamento non presenta rischi particolari per i diritti fondamentali dell'interessato. 25

A causa del quadro costituzionale, anche in questo caso è ipotizzabile - anche se gli esempi saranno probabilmente rari - che si verifichino deviazioni non specificamente enumerate dal cpv. 3: Ad esempio, l'esplosività sociale di un argomento potrebbe portare a una situazione in cui la forma giuridica deve comunque essere richiesta per il corrispondente trattamento dei dati; è quindi la modalità del trattamento dei dati, piuttosto che lo scopo menzionato nel cpv. 3, a dare origine a un aumento del livello normativo. 26

a. Indispensabilità per un compito descritto dalla legge (lett. a)

Per quanto riguarda la formulazione del cpv. 3 lettera a, rispetto alla versione precedente (art. 17 cpv. 2 lettera aDSG) si nota che non dovrebbe essere più possibile fare riferimento al livello normativo ridotto solo "in via eccezionale". 27

Nella versione precedente, si poteva ritenere che si trattasse solo di un trattamento eccezionale e selettivo dei dati in situazioni in cui tale trattamento non sarebbe stato normalmente necessario per adempiere al corrispondente compito legale. L'attuale formulazione si discosta chiaramente da questo punto di vista, eliminando il requisito dell'esistenza di una situazione eccezionale. Di conseguenza, si deve ritenere che il trattamento di dati personali particolarmente sensibili e di profili della personalità su base permanente sia possibile anche sulla base di un'ordinanza, se sono soddisfatti i due requisiti del cpv. 3.

b. La finalità del trattamento non comporta rischi particolari per i diritti fondamentali dell'interessato (lett. b).

28 Cpv. 3 let. b si applica ai trattamenti che rientrano in una categoria intermedia: Sebbene si tratti di tipi di trattamento che di norma comportano una grave violazione dei diritti fondamentali (motivo per cui il cpv. 2 richiede di norma una base giuridica formale), nel caso specifico la finalità del trattamento non presenta rischi particolari per i diritti fondamentali delle persone interessate. Secondo il messaggio del Consiglio federale, si tratta in particolare di dati che richiedono una protezione speciale e che sono trattati nell'ambito delle attività del Consiglio federale, dei dipartimenti e dei funzionari; si pensi alle decisioni di ricorso, ai casi di responsabilità dello Stato o alle attività del personale federale. Inoltre, la base giuridica formale deve specificare sufficientemente la natura dei compiti per i quali è necessario il trattamento dei dati personali.

29 La formulazione del paragrafo 3, lettera b, può sorprendere, in quanto si riferisce solo alla "finalità del trattamento" senza includere le "modalità del trattamento dei dati" precedentemente menzionate nel paragrafo 2, lettera c. La formulazione del paragrafo 3, lettera b, non è chiara. Si può supporre che il legislatore abbia voluto ricordare in primo luogo che il trattamento dei dati, che già a causa della sua finalità appare sensibile in termini di diritti fondamentali, richiede in ogni caso una base sotto forma di legge, anche se il tipo e le modalità di trattamento nel singolo caso comportano pochi rischi propri.

4. Paragrafo 4: punto di raccolta per le eccezioni ai requisiti dei paragrafi 1-3.

cpv. 4 esenta tre situazioni ideali (scritte come alternative) dall'obbligo di uno strumento legale: 30

- Autorizzazione del trattamento da parte dell'esecutivo (in questo caso il Consiglio federale), anche in questo caso l'autorizzazione deve basarsi sul requisito che i diritti delle persone interessate non possano essere messi in pericolo (lett. a);
- il consenso dell'interessato nel singolo caso o il rilascio incondizionato dei dati personali da parte dello stesso (lett. b) oppure
- l'interesse urgente e prevalente della protezione della vita o dell'integrità fisica dell'interessato o di un terzo in una situazione che rende impossibile ottenere il consenso (lett. c).

Mentre il paragrafo 3 si limita a ridurre i requisiti della base giuridica, il paragrafo 4 prevede per alcuni casi la formulazione che non è richiesto alcun principio giuridico, né una legge né un principio giuridico di natura sostanziale. Nella misura in cui si rinuncia esplicitamente al requisito di un principio giuridico, questa disposizione rappresenta formalmente la maggiore innovazione rispetto alle versioni precedenti della stessa disposizione della LPD. Per le circostanze di cui alle lettere a e b, entrambe già presenti nella versione precedente, viene fornito un gradito chiarimento; dalla formulazione della norma precedente non si poteva leggere con certezza se si intendesse o meno rinunciare completamente a una base giuridica. 31

a. Autorizzazione del Consiglio federale (lett. a)

Secondo la lettera a, il Consiglio federale autorizza il trattamento perché "non ritiene che i diritti della persona interessata siano a rischio". Mentre nella versione precedente si affermava esplicitamente che tale autorizzazione era limitata al singolo caso, questa aggiunta manca nella formulazione attuale. Secondo il dispaccio, tuttavia, nonostante la differenza di formulazione, non cambia nulla nella norma, come si evince anche dal contesto a un esame più attento. L'autorizzazione deve essere vista come una forma di decisione in contrasto con il regolamento generale-astratto. Quest'ultima assume la forma di un'ordinanza del Consiglio federale (art. 182 cpv. 1 Cost.), ossia una base 32

giuridica sostanziale che è esecutiva o rappresentativa del diritto (e nel secondo caso richiede l'autorizzazione di una legge). Il caso di azione senza principio giuridico previsto dal cpv. 4 lett. a è quindi necessariamente concepito per il singolo caso.

33 Come nella versione precedente, è altrettanto oscura la formulazione secondo cui "i diritti della persona interessata non devono essere messi in pericolo". Questa formulazione differisce da quella del cpv. 3 lett. b, che afferma che la finalità del trattamento "non comporta rischi particolari per i diritti fondamentali dell'interessato". Tuttavia, dato che ogni trattamento di dati da parte di enti pubblici rappresenta una violazione dei diritti fondamentali, si può presumere che la formula utilizzata nel paragrafo 4 abbia lo stesso significato del paragrafo 3, lettera b), ossia che si debba presumere una violazione minore dei diritti fondamentali.

b. Consenso (lett. b)

34 Nella lettera b, il consenso sostituisce la base giuridica. In caso di rilascio incondizionato dei dati, il consenso si presume; in questo caso, è necessaria una comunicazione consapevole e volontaria da parte dell'interessato. Sul consenso in generale si veda l'art. 6 cpv. 6 e 7 LPD e sulla questione del consenso come valido sostituto di una base giuridica infra n. 42 e segg.

c. Clausola di polizia ai sensi della legge sulla protezione dei dati (lit. c)

35 La lettera c si concentra sulla tutela di interessi urgenti e preminenti, concretizzati nella protezione della vita o dell'integrità fisica dell'interessato o di un terzo. Il prerequisito è che non sia possibile ottenere il consenso della persona interessata entro un periodo di tempo ragionevole, il che avviene, ad esempio, se la persona non è in uno stato reattivo (coma o simile) o non può essere trovata. Questa norma è un caso di "interesse di polizia" specificato nella legge sulla protezione dei dati. A questo proposito, si inserisce facilmente nello schema dell'art. 36 par. 1 Cost. che esenta dal requisito di una base giuridica i "casi di pericolo grave e imminente che non può essere evitato in altro modo". Non è esplicitamente scritto, ma è insito nella natura della clausola di polizia, il requisito che deve trattarsi di un caso individuale, il che significa, ad esempio, che il trattamento dei dati della polizia o dei servizi di intelligence nel contesto di situazioni di pericolo ricorrenti non può essere effettuato solo sulla base del cpv. 4, lett. c. 5.

5. Casistica sull'intensità dell'intervento e sui requisiti della norma

Ai sensi dell'art. 17 cpv. 2 aDSG, il trattamento dei dati di assistenza amministrativa relativi a rapporti commerciali o a conti bancari non richiede una base giuridica. La violazione dei diritti costituzionali in relazione ai dati da raccogliere nel caso dell'assistenza amministrativa non è generalmente particolarmente grave, per cui anche i requisiti di definitività della norma non sono "eccessivamente elevati" (DTF 148 II 349 E. 5.3.3-5.3.4). 36

La base giuridica che prevede l'utilizzo di contatori d'acqua via radio da parte della rete idrica comunale deve prevedere esplicitamente che i valori orari registrati vengano memorizzati sul contatore per X giorni e inviati via radio a intervalli regolari (DTF 147 I 346 E. 5.4.1). 37

Se, oltre alla targa e quindi all'identità del proprietario, durante la ricerca automatizzata del veicolo si ottengono anche l'ora, la posizione, la direzione di marcia e l'identità degli altri occupanti del veicolo, questo trattamento dei dati rientra nell'ambito di una "determinazione convenzionale dell'identità", che non costituisce ancora una grave violazione dei diritti fondamentali. Tuttavia, la situazione cambia notevolmente con la fusione e il confronto automatico di questi dati con altri record di dati (si parla di un "trattamento seriale e simultaneo di record di dati grandi e complessi in frazioni di secondo") e il successivo utilizzo da parte delle autorità; l'intensità dell'interferenza aumenta "considerevolmente", tra l'altro a causa del pericolo che le persone vengano sospettate erroneamente (DTF 146 I 11 E. 3.2). 38

L'iscrizione in una lista di sorveglianza tenuta dalla FINMA, che serve come fase preliminare a eventuali restrizioni dell'attività lavorativa nel settore del mercato finanziario e porta complessivamente a un vero e proprio profilo della personalità, costituisce una grave violazione dell'art. 13 cpv. 2 Cost. e richiede una base sotto forma di legge (DTF 143 I 253 E. 4). 39

Se una legge di polizia pone la sorveglianza tecnica di luoghi generalmente accessibili sotto la voce "salvaguardia dell'ordine pubblico e della sicurezza", questa dichiarazione di scopo è insufficiente e, in particolare, non consente di esaminare la base giuridica per la sua proporzionalità (in particolare il rapporto tra i fini e i mezzi). (BGE 136 I 87 E 8.3-8.4). 40

La sufficiente determinatezza di una norma può derivare anche dalla rete di norme applicabili: Se si obietta che l'art. 91 cpv. 5 LEF ha una densità di 41

norme insufficiente per la divulgazione di dati contenenti dati personali e/o profili della personalità particolarmente meritevoli di protezione, si deve controbattere che la disposizione si applica solo nell'ambito dell'esecuzione del sequestro. Lo scopo e l'ambito del trattamento dei dati sono quindi definiti con sufficiente precisione. (DTF 124 III 170 E. 3a)).

6. Excursus: consenso "in singoli casi" (cpv. 4 lett. b)

42 Nel diritto pubblico della protezione dei dati, spesso non è chiaro in che misura il consenso possa sostituire la base giuridica. La questione del consenso si pone in modo particolarmente acuto quando si tratta di gravi violazioni dei diritti fondamentali; in primo piano vi è la rinuncia ai diritti fondamentali o il consenso a violazioni particolarmente gravi dei diritti fondamentali. All'altro estremo dello spettro di violazione, tuttavia, possono esserci altrettanti punti interrogativi, ad esempio quando si tratta dell'invio di una newsletter da parte di un'autorità pubblica o dell'ottenimento di referenze in una procedura di assunzione. L'art. 34 LPD prevede al cpv. 4 lett. b il consenso come sostituto dello Stato di diritto, e lo stesso vale per l'art. 36 cpv. 2 lett. b LPD per quanto riguarda la divulgazione di dati personali. In entrambi i casi, il consenso è legato al singolo caso, ma non è altrimenti soggetto alla condizione che i fatti del caso siano poco o per nulla pericolosi. A differenza del consenso nel diritto privato della protezione dei dati (cfr. art. 6 cpv. 6 e 7 LPD), nel diritto pubblico non è sufficiente che il consenso sia volontario e informato. Inoltre, il consenso deve essere idoneo nel caso specifico ad assumere le funzioni del principio di legalità in gioco. Al di là di questi requisiti sostanziali, il consenso nel diritto pubblico non è vincolato ad alcuna forma.

43 Il Tribunale federale e la dottrina concordano sul fatto che il principio di legalità svolge due tipi di funzioni. Da un lato, persegue interessi democratici, tra cui la supremazia della volontà popolare da un lato e la separazione dei poteri dall'altro. Dall'altro lato, svolge le funzioni dello Stato di diritto; in questo contesto, assicura la protezione dell'individuo contro l'azione arbitraria dello Stato, la parità di trattamento e la prevedibilità dell'azione statale.

44 A determinate condizioni, il consenso può certamente sostituire le funzioni costituzionali di protezione dall'arbitrio e di prevedibilità dell'azione statale. Affinché ciò avvenga, la portata del consenso deve essere riconoscibile nel

momento in cui viene prestato e il contesto deve essere tale da far presumere la natura volontaria del consenso in buona fede.

Tuttavia, una prima restrizione deriva dalla funzione costituzionale della parità di trattamento: nel momento in cui si tratta di concedere diritti o imporre doveri, il consenso può essere operativo come sostituto di un principio giuridico solo se sono interessate solo singole persone. Nei casi in cui le preoccupazioni democratiche sono in primo piano, il consenso non è più in grado di fornire alcuna compensazione funzionale. 45

Di conseguenza, a seconda delle circostanze, si deve esaminare, facendo ricorso alle preoccupazioni del principio di legalità e ai criteri per il requisito della forma giuridica (cfr. supra n. 9-10), se la rinuncia a una base giuridica e l'affidamento al consenso possano essere giustificati. 46

Per il trattamento dei dati da parte degli organi federali, l'art. 34 cpv. 4 lett. b LPD delimita l'ammissibilità limitando il consenso al singolo caso. Alla luce di quanto detto, si deve presumere che il numero di situazioni debba essere molto limitato, sia in termini di oggetto che di tempo, e inoltre per l'introduzione di diritti e obblighi anche in termini personali. 47

Pertanto, nonostante la specificazione schematica della LPD in merito alle violazioni dei diritti fondamentali, la questione può essere risolta in modo affidabile solo in termini concreti, tenendo conto delle preoccupazioni in questione. Ad esempio, la summenzionata newsletter di un'autorità può essere inviata anche a un numero molto elevato di destinatari e con una periodicità illimitata sulla base del consenso, mentre l'uso di sistemi di riconoscimento facciale non è probabilmente ammissibile sulla base del consenso in singoli casi, anche in un ambito strettamente definito in termini di luogo, tempo e personale, a causa dell'intensità della violazione dei diritti fondamentali delle persone interessate e dell'esplosività sociale della tecnologia utilizzata. 48

BIBLIOGRAFIA

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.

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 35 LPD

Un commentario di Sandra Husi-Stämpfli

CITAZIONE SUGGERITA

Sandra Husi-Stämpfli, Kommentierung zu Art. 35 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Husi-Stämpfli, N XXX zu Art. 35 DSG.

Art. 35 Trattamento automatizzato di dati personali nell'ambito di sistemi pilota

[1] Il Consiglio federale può autorizzare il trattamento automatizzato di dati personali degni di particolare protezione o altri trattamenti ai sensi dell'articolo 34 capoverso 2 lettere b e c prima dell'entrata in vigore di una legge in senso formale se:

a. i compiti che richiedono tale trattamento sono disciplinati in una legge in senso formale già in vigore;

b. sono prese misure sufficienti per ridurre al minimo l'ingerenza nei diritti fondamentali della persona interessata; e

c. per l'attuazione pratica del trattamento è imprescindibile una fase sperimentale prima dell'entrata in vigore della legge formale, in particolare per ragioni tecniche.

[2] Il Consiglio federale chiede previamente il parere dell'IFPDT.

[3] L'organo federale competente presenta un rapporto di valutazione al Consiglio federale al più tardi due anni dopo la messa in opera del sistema pilota. Nel rapporto propone la continuazione o l'interruzione del trattamento.

[4] Il trattamento automatizzato di dati personali deve in ogni caso essere interrotto se entro cinque anni dalla messa in opera del sistema pilota non è entrata in vigore una legge in senso formale che prevede la pertinente base legale.

STRUTTURA

In breve 470
I. Aspetti generali 470
A. Contesto 470
B. Scopo della norma 470
C. Storia 471
II. Prerequisiti per un test pilota ammissibile (cpv. 1) 471
A. Norma di compito in una legge in senso formale (lett. a) 471
B. Limitare al minimo le violazioni della personalità (lett. b) 471
C. Indispensabilità della fase di prova (lett. c) 472
III. Regolamentazione del progetto pilota in un'ordinanza 472
IV. Obbligo di ottenere il parere dell'IFPDT (cpv. 2) 473
V. Valutazione e termine della fase pilota (cpv. 3 e 4) 473
VI. valutazione 474
Bibliografia 474

IN BREVE

La disposizione sull'esecuzione di test pilota consente il trattamento di dati personali che richiedono una protezione speciale, anche se non esiste ancora una base giuridica formale. Lo scopo della disposizione è quello di consentire il trattamento sperimentale dei dati per un periodo di tempo limitato, se ciò è indispensabile per affrontare determinate innovazioni tecniche, questioni organizzative o ulteriori incertezze.

I. ASPETTI GENERALI

A. Contesto

1 La necessità di applicazioni potenti non solo nelle cosiddette "e-aree", cioè nell'eGovernment o nell'eHealth, ma più in generale nell'ambito dell'adempimento di compiti ufficiali, cresce con la digitalizzazione dei nostri ambiti di vita e di attività.

2 Poiché i progetti di digitalizzazione comportano solitamente elevati costi di investimento, ma allo stesso tempo è spesso impossibile valutare se le applicazioni in questione possano essere tecnicamente implementate come sperato, è necessario fornire opportunità per poter valutare la concezione e soprattutto la messa in rete delle applicazioni nell'ambito di prove pilota. Le prove pilota devono essere intese come test per acquisire conoscenze sulla fattibilità o sull'accettazione di un progetto.

B. Scopo della norma

3 Le prove pilota non devono compromettere i principi dello Stato di diritto. Anche se, a causa della natura sperimentale del trattamento dei dati e della complessità del processo legislativo, al momento del progetto pilota non è ancora possibile ricorrere alle basi giuridiche fornite dalla Costituzione (con un livello e una densità adeguati di norme), devono comunque essere rispettati i requisiti legali minimi.

4 L'art. 35 LPD consente quindi al Consiglio federale di effettuare test pilota per un periodo di tempo limitato, basandosi solo su un'ordinanza (e non su una

legge in senso formale, come sarebbe richiesto per i dati personali particolarmente sensibili, art. 34 cpv. 2 LPD).

C. Storia

Già nel 1999 è stata presentata la mozione "Maggiore protezione dei dati personali nelle connessioni online". Essa ha costituito la base per il successivo art. 17a aDSG e per la regolamentazione del trattamento dei dati nell'ambito di test pilota in cui i diritti personali delle persone interessate potrebbero essere particolarmente a rischio. Il contenuto dell'art. 35 LPD è stato incorporato nella nuova legge sulla protezione dei dati in modo sostanzialmente invariato e incontestato nelle deliberazioni parlamentari. 5

II. PREREQUISITI PER UN TEST PILOTA AMMISSIBILE (CPV. 1)

I dati personali che richiedono una protezione particolare o altri trattamenti di dati ai sensi dell'art. 34 cpv. 2 lett. b e c LPD possono essere trattati nell'ambito di un test pilota e in deroga all'obbligo di una base giuridica solo se sono soddisfatte cumulativamente le seguenti condizioni: 6

A. Norma di compito in una legge in senso formale (lett. a)

I compiti per l'adempimento dei quali è necessario il progetto pilota con il trattamento automatizzato di dati personali sensibili devono essere già disciplinati in una legge in senso formale al momento del progetto pilota (cfr. OK-Zysset sull'art. 34 LPD), e la legge deve anche essere già in vigore. 7

Non è sufficiente che la base giuridica formale disciplini solo i compiti che rendono necessario il trattamento. Il requisito della densità normativa deve essere soddisfatto, se non per il progetto pilota in sé, almeno per i compiti alla base del progetto. La base giuridica deve quindi descrivere l'organismo che ha accesso ai dati, lo scopo specifico dell'accesso e la portata dell'autorizzazione all'accesso. 8

B. Limitare al minimo le violazioni della personalità (lett. b)

Al fine di ridurre al minimo i rischi che il progetto pilota comporta per gli interessati, devono essere adottate misure organizzative, tecniche e legali, in 9

particolare per garantire la sicurezza dei dati. Le misure di protezione devono ridurre al minimo la possibile minaccia di violazioni della personalità. La nuova formulazione dell'art. 35 cpv. 1 lett. b LPD rende quindi giustizia al fatto che il rischio di violazioni della personalità nel contesto del trattamento dei dati digitalizzati non può di fatto mai essere completamente escluso.

C. Indispensabilità della fase di prova (lett. c)

10 I progetti pilota per il trattamento di dati personali particolarmente sensibili e la relativa relativizzazione del principio di legalità non devono essere avviati a cuor leggero: L'art. 35 cpv. 1 lett. c LPD richiede che la fase di prova sia indispensabile, in particolare per motivi tecnici. Allo stesso tempo, però, il legislatore ammette che ci possono essere altre ragioni, ad esempio organizzative, che rendono necessario un test pilota per il trattamento di dati personali particolarmente sensibili ("in particolare").

11 Sono inoltre ipotizzabili combinazioni di condizioni tecniche e organizzative che da sole non giustificherebbero il ricorso all'art. 35 LPD, ma che insieme rendono necessaria una prova pilota, soprattutto quando si tratta di testare i sistemi informatici e verificare le interfacce tra i livelli federali. Infine, la pandemia Covid ha dimostrato che possono esserci anche motivi imprevisti per effettuare un test pilota: L'applicazione svizzera Covid è stata gestita sulla base dell'allora art. 17a aDSG (in combinato disposto con l'art. 78 cpv. 1 EpG) durante una fase di prova di un mese, al fine di testare gli "approcci risolutivi di nuova concezione per quanto riguarda la natura decentralizzata dell'elaborazione dei dati e i metodi crittografici, (la) stabilità del funzionamento, (la) protezione da manipolazioni involontarie o non autorizzate, (la) facilità d'uso (nonché) la comprensibilità delle informazioni per i partecipanti e per i professionisti autorizzati ad accedervi". In questo caso e a causa dell'urgenza della situazione, la fase pilota è durata solo dal 14 maggio 2020 al 25 giugno 2020, dopodiché l'app è stata messa in funzione regolarmente.

III. REGOLAMENTAZIONE DEL PROGETTO PILOTA IN UN'ORDINANZA

12 Anche se l'art. 35 LPD, a differenza della precedente disposizione dell'art. 17a cpv. 3 aDSG, non prevede più esplicitamente che il Consiglio federale debba

disciplinare il progetto pilota proprio nell'ambito di un'ordinanza, tale obbligo non solo continua a sussistere ai sensi dell'art. 33 cpv. 2 lett. e LPD (obbligo dell'organo federale competente di consultare l'IFPD nell'ambito della procedura di autorizzazione e di sottoporgli un progetto di ordinanza): Si tratta del principio di legalità sancito dall'art. 5 cpv. 1 Cost. da cui si può dedurre che un livello minimo di controllo da parte dello Stato di diritto deve essere mantenuto anche durante un progetto pilota, oppure che gravi violazioni dei diritti fondamentali richiedono almeno una base giuridica a livello di ordinanza, anche nel caso di progetti pilota.

L'ordinanza deve contenere tutte quelle regole che (al di fuori di un progetto pilota) dovrebbero essere stabilite a livello di leggi e ordinanze. È importante - soprattutto per quanto riguarda la valutazione obbligatoria (n. 16) - che sia specificato il più precisamente possibile in anticipo che cosa esattamente deve essere testato. 13

IV. OBBLIGO DI OTTENERE IL PARERE DELL'IFPDT (CPV. 2)

Il progetto pilota deve essere sottoposto al parere dell'IFPDT. Questa norma stabilisce un meccanismo di controllo essenziale che tiene conto del fatto che i progetti pilota possono discostarsi dal principio costituzionale del livello standard. Come elemento di "checks and balances", l'IFPDT è responsabile almeno della verifica della plausibilità del progetto pilota, del controllo dei meccanismi di protezione adottati, della revisione dell'ordinanza e delle valutazioni periodiche. A tal fine, ai sensi dell'art. 33 cpv. 2 e 3 LADP, devono essere trasmesse all'IFPDT informazioni dettagliate, in particolare sul progetto pilota in sé e per sé, sulle misure organizzative e tecniche (di sicurezza), su una bozza o almeno su un concetto dell'ordinanza che deve regolare il test pilota, nonché su un piano del progetto. 14

Anche se l'IFPDT non può emettere un parere vincolante, si può presumere che il Consiglio federale seguirà generalmente la valutazione dell'IFPDT. 15

V. VALUTAZIONE E TERMINE DELLA FASE PILOTA (CPV. 3 E 4)

Il progetto pilota deve essere valutato al più tardi entro due anni dall'entrata in funzione (art. 35 cpv. 3 LPD). L'ente responsabile del progetto pilota deve spiegare al Consiglio federale nel rapporto di valutazione se il progetto può 16

già essere trasferito a un servizio regolare, se il progetto pilota deve essere continuato (ma si noti il limite massimo di cinque anni, n. 17) o se il progetto deve essere interrotto.

17 In generale, la fase pilota può durare al massimo cinque anni (art. 35 cpv. 4 LPD). Questo periodo non può essere prorogato, anche se il progetto pilota deve essere convertito in un servizio regolare, ma non è ancora stata sviluppata una base legale - un funzionamento "regolare" basato su una semplice bozza non è ammissibile per ragioni di stato di diritto.

VI. VALUTAZIONE

18 Sebbene l'art. 17a aDSG sia stato finora utilizzato solo molto raramente e il Consiglio federale affermi che ricorrerà all'art. 35 LPD solo in casi eccezionali, si può presumere che con la trasformazione digitale dell'amministrazione anche la disposizione relativa ai test pilota sarà utilizzata più spesso. Ciò può essere nell'interesse dello sviluppo digitale dell'Amministrazione federale, ma non va dimenticato che l'applicazione dell'art. 17a aDSG o dell'art. 35 LPD è sempre accompagnata da una violazione del principio di legalità. Si dovrebbe quindi evitare un ricorso troppo generoso all'art. 35 LPD, senza che, ad esempio, esista una norma sul compito in senso formale o che sia stata esaminata seriamente l'indispensabilità della fase di prova. Dopotutto, non si può negare che i progetti pilota siano sempre accompagnati da alti costi di investimento: la decisione di non continuare a gestire un sistema dopo la fine della fase di test dovrebbe quindi essere non solo difficile, ma anche rara.

L'autrice fornisce la sua valutazione personale in questo commento.

BIBLIOGRAFIA

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 38 LPD

Un commentario di Claudia Schreiber

CITAZIONE SUGGERITA

Claudia Schreiber, Commentario dell'art. 38 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Schreiber, art. 38 LPD N. XXX.

Art. 38 Offerta di documenti all'Archivio federale

[1] Conformemente alla legge federale del 26 giugno 1998[9] sull'archiviazione, gli organi federali offrono all'Archivio federale i dati personali di cui non necessitano più in modo permanente.

[2] L'organo federale distrugge i dati personali che l'Archivio federale ha designato come non aventi valore archivistico, salvo che tali dati:

a. siano resi anonimi;

b. debbano essere conservati a titolo di prova, per misura di sicurezza o per salvaguardare un interesse degno di protezione della persona interessata.

STRUTTURA

I. In breve 479
II. Informazioni generali 479
A. Storia dell'origine 479
B. Ambito di applicazione 481
C. Termini 482
III. Offerta di documenti nel contesto della valutazione prospettica (cpv. 1) 483
IV. Dati personali non più necessari in modo permanente (cpv. 1) 485
V. Distruzione dei documenti non meritevoli di archiviazione (cpv. 2) 486
VI. Anonimizzazione dei dati personali (cpv. 2 lett. a) 487
VII. Conservazione a fini probatori o di sicurezza, salvaguardia dei legittimi interessi dell'interessato (cpv. 2 lett. b) 487
VIII. Attuazione con malintesi 488
IX. Valutazione 490
Bibliografia 491
I Materiali 491

I. IN BREVE

L'art. 38 LPD svolge un'importante funzione di ponte tra la Legge federale sulla protezione dei dati (LPD) e la Legge federale sull'archiviazione (LCA). 1

Oggi l'art. 38 LPD può dare adito a malintesi, poiché la prassi archivistica è cambiata a livello federale, in particolare in seguito all'introduzione della valutazione prospettica nel 2010. 2

II. INFORMAZIONI GENERALI

A. Storia dell'origine

Il fatto che la protezione dei dati, l'archiviazione e la ricerca storica, che si basa su documenti archiviati, abbiano interessi diversi è già stato sufficientemente discusso. In concomitanza con la stesura della prima legge federale sulla protezione dei dati alla fine degli anni '70, in alcuni settori del mondo archivistico si temeva che l'impegno per la protezione dei dati potesse portare a una "crescente tendenza alla distruzione/cancellazione" e a una "limitazione dell'uso e delle pratiche di autorizzazione dei singoli dipartimenti". Questi timori sono sorti in particolare perché la prima legge sulla protezione dei dati a livello federale è stata redatta in un periodo in cui l'archiviazione a livello federale era regolamentata solo a livello di regolamenti e direttive. 3

Inizialmente sembrava che la nuova legge sulla protezione dei dati avrebbe affrontato la questione dell'archiviazione dei dati personali in modo dettagliato, in quanto il gruppo di lavoro sulla protezione dei dati nell'Amministrazione federale aveva proposto di redigere un articolo 20 intitolato "Distruzione e archiviazione dei dati" o "Archiviazione e distruzione dei dati", che avrebbe contenuto norme dettagliate sull'archiviazione dei dati (personali): In una bozza del gruppo di lavoro si legge: "I supporti di dati di valore permanente possono essere archiviati (var.: conservati) nell'Archivio federale oltre il tempo del trattamento originariamente necessario; il loro ulteriore trattamento è consentito solo nell'ambito del regolamento dell'Archivio federale". 4

5 Tuttavia, questa proposta non è stata successivamente accettata. Si è rinunciato a un regolamento speciale sull'archiviazione dei dati: L'allora art. 18 cpv. 2 LPD e l'art. 21 della prima LPD del 19 giugno 1992 eliminarono l'archiviazione dal titolo e stabilirono, sotto il titolo "Anonimizzazione e distruzione dei dati personali", che gli organi federali dovevano anonimizzare o distruggere i dati personali di cui non avevano più bisogno, a meno che "i dati servissero a scopi probatori o di sicurezza" o "dovessero essere consegnati all'Archivio federale". In questo modo sono state gettate le basi per il carattere dell'attuale art. 38 LPD.

6 Poco dopo l'entrata in vigore della prima LPD a livello federale nel 1992, il Consiglio federale ha incaricato il Dipartimento federale dell'interno (DFI) di elaborare un progetto preliminare per la creazione di una legge federale sull'archiviazione con una risoluzione del 18 agosto 1993. Il lavoro è stato successivamente intrapreso da un gruppo di lavoro interdipartimentale. L'esigenza di una base giuridica per l'archiviazione in una legge federale formale è nata dagli evidenti sconvolgimenti nel settore dell'archiviazione (tra cui il massiccio aumento del volume di documenti prodotti dagli enti federali dopo la Seconda guerra mondiale e l'incremento della produzione di documenti elettronici nell'ultimo quarto del XX secolo) e dalla richiesta di "realizzare un'adeguata protezione dei dati", come indicato nel messaggio sulla legge federale sull'archiviazione del 26 febbraio 1997.

7 Allo stesso tempo, il messaggio sulla BGA affermava che il diritto di consultare i documenti d'archivio non significa il diritto alla divulgazione incontrollata o alla trasmissione acritica di dati personali. Piuttosto, il diritto di consultare il materiale archivistico "impone una revisione critica del contenuto dei documenti archiviati e della loro interpretazione e presentazione nel rispetto della tutela della privacy"; questa responsabilità spetta agli utenti dell'archivio. Si noti che nel caso di documenti che si trovano ancora nel periodo di protezione e che non erano già accessibili al pubblico prima della loro consegna (cfr. art. 9 cpv. 2 BGA), nell'ambito dell'elaborazione delle richieste di accesso ai sensi dell'art. 13 BGA, l'autorità che li ha consegnati verificherà innanzitutto, ai sensi dell'art. 13 cpv. 1 lett. b, se non vi siano interessi privati preponderanti che impediscano l'accesso prima della scadenza del periodo di protezione e se, eventualmente, l'accesso debba essere concesso a condizioni e requisiti, come l'anonimizzazione dei dati personali (art. 13 cpv. 3 BGA).

Con l'entrata in vigore del BGA nel 1999, le questioni relative alla protezione dei dati nel settore dell'archiviazione sono state affrontate anche dal punto di vista dell'archiviazione. Con l'introduzione del regolamento sul periodo di protezione e la possibilità così creata di estendere il periodo di protezione per l'ispezione dei documenti in determinati casi (artt. 11 e 12 BGA), il BGA mirava esplicitamente all'"armonizzazione". Poiché i documenti d'archivio non possono essere modificati (art. 14 cpv. 4 LADP), la nota di rifiuto ai sensi dell'art. 15 cpv. 3 LADP integra il regolamento sul periodo di protezione. Inoltre, ai sensi dell'art. 14 cpv. 2 BGA, la consultazione dei dati personali da parte dell'autorità che crea o consegna l'archivio è limitata durante il periodo di protezione, a meno che non si applichino le eccezioni di cui all'art. 14 cpv. 1 (lett. a-d). Secondo il dispaccio sul BGA, ciò garantisce che "da un lato, gli interessi delle persone interessate devono essere protetti, ma dall'altro, la ricerca (storica) di interesse pubblico non deve essere ostacolata". 8

Il nuovo BGA ha quindi avuto un impatto sulla legge esistente sulla protezione dei dati. Tuttavia, fino al 2006, l'articolo 21 della legge sulla protezione dei dati regolava solo il trasferimento dei dati personali all'Archivio federale come eccezione per l'anonimizzazione e la distruzione. 9

Tuttavia, l'attuale articolo 38 LPD ha subito una modifica significativa nel 2008 (versione conforme al n. I della legge federale del 24 marzo 2006, in vigore dal 1° gennaio 2008). Di conseguenza, l'archiviazione dei dati personali non è più un caso eccezionale di distruzione o anonimizzazione. Al contrario, è stato fatto riferimento alla nuova legge federale sull'archiviazione, che è entrata in vigore nel frattempo. Questa legge introduce ora anche nella legge sulla protezione dei dati i concetti del mondo dell'archiviazione con i termini "offerta" o "offerta" e "valore archivistico". 10

Dal 2008, l'articolo 21 dell'aDSG, ora articolo 38 della nuova LPD, entrata in vigore il 1° settembre 2023, è rimasto sostanzialmente invariato, ma l'attuazione della legislazione sull'archiviazione a livello federale si è sviluppata in modo significativo nel corso di questo periodo, come dimostrano le spiegazioni seguenti. 11

B. Ambito di applicazione

L'art. 38 LPD si rivolge a tutti gli organi federali ai sensi dell'art. 2 cpv. 1 lett. b LPD. All'art. 1 cpv. 1, la RICA elenca tutti gli organi la cui archiviazione è 12

disciplinata dalla RICA. Destinatario della norma è anche il Tribunale federale, che ai sensi dell'art. 1 cpv. 3 regolamenta autonomamente l'archiviazione dei propri documenti, ma lo fa nel rispetto dei principi dell'ArchA e previa consultazione dell'Archivio federale svizzero (AFS).

13 Indirettamente, l'art. 38 LPD può essere rilevante anche per i creatori di documenti ai sensi dell'art. 17 cpv. 2 dell'ArchA, ossia per le persone di diritto privato o pubblico di importanza nazionale che consegnano volontariamente i loro documenti all'AFS per una conservazione e comunicazione sicura e adeguata. Di norma, nei relativi contratti di donazione e deposito si fa riferimento al fatto che i documenti sono soggetti alle stesse disposizioni di consultazione dei documenti dello Stato federale (art. 9 e segg. della Legge federale sull'archiviazione, LAC). Si può quindi supporre che, salvo accordi diversi tra il creatore dell'archivio e l'AFS, i documenti di archivi privati che costituiscono o contengono dati personali e sono degni di essere archiviati possano essere sottoposti all'AFS anche per analogia con l'art. 38 LPD e, in particolare, applicando il regolamento sul periodo di protezione ai sensi degli artt. 9 e segg.

14 Per quanto riguarda la questione se l'art. 38 LPD possa applicarsi solo ai dati personali ottenuti o trattati in modo lecito, occorre sottolineare, come hanno fatto Epiney e altri, che la richiesta di distruzione sistematica di documenti che contengono o rappresentano dati personali ottenuti e trattati in modo totalmente o parzialmente illecito può essere contrastata, a seconda della situazione iniziale, da un interesse pubblico alla conservazione di documenti creati dall'amministrazione in modo illecito. Inoltre, una regolamentazione così rigida comprometterebbe i principi e gli obiettivi del BGA e le richieste di accesso da parte delle persone interessate, ad esempio per quanto riguarda le richieste di risarcimento. Gli archivi della sicurezza dello Stato, ad esempio, che sono stati consegnati all'AFS, sono documenti federali preziosi dal punto di vista giuridico, politico e storico, che documentano le pratiche commerciali delle autorità federali, come previsto dall'art. 2 cpv. 1 dell'ArchA.

C. Termini

15 Quando la legislazione sugli archivi e quella sulla protezione dei dati entrano in contatto - come nell'art. 38 LPD - si scontrano prospettive e mondi concettuali diversi. La legislazione sugli archivi si basa sul concetto di "record". Secondo l'art. 3 cpv. 1 LDA, i documenti sono "tutte le informazioni

registrate, indipendentemente dal supporto dell'informazione, che sono state ricevute o create nell'adempimento dei compiti pubblici della Confederazione, nonché tutti i sussidi e i dati supplementari necessari alla comprensione di tali informazioni e al loro utilizzo". La legislazione sulla protezione dei dati si riferisce invece ai dati personali, definiti all'art. 3 lett. a LPD come "qualsiasi informazione relativa a una persona identificata o identificabile". Si pone quindi la questione del rapporto tra questi due termini. Per le spiegazioni che seguono, si ipotizza che i dati personali siano sia una sottocategoria che una possibile caratteristica delle informazioni registrate (documenti). In altre parole, i dati personali sono sempre documenti ai sensi del BGA. Al contrario, i documenti possono contenere dati personali, ma non devono necessariamente contenerli.

L'articolo 38 LPD getta un altro ponte verso il BGA con l'uso dei termini "offerta" e "proposta". Tuttavia, i termini "offerta" e "offerta" sono utilizzati in modo diverso nella FADP e nella corrispondente legislazione di attuazione, e il loro significato è cambiato in una certa misura negli ultimi quindici anni. 16

Da un lato, l'AFS fa riferimento alle "autorità obbligate a offrire" e quindi, in combinato disposto con l'art. 1 cpv. 1 dell'AFS, delinea il rapporto tra l'AFS e le autorità federali che sono soggette all'obbligo di impartire istruzioni e sono obbligate a offrire all'AFS. D'altra parte, i termini "offerta" e "offerta" descrivono anche fasi di lavoro nel ciclo di vita dei documenti. Queste fasi sono legate alla valutazione dei documenti e sono oggetto di un cambiamento significativo nella prassi, il passaggio dalla valutazione retrospettiva a quella prospettica, descritto nel concetto generale di valutazione dell'Archivio federale nel 2010. Questo cambiamento di prassi è discusso nei capitoli seguenti. 17

III. OFFERTA DI DOCUMENTI NEL CONTESTO DELLA VALUTAZIONE PROSPETTICA (CPV. 1)

Il concetto globale di valutazione dell'Archivio federale, pubblicato nel 2010, prevede in linea di principio l'abbandono della valutazione retrospettiva a favore di quella prospettica. 18

Mentre la valutazione retrospettiva consiste nel valutare il valore archivistico di documenti già creati, la valutazione prospettica consiste nel valutare i documenti prima della loro creazione. Questa valutazione avviene durante lo 19

sviluppo o la revisione dei sistemi di classificazione ai sensi degli articoli 7 e 8 dell'ordinanza GEVER. I sistemi organizzativi sono elaborati dagli organi federali e, nel caso degli organi soggetti all'obbligo di offerta, sono esaminati e approvati dall'AFS, a condizione che soddisfino i requisiti dell'ArchA e le disposizioni di attuazione della LOGA. In un sistema di classificazione, le serie di documenti vengono valutate a livello di categoria, vale a dire che si stabilisce se i documenti che si presenteranno nel corso delle mansioni di un'agenzia federale sono completamente, parzialmente (selezione o campionamento) o per nulla degni di essere archiviati. Vengono valutati solo i documenti rilevanti per l'azienda; i documenti non rilevanti per l'azienda non sono considerati documenti ai sensi del BGA e non sono soggetti all'obbligo di offerta.

20 Il passaggio alla valutazione prospettica non è stato privo di conseguenze per il significato del termine "offerta" o "offerta". Nel caso della valutazione retrospettiva in applicazione dell'art. 6 cpv. 1 dell'ArchA, le serie di documenti esistenti sono state offerte all'AFS dalle agenzie archivistiche non indipendenti con una proposta di valutazione giuridico-amministrativa (offerta di acquisizione) e l'AFS ha anche effettuato una valutazione retrospettiva dal punto di vista delle scienze storico-sociali.

21 Con l'introduzione della valutazione prospettica, le "offerte" vengono fatte all'AFS in due momenti diversi del ciclo di vita dei documenti. La valutazione dei documenti avviene nell'ambito dello sviluppo o dell'aggiornamento di un sistema di classificazione e va intesa come un'offerta di valutazione. I documenti creati successivamente e meritevoli di essere archiviati vengono presentati al SFA per l'inoltro in un secondo momento (ad esempio, trasmissione dei Submission Information Packages SIP contenenti i file con i metadati e i dati di indicizzazione per l'inoltro di documenti elettronici o scatole d'archivio contenenti i fascicoli cartacei per l'inoltro di documenti cartacei). Dall'introduzione della valutazione prospettica, la valutazione dei documenti in collaborazione tra i creatori dei fascicoli e l'AFS e la trasmissione o la presentazione dei documenti all'AFS non coincidono più.

22 Come indicato sopra, sia nella valutazione retrospettiva, praticata prevalentemente prima del 2010, sia nella valutazione prospettica dopo il 2010, l'agenzia federale interessata partecipa alla valutazione insieme all'AFS. L'agenzia federale che crea il fascicolo valuta i documenti per categoria dal punto di vista giuridico-amministrativo. Questa valutazione è di competenza

della direzione degli uffici federali interessati e garantisce che vengano presi in considerazione gli aspetti tecnici, giuridici e politici. In una seconda fase, l'AFS esamina la valutazione giuridico-amministrativa dell'autorità che ha creato il fascicolo ed effettua anche una valutazione secondo i criteri delle scienze storico-sociali. Se una delle due valutazioni è positiva, i documenti sono considerati archiviabili (in toto o in parte sotto forma di campionamento o selezione). In casi eccezionali, la valutazione prospettica può essere oggetto di una successiva revisione.

IV. DATI PERSONALI NON PIÙ NECESSARI IN MODO PERMANENTE (CPV. 1)

La letteratura tratta spesso la questione di quando i dati personali non sono più necessari in modo permanente senza fare riferimento al contesto documentale. Questo approccio è difficilmente attuabile nella pratica. Questo perché i dati personali sono sempre documenti ai sensi del BGA, a meno che non siano irrilevanti per l'azienda. L'art. 6 della FADP stabilisce che i documenti devono essere presentati all'AFS quando non sono più necessari in modo permanente. 23

Se si ipotizzasse che la questione del momento in cui i dati personali non sono più necessari in modo permanente debba essere risolta in modo diverso da quella del momento in cui i documenti non sono più necessari in modo permanente, se ne dedurrebbe che i documenti meritevoli di archiviazione che contengono o rappresentano dati personali potrebbero dover essere trasmessi all'AFS in un momento diverso rispetto ai documenti che non contengono o rappresentano dati personali. Tuttavia, l'AFS parte dal presupposto che il fascicolo aziendale sia l'unità rilevante per l'archiviazione. A questo proposito, i dossier aziendali sono spesso di natura mista: sono costituiti da documenti che contengono dati personali e da documenti che non contengono o rappresentano dati personali. È quindi opportuno che le autorità federali si interroghino sul momento in cui i dati personali non sono più necessari in modo permanente nell'ambito dei documenti e che osservino le disposizioni di attuazione della LADP a questo proposito. 24

Ai sensi dell'art. 4 cpv. 1 OBGA, i documenti si considerano non più necessari in modo permanente se l'organo tenuto a fornirli non ne fa più un uso frequente e regolare, ma al più tardi cinque anni dopo l'ultima aggiunta al 25

fascicolo. L'art. 3 cpv. 1 delle direttive sull'obbligo di offerta e sulla consegna di documenti all'Archivio federale svizzero del 28 settembre 1999 stabilisce inoltre che gli enti soggetti all'obbligo di offerta devono rivedere regolarmente, ma almeno ogni cinque anni, i loro archivi e i loro depositi di informazioni per quanto riguarda i documenti di cui non hanno più bisogno in modo frequente e regolare. L'art. 4 cpv. 2 VBGA e l'art. 3 cpv. 2 delle direttive regolano l'estensione di questo periodo. L'art. 4 cpv. 3 VBGA e l'art. 3 cpv. 3 delle direttive disciplinano anche i casi di riduzione dei termini. Per alcune categorie di documenti si applicano requisiti più specifici ai sensi dell'art. 4 cpv. 3 OBGA e dell'art. 4 delle direttive.

26 Dall'introduzione della valutazione prospettica nel 2010, questi termini sono da intendersi come il termine per la presentazione all'AFS di documenti già valutati, ossia meritevoli di archiviazione.

V. DISTRUZIONE DEI DOCUMENTI NON MERITEVOLI DI ARCHIVIAZIONE (CPV. 2)

27 Per quanto riguarda il processo di distruzione, si fa riferimento all'art. 5 lett. d e all'art. 6 cpv. 4 LPD.

28 L'espressione "dati personali designati dall'Archivio federale come non meritevoli di archiviazione" utilizzata nel paragrafo 2 dell'art. 21 è fuorviante perché, come spiegato sopra, la valutazione dei documenti (e quindi anche dei dati personali) non viene effettuata solo dall'AFS, ma dall'autorità che crea l'archivio insieme all'AFS. Dall'introduzione della valutazione prospettica nel 2010, nel momento in cui i documenti vengono archiviati nel sistema di gestione elettronica dei documenti (GEVER), è chiaro dal collegamento tra il fascicolo aziendale corrispondente (o una domanda specializzata) e una categoria del sistema di classificazione valutato se i documenti che contengono o rappresentano dati personali sono degni di essere archiviati (in parte o completamente) o meno.

29 In questo contesto, va ricordato che la distruzione dei documenti deve essere registrata e che i relativi verbali di cassazione devono essere presentati all'AFS.

VI. ANONIMIZZAZIONE DEI DATI PERSONALI (CPV. 2 LETT. A)

Per quanto riguarda il termine anonimizzazione, si rimanda al commento dell'art. 2 cpv. 1 lett. a LPD e dell'art. 6 cpv. 4 LPD. Il cpv. 2 lett. a LPD consente alle autorità federali di conservare i documenti non meritevoli di archiviazione o quelli solo parzialmente meritevoli di archiviazione (campionatura o selezione) che non sono più necessari in modo permanente, oppure di conservarli integralmente, a condizione che siano resi anonimi. Tuttavia, dopo il passaggio all'amministrazione elettronica degli affari, tale conservazione può essere solo temporanea e non un'archiviazione ai sensi dell'ArchA, poiché le autorità federali hanno a disposizione l'infrastruttura necessaria per un'archiviazione elettronica a lungo termine solo nell'ambito dell'assoggettamento all'AFS. 30

VII. CONSERVAZIONE A FINI PROBATORI O DI SICUREZZA, SALVAGUARDIA DEI LEGITTIMI INTERESSI DELL'INTERESSATO (CPV. 2 LETT. B)

Nell'ambito della valutazione giuridico-amministrativa, l'ente che crea il fascicolo deve verificare se i documenti devono essere conservati in modo permanente. Il coinvolgimento dei creatori dei file ha lo scopo di garantire che "gli aspetti tecnici, legali e politici siano attentamente presi in considerazione nella valutazione". Dal punto di vista giuridico-amministrativo, i documenti sono degni di essere archiviati in particolare se servono come prova della pratica commerciale, hanno rilevanza giuridica o servono a garantire la certezza del diritto. 31

Se i documenti che contengono dati personali o che costituiscono dati personali devono essere conservati a fini probatori o di sicurezza o per tutelare i legittimi interessi delle persone interessate, in genere sono già stati valutati come valore archivistico nella valutazione giuridico-amministrativa. Di conseguenza, come nei casi di cui all'art. 38 cpv. 2 lett. a LPD, sono da prevedere come casi di applicazione dell'art. 38 cpv. 2 lett. b LPD solo i dati personali contenuti in documenti o che costituiscono documenti che sono stati giudicati non meritevoli di archiviazione nella valutazione prospettica o che non fanno parte del campione da archiviare o della selezione da archiviare in caso di valore archivistico parziale. Ad esempio, sono ipotizzabili 32

documenti contabili non meritevoli di archiviazione e utilizzati come prove in procedimenti in corso o imminenti.

VIII. ATTUAZIONE CON MALINTESI

33 Nella pratica, tuttavia, l'art. 38 LPD non è ancora coerentemente inteso in questo senso, come si evince dalla letteratura e dalla giurisprudenza. Nella decisione A-4236/2021 del TAF del 21 marzo 2023, che fa riferimento all'art. 21 ADSG, ad esempio, l'AFC, che dispone di un sistema di archiviazione approvato, prende posizione in relazione a una richiesta di distruzione dei dati, affermando che l'AFC "può decidere autonomamente" quando i dati legittimamente elaborati devono essere consegnati all'Archivio federale. Una parte non può chiedere che i dati personali legittimamente elaborati siano offerti all'Archivio federale o distrutti. Non è quindi obbligata a offrire o distruggere all'Archivio federale, su richiesta del ricorrente, i dati personali legalmente trattati di un dossier la cui ultima aggiunta al fascicolo risale al 2020". L'AFC fa quindi riferimento alle scadenze previste dall'AFC e dalla legislazione di attuazione dell'AFC, ma allo stesso tempo omette di sottolineare che i documenti in questione sono già stati valutati dall'AFC e dall'AFS.

34 Nella sua decisione del 21 marzo 2023, anche il Tribunale amministrativo federale segue la prassi di valutazione precedente al 2010 e scrive: "Non spetta al Tribunale amministrativo federale chiarire la questione del valore archivistico dei dati raccolti dall'istanza inferiore nel procedimento di assistenza amministrativa come prima istanza nel procedimento di ricorso, tanto più che la responsabilità di questa decisione non spetta all'istanza inferiore, ma all'Archivio federale, che non ha ancora potuto esprimersi in merito. [...] L'istanza inferiore deve offrire i dati raccolti nel corso della procedura di assistenza amministrativa all'Archivio federale e, se quest'ultimo li classifica come archiviabili, consegnarli. Se i dati non sono classificati come degni di essere archiviati, l'istanza inferiore deve distruggerli".

35 Questa recente decisione del Tribunale amministrativo federale è un esempio dei malintesi che la versione attuale dell'art. 38 cpv. 1 LPD può generare: L'art. 38 cpv. 1 LPD sembra suggerire - almeno secondo l'interpretazione dell'AFC e del TAF - che gli enti obbligati a offrire dati personali, in questo caso sotto forma di dossier aziendale su un caso fiscale relativo a una persona specifica, possano distruggere tali dati solo se l'AFS si è pronunciata in modo specifico

su questo singolo dossier e sulla sua valutazione. Ciò non è compatibile con la prassi di archiviazione dell'AFS per i seguenti motivi:

a) Nel caso in esame, l'AFC, che è tenuta a offrire, e l'AFS hanno già effettuato una valutazione prospettica al momento dell'elaborazione del sistema normativo dell'AFC nel 2015. Il fatto che i documenti derivanti da questa specifica attività dell'AFC (scambio di informazioni in materia fiscale) siano o meno degni di essere archiviati si evince dal sistema di classificazione dell'AFC o dal collegamento del fascicolo aziendale in questione a una sezione del sistema di classificazione. L'AFS e l'AFC hanno quindi già stabilito se la serie di documenti a cui appartiene il dossier o il documento in questione è archiviabile (in parte o in toto) o meno.

b) La valutazione, sia prospettica che retrospettiva, si riferisce a serie di documenti che nascono nell'adempimento di compiti specifici e, se del caso, ad applicazioni specialistiche - ma non a singole registrazioni di dati, a singoli dati personali, a singoli documenti o a dossier aziendali. In altre parole: Il modo in cui vengono create queste serie di documenti e, in particolare, la forma in cui i documenti vengono archiviati nei fascicoli è di competenza dell'Autorità federale per la protezione dei dati ai sensi dell'art. 2 cpv. 2 e dell'art. 5 cpv. 2 e 3 BGA in combinato disposto con l'art. 3 VBGA e l'art. 3 VBGA. L'art. 3 VBGA nonché l'art. 6 dell'ordinanza GEVER e l'art. 22 RVOV rientrano nell'ambito di responsabilità delle autorità tenute a offrire o creare file. Queste sono tenute a garantire la tracciabilità e la verificabilità delle loro attività commerciali nei loro registri.

Se, nel caso citato, la serie di documenti corrispondente fosse stata valutata 36
nel sistema normativo dell'AFC come degna di essere archiviata o parzialmente degna di essere archiviata (selezione o campionamento), l'ufficio di creazione dei fascicoli dovrebbe solo decidere, in applicazione dell'AFS e delle disposizioni di attuazione dell'AFS, quando il fascicolo in questione deve essere sottoposto all'AFS. Inoltre, in questo caso, l'ufficio che crea il fascicolo deciderà se il documento in questione è necessario per la tracciabilità e la verificabilità delle attività commerciali in questo fascicolo. Nel caso di valore archivistico parziale, l'autorità che crea il fascicolo attuerebbe anche i criteri di selezione o campionamento stabiliti nel SFA. In questa costellazione, anche l'AFS non sarebbe più autorizzata a prendere una decisione dopo aver effettuato la valutazione prospettica.

37 Se la serie di documenti corrispondente fosse stata valutata non degna di essere archiviata, l'autorità che crea il fascicolo deciderebbe anche cosa fare del documento o del fascicolo aziendale in questione contenente dati personali. In altre parole, se debba essere conservato temporaneamente in forma anonima ai sensi dell'art. 38 cpv. 2 lett. a LPD o in forma non anonima ai sensi dell'art. 38 cpv. 2 lett. b LPD per scopi probatori e di sicurezza o per tutelare gli interessi dell'interessato meritevole di protezione. Anche in questo caso, l'AFS non sarebbe più autorizzata a prendere una decisione dopo l'esecuzione della valutazione prospettica.

38 In questo contesto, l'art. 8 cpv. 1 dell'ArchA va inteso nel senso che solo i documenti che non sono stati offerti all'AFS per una valutazione (prospettica) non possono essere distrutti senza il consenso dell'AFS. Considerato l'obbligo generale di offrire i documenti all'AFS, è probabile che tali documenti siano rari.

IX. VALUTAZIONE

39 L'art. 38 LPD risale agli anni '80 ed è stato concepito come strumento per impedire ai creatori di archivi di utilizzare il pretesto della protezione dei dati per ritirare dall'archiviazione dell'AFS documenti degni di essere archiviati che contengono dati personali o che rappresentano dati personali solo sulla base di questo fatto. L'art. 38 LPD è ancora oggi di rilevanza pratica, in quanto la disposizione specifica il principio del trattamento proporzionato dei dati in relazione all'archiviazione: Non solo l'anonimizzazione o la distruzione di documenti non meritevoli di archiviazione che contengono dati personali o che rappresentano dati personali è proporzionata una volta completato il trattamento necessario da parte delle autorità che hanno creato il fascicolo, ma anche l'invio di tali documenti (non anonimizzati) all'AFS, purché siano meritevoli di archiviazione.

40 Nella sua versione attuale, l'art. 38 cpv. 1 LPD si basa sulla prassi della valutazione retrospettiva, che fino agli anni Duemila era la prassi standard dell'AFS. Da quando si è passati alla valutazione prospettica come processo standard, tutti i servizi federali valutano i loro documenti in base all'art. 1 cpv. 1 LADP da un punto di vista giuridico-amministrativo e l'AFS da un punto di vista storico-scientifico nell'ambito dello sviluppo dei sistemi di classificazione, vale a dire prima della creazione dei documenti.

Sotto il titolo "Archiviazione dei dati personali", un articolo 38 rivisto potrebbe in futuro limitarsi ad affermare che i documenti ai sensi dell'ArchA possono contenere o costituire dati personali e devono essere trattati in conformità ai requisiti dell'ArchA (paragrafo 1). Un nuovo cpv. 2 potrebbe stabilire che i documenti non meritevoli di archiviazione che contengono o rappresentano dati personali devono essere distrutti, a meno che non si applichino le condizioni di cui all'attuale cpv. 2, lettere a e b. 41

L'autore desidera ringraziare l'ISc MAS Barbara Kräuchi per lo stimolante scambio di competenze nel corso delle ricerche per questo articolo.

BIBLIOGRAFIA

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).

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 39 LPD

Un commentario di Philipp do Canto

CITAZIONE SUGGERITA

Philipp do Canto, Commentario all'art. 39 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-do Canto, art. 39 LPD N. XXX.

Art. 39 Trattamento di dati personali per scopi impersonali

[1] Gli organi federali hanno il diritto di trattare dati personali per scopi impersonali, in particolare nei settori della ricerca, della pianificazione o della statistica, se:

a. rendono anonimi i dati non appena lo scopo del trattamento lo permette;

b. comunicano a privati i dati personali degni di particolare protezione soltanto in una forma che non permetta d'identificare le persone interessate;

c. il destinatario trasmette a terzi i dati soltanto con l'autorizzazione dell'organo federale che glieli ha comunicati; e

d. i risultati sono pubblicati soltanto in una forma che non permetta d'identificare le persone interessate.

[2] Gli articoli 6 capoverso 3, 34 capoverso 2 e 36 capoverso 1 non sono applicabili.

STRUTTURA

In breve 498
I. Informazioni generali 498
II. Cpv. 1, requisiti in dettaglio 499
A. Reato base: scopo non personale 499
B. Cpv. a, anonimizzazione più precoce possibile 500
C. Cpv. b, Dati particolarmente sensibili 501
D. Cpv. c, obbligo di consenso per la divulgazione 501
E. Cpv. d, Pubblicazione dei risultati 502
III. Cpv. 2, eccezioni 502
IV. Legislazione speciale 503
A. Legge federale sulla statistica 503
B. Legge sull'armonizzazione dei registri 504
C. Sistemi informativi di polizia 504
D. Legge sulla ricerca umana e ricerca all'ETH 504
E. Archivi della Confederazione 505
Bibliografia 505
I Materiali 506

IN BREVE

L'art. 39 LPD autorizza gli organi federali a trattare dati per scopi non personali a determinate condizioni. La norma concede agevolazioni ai sensi del "privilegio della ricerca" per la ricerca, la statistica, la pianificazione e altri settori. La motivazione è il grande interesse pubblico delle attività in questione. Il privilegio si applica solo se sono soddisfatte le condizioni generali. In primo luogo, l'art. 39 cpv. 1 LPD richiede la più rapida anonimizzazione possibile dei dati personali trattati. In secondo luogo, è necessario il consenso dell'organo federale per la divulgazione dei dati del destinatario a terzi. In terzo luogo, come nel caso del trattamento di dati privati ai sensi dell'art. 31 cpv. 2 lett. e LPD, gli enti federali possono pubblicare i risultati di ricerche o altro solo in modo tale che le persone interessate non possano essere identificate.

Poiché l'identità delle persone interessate non è coinvolta nel trattamento dei dati non personali, l'art. 39 cpv. 2 LPD dichiara che importanti principi non sono applicabili. Ad esempio, il requisito della limitazione delle finalità e il requisito della base giuridica non si applicano in alcune costellazioni, ad esempio per la divulgazione di dati personali. D'altro canto, è necessario osservare numerose disposizioni giuridiche speciali, in particolare nel settore della statistica e della ricerca, che relativizzano il significato pratico dell'art. 39 LPD.

I. INFORMAZIONI GENERALI

1 L'art. 39 LPD sul trattamento dei dati a fini non personali da parte degli organi federali riprende in larga misura la disposizione precedente dell'art. 22 aDSG con il cosiddetto "**privilegio della ricerca**". La novità è rappresentata da un chiarimento sui dati personali particolarmente sensibili. Ai sensi dell'art. 39 LPD, gli organi federali dovrebbero (continuare a) beneficiare di semplificazioni per il trattamento a fini non personali se rispettano le condizioni quadro. Questo privilegio è giustificato dall'interesse pubblico nelle attività pertinenti dello Stato. La ricerca e le statistiche sono alla base di tutti gli aspetti della vita pubblica.

2 Le **condizioni per l'agevolazione** includono, da un lato, l'obbligo di anonimizzazione il più presto possibile (cpv. 1 lett. a). In secondo luogo,

devono essere rispettate le condizioni relative alla divulgazione di dati personali particolarmente sensibili a terzi (cpv. 1 lett. b). Poi c'è il requisito del consenso del destinatario alla divulgazione (cpv. 1 lett. c) e infine il requisito della non identificabilità quando si pubblicano i risultati (cpv. 1 lett. d). L'art. 39 cpv. 2, dichiara che alcuni principi della LPD non sono applicabili a causa della riduzione dei rischi nel caso di trattamento di dati non personali (cpv. 2).

La disposizione si riferisce solo al **trattamento dei dati da parte degli organi federali**. La disposizione cita la ricerca, la statistica e la pianificazione come aree privilegiate, sebbene l'elenco non sia esaustivo. Oltre alle statistiche federali, sono comprese le ricerche condotte dalle istituzioni federali o per loro conto, la pianificazione territoriale e dei trasporti, la Banca nazionale, la gestione della migrazione e la sanità pubblica. A differenza del settore privato, la ricerca medica, disciplinata dalla legge sulla ricerca umana, tende a passare in secondo piano, poiché questo settore è sostenuto principalmente dagli ospedali universitari cantonali e dalla ricerca farmaceutica privata. È invece coperta la ricerca condotta dal settore dei PF come unità federale decentralizzata. 3

A causa del requisito di una base giuridica per il trattamento dei dati statali, le varie attività sono ora ampiamente **regolamentate da una legislazione specializzata** (infra, IV). L'art. 39 LPD perde quindi il suo significato indipendente in numerose costellazioni o deve essere letto in combinazione con le disposizioni specifiche del soggetto. 4

II. CPV. 1, REQUISITI IN DETTAGLIO

A. Reato base: scopo non personale

L'elemento centrale della disposizione è il trattamento per scopi non personali. Per finalità non personali si intendono finalità per le quali l'**identità della persona interessata è irrilevante**. In altre parole, lo scopo dell'attività è soddisfatto anche se vengono trattati dati anonimizzati o criptati. Il trattamento dei dati di ampie fasce della popolazione e di singoli gruppi è coperto, purché riguardi solo le caratteristiche e non l'identità delle persone registrate. Se vengono trattati solo dati di fatto o dati precedentemente anonimizzati, la disposizione non è applicabile. 5

6 L'esplicita menzione delle aree non significa che il trattamento dei dati nelle aree di ricerca, statistica e pianificazione abbia finalità non personalizzate. In particolare, esistono attività di trattamento che hanno **anche finalità personali**. Per tali attività, l'art. 35 OPDa stabilisce che le eccezioni di cui all'art. 39 cpv. 2 LPD si applicano solo al trattamento per scopi non personali.

7 La frase introduttiva del cpv. 1 contiene la conseguenza giuridica, ossia l'**autorizzazione** semplificata **del trattamento dei dati** se sono soddisfatti i requisiti della disposizione, illustrati di seguito.

B. Cpv. a, anonimizzazione più precoce possibile

8 Gli organi federali devono (in linea di principio) **rendere anonimi** i dati non appena lo scopo del trattamento lo consente. La disposizione riprende quindi il principio dell'art. 6 cpv. 4 LPD. Non viene specificato un termine per l'anonimizzazione. Un regolamento generale e astratto non soddisferebbe le esigenze di statistica, ricerca e pianificazione.

9 A differenza dell'art. 31 cpv. 2 lett. e LPD, non è stata inserita alcuna eccezione che consenta altre misure per impedire l'identificabilità della persona se l'anonimizzazione è impossibile o sproporzionata. Le opinioni divergono sulla questione se sia sufficiente **la pseudonimizzazione** o la crittografia dei dati personali. Se è disponibile un codice o una chiave con cui i dati personali (parzialmente) anonimizzati possono essere nuovamente identificati, si parla di pseudonimizzazione. Alcuni studiosi vogliono consentire la crittografia solo se il trattamento porta alla fine all'anonimizzazione. Il punto di vista opposto si basa sulla necessità diffusa nella pratica di poter risalire all'identità della persona interessata, che si oppone all'anonimizzazione, soprattutto a quella precoce. Inoltre, l'anonimizzazione generale non è in linea con la lettera b, secondo cui per i dati personali particolarmente sensibili è sufficiente che non possano essere identificati quando vengono comunicati a privati, il che consente anche la crittografia. Se la crittografia o l'"anonimizzazione di fatto" è sufficiente per la divulgazione di dati particolarmente sensibili, ciò dovrebbe valere anche *per* i dati meno sensibili. Il messaggio sull'aDSG menziona la necessità di una pseudonimizzazione. Una decisione della Corte Suprema Federale non risponde alla domanda in modo definitivo, ma vede la soluzione nello scopo della rispettiva procedura: "Ci sono, ovviamente, dei limiti all'occultamento. Non deve portare a una sentenza non più comprensibile. Non si può quindi escludere completamente che le persone che conoscono i

dettagli del caso siano in grado di riconoscere chi è coinvolto nonostante l'occultamento". Se l'anonimizzazione elimina quindi lo scopo del trattamento (che, tuttavia, non deve sempre essere personale), dovrebbero essere consentite anche altre misure appropriate per evitare che la persona sia identificabile.

C. Cpv. b, Dati particolarmente sensibili

Il secondo requisito riguarda la divulgazione di dati particolarmente sensibili a privati. Si tratta di una norma specifica che si aggiunge alle disposizioni generali sulla divulgazione dei dati di cui all'art. 36 LPD. Nel caso di dati particolarmente sensibili, si applica il principio secondo cui tali dati possono essere comunicati a terzi solo in modo tale che **la persona interessata non possa essere identificata**. Contrariamente alla formulazione della lettera a, in questo caso non è richiesta l'anonimizzazione, ma è sufficiente anche la cifratura preventiva per una maggiore protezione dei dati. 10

Per quanto riguarda le misure volte a impedire l'identificazione, occorre fare riferimento all'ampio catalogo di **misure tecniche e organizzative** di cui all'art. 3 dell'OPDa, in particolare alle norme sulla riservatezza e sull'integrità. Esistono anche diverse linee guida sulla crittografia, come le linee guida vincolanti di collegamento scientifico dell'Ufficio federale di statistica o le linee guida dell'Agenzia europea per la sicurezza informatica (Enisa). Le linee guida contengono, tra l'altro, requisiti per la gestione dei codici e per la de-pseudonimizzazione. 11

Anche le **norme di legge sulla riservatezza** svolgono un ruolo importante. Quando la legislazione speciale non autorizza la divulgazione di dati particolarmente sensibili (a soggetti privati), essa ha la precedenza come regolamento speciale. La lettera b non può quindi essere utilizzata come giustificazione per la divulgazione di dati soggetti a tutela del segreto. 12

D. Cpv. c, obbligo di consenso per la divulgazione

In terzo luogo, i dati possono essere divulgati per il trattamento a fini non personali. Tuttavia, ai sensi della lettera c, per la divulgazione dei dati è necessario il consenso dell'organismo federale. Il consenso dell'organo federale deve essere accompagnato dalla condizione che gli obblighi di anonimizzazione e pubblicazione siano trasferiti al terzo. 13

14 Per la **Banca nazionale** si applica la disposizione speciale dell'art. 16 cpv. 4bis LBN, in base alla quale la Banca nazionale è autorizzata a comunicare all'UST dati in forma non aggregata a fini statistici. In deroga all'art. 39 LPD, l'UST non può trasmettere i dati della Banca nazionale senza il suo consenso.

15 L'art. 39 cpv. 1 lett. c lascia aperta la **forma del consenso**. Secondo il messaggio dell'aDSG, il consenso può o deve essere dato per contratto o per ordine.

E. Cpv. d, Pubblicazione dei risultati

16 L'art. 16 lett. d riprende la precedente disposizione secondo cui le persone interessate non devono essere identificabili quando vengono pubblicati i risultati (art. 22 cpv. 1 lett. c aDSG). Nonostante la stessa formulazione dell'art. 31 cpv. 2 lett. e n. 3 LPD, per la pubblicazione è richiesta l'**anonimizzazione** (completa). Un'anonimizzazione parziale o una pseudonimizzazione, come avviene ad esempio nella ricerca medica sull'uomo, non è quindi sufficiente. Sono tuttavia possibili delle eccezioni se i dati si riferiscono a persone di storia contemporanea o se interessi superiori alla trasparenza richiedono l'accesso al file.

17 In dottrina si osserva che la pubblicazione di studi con un numero ridotto di soggetti può comportare il **rischio di trarre conclusioni** sull'individuo, ad esempio nel caso di statistiche relative a piccole aree geografiche. Tuttavia, questo sembra essere un problema minore quando si pubblicano risultati basati su dati provenienti da un numero elevato di soggetti, poiché è più difficile identificare la persona da un essere umano. I sistemi tecnologici, invece, funzionano indipendentemente dalle restrizioni geografiche o numeriche, per cui il progresso tecnico aumenta costantemente i requisiti per la pubblicazione dei risultati.

III. CPV. 2, ECCEZIONI

18 L'art. 39 cpv. 2 LPD dichiara inapplicabili tre disposizioni della LPD.

19 In primo luogo, non è applicabile il **requisito della limitazione dello scopo** o del divieto di cambiamento dello scopo ai sensi dell'art. 6 cpv. 3 LPD. Poiché i lavori di ricerca, pianificazione e statistica non hanno un impatto diretto sulle persone interessate ai sensi dell'art. 39 LPD, i dati possono essere utilizzati anche in un contesto diverso da quello per cui sono stati raccolti.

Tuttavia, il limite di utilizzo è fissato dall'art. 39 cpv. 1, secondo il quale i dati possono essere utilizzati solo per scopi non personalizzati. In questo quadro, i dati possono essere trattati per qualsiasi finalità lecita. In altre parole, l'eccezione non consente il trattamento per altri scopi personali.

La seconda eccezione è l'art. 34 cpv. 2 LPD. Di conseguenza, il **requisito di una base giuridica formale** non si applica al trattamento di dati e profili personali particolarmente sensibili o ad attività che rischiano di interferire gravemente con i diritti fondamentali. Il principio di legalità non è quindi completamente eliminato. L'art. 34 cpv. 1 LPD rimane applicabile. Pertanto, per questo tipo di trattamento è ancora richiesta una base giuridica a livello di ordinanza. 20

La terza eccezione riguarda l'art. 36 cpv. 1 LPD sulla divulgazione dei dati personali. Di conseguenza, **non è richiesta alcuna base giuridica specifica** per la **divulgazione dei dati personali**. A parte il fatto che l'art. 39 cpv. 1 LPD contiene requisiti per la divulgazione dei dati personali, i requisiti dovranno essere rispettati regolarmente anche in base alla legislazione speciale. In mancanza di una normativa, un organo federale può avvalersi di questa eccezione. Tuttavia, il principio di legalità della divulgazione non è annullato da questa disposizione. 21

IV. LEGISLAZIONE SPECIALE

A causa del già citato **requisito di una base giuridica** per il trattamento dei dati statali, esiste un'ampia legislazione speciale che disciplina le attività degli organi federali. A seconda del livello di dettaglio, queste possono sostituire in larga misura l'art. 39 LPD, farvi riferimento o integrare la disposizione. 22

A. Legge federale sulla statistica

L'art. 19 cpv. 2 LStat contiene una disposizione quasi identica sulla divulgazione di dati per scopi non personalizzati ai produttori di statistiche federali. La disposizione si limita alla divulgazione perché la Legge federale sulla statistica contiene disposizioni autorevoli sulla raccolta e l'elaborazione (art. 4 e segg. LStat). Oltre ai requisiti di cui all'art. 39 cpv. 1 LPD, l'art. 19 cpv. 2 lett. d LStat richiede il rispetto del **segreto statistico** e delle altre disposizioni sulla protezione dei dati. L'art. 16 cpv. 1 LStat chiarisce che le disposizioni in 23

materia di ricerca, statistica e pianificazione della LPD si applicano "in aggiunta", ossia in via sussidiaria, ai dati personali.

B. Legge sull'armonizzazione dei registri

24 Nel settore delle **statistiche demografiche**, la legge sull'armonizzazione dei registri (LRRa) è autorevole. L'armonizzazione dei registri serve a standardizzare e semplificare i registri comunali e cantonali per aumentarne l'utilità statistica e ridurre l'onere amministrativo. L'armonizzazione dei registri facilita anche i registri interessati. Essa consente lo scambio elettronico di dati tra i vari registri ufficiali, regolamentato per legge (cfr. art. 1 del LArRa).

C. Sistemi informativi di polizia

25 La polizia e le autorità giudiziarie gestiscono numerosi registri e sistemi informativi. I sistemi sono disciplinati dalla Legge federale sui sistemi informativi della polizia federale (FPSI). L'art. 6 cpv. 4 dell'IPB consente ai responsabili di conservare i dati anonimi destinati alla cancellazione, nella misura in cui ciò sia necessario a **fini statistici o di analisi criminale**. Tuttavia, la ricerca con i corrispondenti dati anonimizzati non rientra più nell'art. 39 LPD, in quanto non si tratta più di dati personali.

D. Legge sulla ricerca umana e ricerca all'ETH

26 È importante anche la legge sulla ricerca umana (attualmente in fase di revisione) con la LRMT e le leggi correlate, come la legge sulla registrazione dei tumori, che contengono disposizioni proprie sulla pseudonimizzazione e disposizioni di triage sull'applicazione della LRMT e della LPD (ad es. art. 28 LRMT). Particolarmente importante nel campo della ricerca è lo sviluppo del **consenso elettronico** (il cosiddetto e-consent, art. 8b HRA), che consente di rinunciare al consenso scritto a determinate condizioni. Il consenso elettronico riveste un ruolo particolare per il futuro riutilizzo nella ricerca, dove i progetti spesso non hanno (o non hanno più) finalità personali (art. 17 LRUm).

27 Infine, per il **settore dei PF**, l'art. 36c cpv. 1 della Legge sui PF stabilisce che i dati personali, compresi quelli particolarmente sensibili, possono essere trattati nell'ambito di progetti di ricerca, nella misura in cui ciò sia necessario

per il progetto corrispondente. Ai sensi del cpv. 2, deve essere rispettata la LPD.

E. Archivi della Confederazione

Infine, va menzionata la Legge federale sull'archiviazione (LAr), che contiene 28
il quadro normativo per gli archivi della Confederazione, in particolare per l'Amministrazione federale, il Parlamento e i tribunali federali. Per quanto riguarda i dati personali particolarmente sensibili contenuti in archivi non anonimizzati, l'art. 11 cpv. 1 LAr prevede un **periodo di protezione esteso a** 50 anni.

BIBLIOGRAFIA

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).

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 40 LPD

Un commentario di Anna Kuhn

CITAZIONE SUGGERITA

Anna Kuhn, Kommentierung zu Art. 40 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Kuhn, N. XXX zu Art. 40 DSG.

Art. 40 Attività di diritto privato di organi federali

Se un organo federale compie un'attività soggetta al diritto privato, il trattamento dei dati personali è retto dalle disposizioni applicabili ai privati.

STRUTTURA

In breve 509
I. Aspetti generali 509
A. Osservazioni preliminari 509
B. Finalità della legge e contesto 509
C. Storia delle origini 510
II. Ambito di applicazione 511
III. Azione sovrana e di diritto privato dello Stato 511
A. Categorizzazione dell'azione statale 511
B. L'azione sovrana come principio 511
C. Azione di diritto privato 512
1. Principi di base 512
2. Delimitazione in base al pluralismo dei metodi 513
3. Casi di azione consentita dal diritto privato 513
IV. Conseguenze legali 514
A. Disposizioni applicabili in materia di protezione dei dati 514
B. Questioni procedurali 515
C. Ulteriore applicabilità del diritto pubblico 515
1. Principi costituzionali 515
2. Impegno per i diritti fondamentali 515
3. Teoria a due fasi nella procedura di presentazione 516
V. Casistica 516
Bibliografia 518
I Materiali 518

IN BREVE

L'art. 40 LPD si applica quando gli organi federali agiscono in base al diritto privato ai sensi dell'art. 5 lett. i LPD. Ciò è possibile se un settore non è disciplinato in modo definitivo dal diritto pubblico e lascia quindi spazio ad azioni di diritto privato. Per determinare questo aspetto nel singolo caso, si deve innanzitutto esaminare l'esistenza di una regolamentazione giuridica speciale e quindi operare una demarcazione tra azioni di diritto sovrano e azioni di diritto privato. Con le attività di supporto amministrativo, l'amministrazione di beni finanziari, le attività statali del settore privato e parti dell'amministrazione dei servizi, sono emerse aree in cui l'azione di diritto privato da parte del settore pubblico è normalmente consentita e rilevante. Se si tratta di un'azione di diritto privato, gli organi federali sono soggetti alle disposizioni previste per i privati in caso di trattamento dei dati corrispondenti.

Tuttavia, anche applicando l'art. 40 LPD, le autorità pubbliche che agiscono in base al diritto privato non possono mai rinunciare completamente ai principi costituzionali. Ad esempio, l'obbligo di rispettare i diritti fondamentali o il principio di legalità continuano ad essere applicati.

I. ASPETTI GENERALI

A. Osservazioni preliminari

L'art. 40 LPD rimane invariato rispetto alla versione precedente (art. 23 cpv. 1 aDSG) e ha subito solo lievi modifiche redazionali. 1

Il precedente secondo paragrafo, secondo il quale la vigilanza è disciplinata dalle disposizioni per gli organi federali (art. 23 cpv. 2 aDSG), è stato eliminato senza sostituirlo. Il motivo è che la versione della LPD qui commentata prevede già lo stesso sistema di vigilanza per i privati e gli organi federali. 2

B. Finalità della legge e contesto

La LPD è concepita come una legge uniforme e disciplina il trattamento dei dati da parte di privati e di organi federali in un unico decreto. In quanto parte della comunità, gli organi federali sono generalmente soggetti a requisiti legali 3

più severi, che si applicano anche al trattamento dei dati personali e agli obblighi di protezione dei dati (cfr. art. 5 lett. i LPD).

4 L'art. 40 LPD rompe questa dicotomia. La disposizione stabilisce che gli organi federali che agiscono in base al diritto privato sono soggetti alle disposizioni meno severe della legge sulla protezione dei dati per i privati (in particolare il capitolo 5 LPD). La disposizione mira a garantire che gli organismi federali non subiscano svantaggi rispetto ai concorrenti privati quando partecipano alla concorrenza economica. Il legislatore affronta così il fatto che gli organi federali, in quanto soggetti di diritto privato, non esercitano un potere sovrano e che talvolta non esiste un rapporto di subordinazione con i privati che possa essere compensato da una veste giuridica più rigida.

5 L'art. 40 LPD è in un certo senso la controparte dell'art. 5 lett. i LPD, secondo cui i privati che svolgono funzioni pubbliche sono soggetti alle disposizioni più severe previste per gli organi federali (cfr. il commento all'art. 5 lett. i LPD).

C. Storia delle origini

6 Il progetto del Consiglio federale della prima legge federale sulla protezione dei dati del 1988 prevedeva già che le attività di diritto privato degli organi federali fossero soggette alle disposizioni per i privati. Questo principio è tuttora valido.

7 Durante le deliberazioni parlamentari sull'avamprogetto del 1988, il Consiglio degli Stati ha sostenuto che gli organi federali dovrebbero rimanere soggetti alle disposizioni per gli organi federali anche quando agiscono in base al diritto privato. Ciò con la riserva di concedere al Consiglio federale la competenza di disciplinare situazioni eccezionali. Il Consiglio degli Stati era preoccupato che disposizioni meno restrittive in materia di protezione dei dati non rendessero inutilmente attraente per le autorità pubbliche agire in base al diritto privato. Occorre inoltre garantire che le azioni di diritto privato degli organi federali - qualora si verifichino in casi eccezionali - poggino su una base giuridica. Dopo che il Consiglio nazionale ha appoggiato il progetto del Consiglio federale, il Consiglio degli Stati lo ha infine approvato. Tuttavia, ha imposto la condizione di inasprire i requisiti per la base giuridica degli organi federali di diritto privato.

La versione originale della LPD 1988 prevedeva che la vigilanza degli organi federali non sarebbe stata allentata nell'ambito delle attività di diritto privato. Pertanto, dovevano rimanere in vigore le stesse possibilità di vigilanza. Nella versione qui commentata, tuttavia, questa disposizione (art. 23 cpv. 2 aDSG) è stata eliminata senza sostituirla. Il motivo è la standardizzazione del regime di vigilanza per gli enti privati e federali. 8

II. AMBITO DI APPLICAZIONE

L'art. 40 LPD è legato al concetto di ente federale. Secondo l'art. 5 lett. i LPD, gli organi federali sono autorità e agenzie della Confederazione, nonché persone private incaricate di compiti pubblici (per i dettagli, si veda il commento all'art. 5 lett. i LPD). 9

In linea di principio, agli organi federali si applicano le disposizioni specifiche (in particolare il capitolo 6 LPD). Tuttavia, nel caso in cui un organo federale agisca a titolo privato, è soggetto alle disposizioni previste per i privati dall'art. 40 LPD (in particolare il capitolo 5 LPD). 10

III. AZIONE SOVRANA E DI DIRITTO PRIVATO DELLO STATO

A. Categorizzazione dell'azione statale

Le opinioni su come suddividere e classificare l'azione dello Stato sono tanto diverse quanto le manifestazioni dell'azione stessa. Nel contesto dell'art. 40 LPD, la suddivisione in "azione sovrana" e "azione di diritto privato" è rilevante, perché la disposizione richiede un'azione di diritto privato. La coppia di termini funge da controparte e descrive la forma dell'azione statale, non il suo oggetto e contenuto. 11

B. L'azione sovrana come principio

In linea di principio, lo Stato agisce in modo sovrano nell'adempimento dei suoi compiti. L'azione sovrana comprende il potere di determinare unilateralmente i diritti e gli obblighi dei privati ed è accompagnata da una superiorità dello Stato rispetto ai privati (rapporto di subordinazione). Un esempio di azione sovrana è l'emissione di decreti in cambio della conclusione di contratti di diritto privato. 12

13 Lo Stato agisce sovranamente, ad esempio, nell'ambito dell'amministrazione degli interventi. Ciò comporta un'ingerenza nei diritti e nelle libertà dei privati, che devono tollerarla. L'intervento serve direttamente all'adempimento di compiti pubblici. Ne sono un esempio l'esproprio o le restrizioni di polizia sulla proprietà della terra. Lo Stato agisce in modo sovrano anche in parti dell'amministrazione dei servizi, cioè quando servizi statali di natura economica e sociale sono forniti a privati (ad esempio, la fornitura di assicurazioni sociali statali). Inoltre, serve direttamente all'adempimento di compiti pubblici.

C. Azione di diritto privato

1. Principi di base

14 È indiscutibile che il settore pubblico possa agire anche in base al diritto privato in determinate costellazioni. Tuttavia, la possibilità che lo Stato agisca in base al diritto privato deve essere determinata caso per caso. Il punto di partenza è che lo Stato è sempre vincolato al principio di legalità nelle sue azioni (cfr. art. 5 cpv. 1 Cost.). In linea di principio, quindi, non ha alcuna autonomia nel configurare i propri rapporti giuridici. Se un'area del diritto è regolata in modo definitivo dal diritto pubblico, non c'è quindi spazio per un'azione di diritto privato. Ciò è possibile solo alle seguenti condizioni:

- Non esiste una regolamentazione definitiva di diritto pubblico.
- L'azione di diritto privato è la forma di azione appropriata per il rispettivo settore di competenza.

15 Nel contesto dell'art. 40 LPD, anche l'azione di diritto privato da parte di un organo federale è decisiva. L'azione di diritto privato è caratterizzata dal fatto che a un'attività non si applica alcuna norma di diritto pubblico, non esiste di conseguenza alcun rapporto di subordinazione e lo Stato e i terzi trattano sullo stesso piano (ad esempio, la conclusione di un contratto di diritto privato). Per contro, l'esistenza di un rapporto di concorrenza con i privati non è necessaria ai sensi dell'art. 40 LPD.

16 Nell'ambito del diritto della protezione dei dati, la natura giuridica del rapporto di base con l'interessato viene utilizzata per distinguere tra azioni di diritto privato e azioni di diritto pubblico. Questa distinzione spesso non è banale. Il pluralismo dei metodi può essere d'aiuto (cfr. infra, n. 18). Inoltre,

sono sorte alcune costellazioni di casi in cui lo Stato agisce normalmente in base al diritto privato (cfr. infra n. 21 e segg.).

2. Delimitazione in base al pluralismo dei metodi

In base al principio di legalità, per attribuire il rapporto di base tra l'interessato e l'ente pubblico al diritto pubblico o al diritto privato, occorre innanzitutto verificare se esiste una soluzione di diritto speciale che regoli tale questione (cfr. supra n. 14). 17

In caso contrario o se l'interpretazione della norma lascia dei dubbi, si possono consultare i criteri di delimitazione elaborati dalla dottrina e dalla prassi. In base a questo pluralismo di metodi, vengono esaminati i seguenti punti: 18

- Teoria dell'interesse: il rapporto giuridico è prevalentemente finalizzato al perseguimento di interessi privati o pubblici?
  Teoria della subordinazione: l'istituzione statale che agisce agisce in modo sovrano e quindi superiore rispetto alle parti private?
- Teoria funzionale: il rapporto giuridico ha come oggetto l'adempimento di un compito pubblico?
- Teoria modale: la violazione è sanzionata dal diritto civile o dal diritto pubblico?

Secondo la prassi, occorre esaminare separatamente per ogni singolo caso la teoria più adatta alla delimitazione. Secondo la giurisprudenza delle più alte corti, ad esempio, la teoria funzionale è considerata la più adatta per valutare la natura giuridica dei contratti. 19

3. Casi di azione consentita dal diritto privato

Nella pratica, sono emerse alcune aree di attività in cui l'autorità pubblica agisce normalmente (in modo lecito) in base al diritto privato. 20

Nel caso dell'attività di supporto amministrativo (detta anche amministrazione dei bisogni), l'autorità pubblica si procura le risorse materiali e umane necessarie per l'adempimento diretto dei compiti pubblici. L'attività di supporto amministrativo serve solo indirettamente all'adempimento delle funzioni pubbliche. Per l'attuazione, l'autorità pubblica stipula contratti di diritto privato. 21

22 Le attività finanziarie del settore pubblico comprendono tutti i beni realizzabili. Essi servono all'autorità pubblica solo indirettamente per la realizzazione della funzione pubblica e nella loro gestione agiscono in base al diritto privato. Ne sono un esempio la locazione di immobili sul mercato libero o la compravendita di titoli a scopo di investimento.

23 Se l'autorità pubblica agisce in base al diritto privato, partecipa alla vita economica e si trova in un rapporto di concorrenza con il settore privato. Nel rapporto esterno, cioè nell'interazione con la concorrenza, l'autorità pubblica agisce in base al diritto privato. Ne sono un esempio la gestione di un ristorante comunale o alcuni settori di attività delle banche cantonali.

24 Nel caso dell'amministrazione dei servizi, l'autorità pubblica fornisce servizi economici a privati. Agisce in base al diritto privato se la fornitura di servizi serve solo indirettamente al perseguimento di interessi pubblici, come nel caso dei contratti per il trasporto pubblico o per la fornitura di energia. D'altro canto, agisce in modo sovrano quando eroga le pensioni dell'AI.

IV. CONSEGUENZE LEGALI

A. Disposizioni applicabili in materia di protezione dei dati

25 Se si tratta di un ambito d'azione di diritto privato consentito dallo Stato, agli organi federali si applicano le disposizioni in materia di protezione dei dati personali (art. 40 LPD). In concreto, ciò significa che, oltre alle disposizioni generali (capitolo 2), si applicano le disposizioni speciali per i privati (capitolo 5).

26 Gli organi federali che agiscono in base al diritto privato sono quindi vincolati da disposizioni meno severe. Ciò è caratterizzato, ad esempio, dalla mancata applicazione dell'art. 34 LPD, che prescrive l'esistenza di una base giuridica per il trattamento dei dati da parte degli organi federali. Un'ulteriore conseguenza è l'applicabilità del meccanismo di cui all'art. 31 f. LPD, in base al quale alcune violazioni della personalità possono essere sanate da adeguate ragioni di giustificazione (base giuridica, interesse pubblico o privato prevalente, consenso).

27 Tuttavia, anche nel quadro dell'art. 40 LPD, non vi è un completo distacco dal regime giuridico degli organi federali. Alcuni principi costituzionali devono

essere rispettati anche dagli organi federali che agiscono in base al diritto privato (cfr. infra n. 31 e segg.).

B. Questioni procedurali

Se si applica l'articolo 40 LPD, le disposizioni del diritto privato si applicano anche all'esercizio dei diritti. Se una persona interessata desidera far valere i diritti della persona o altre pretese nei confronti di un organismo federale che agisce in base al diritto privato, si applicano le disposizioni del capitolo 5 della LPD. 28

In caso di procedimento giudiziario, i tribunali civili sono competenti per l'azione. La procedura è disciplinata dal Codice di procedura civile. 29

C. Ulteriore applicabilità del diritto pubblico

1. Principi costituzionali

Nonostante l'applicazione dell'art. 40 FADP, l'obbligo di rispettare i principi costituzionali (cfr. art. 5 Cost.) non può essere trascurato. Le azioni degli organi federali di diritto privato devono sempre essere esaminate per verificare se sono conformi a questi principi fondamentali. 30

In primo luogo, occorre prestare attenzione al principio di legalità (art. 5 cpv. 1 Cost.). Questo principio svolge una funzione sia democratica che costituzionale. Nel regime di diritto privato della LPD, l'attuazione conforme alla legge del principio di trasparenza, dell'obbligo di informazione o dell'ottenimento del consenso può compensare in alcuni casi la funzione dello Stato di diritto. La funzione democratica, invece, non può essere sostituita dai suddetti obblighi (cfr. anche l'art. 34 del presente commento, in particolare l'excursus sul consenso). 31

2. Impegno per i diritti fondamentali

Anche nell'ambito dei diritti fondamentali non è necessaria una completa equivalenza con i privati se lo Stato agisce in base al diritto privato ai sensi dell'art. 40 LPD. La collettività e i privati che svolgono funzioni pubbliche sono sempre vincolati ai diritti fondamentali nelle loro azioni e devono contribuire alla loro realizzazione. Dopo che questo principio è stato inizialmente oggetto di sentenze della Corte suprema, è stato espressamente 32

sancito nella Costituzione federale del 1999 all'art. 35 cpv. 2 Cost. Non è l'azione privata o sovrana a essere decisiva per la natura vincolante dei diritti fondamentali, ma piuttosto - più in generale - l'adempimento di un compito pubblico (l'art. 35 cpv. 2 Cost. parla di "compito statale").

3. Teoria a due fasi nella procedura di presentazione

33 Al fine di distinguere tra azione privata e sovrana, nella procedura di gara viene talvolta utilizzata la teoria delle due fasi. Essa afferma che l'aggiudicazione (formazione della volontà) avviene per mezzo di un decreto ed è quindi di diritto pubblico, mentre il contratto con l'aggiudicatario è di diritto privato.

34 Tuttavia, la teoria delle due fasi non è stata riconosciuta dalla giurisprudenza della Corte suprema. In ogni caso, anche nel contesto della legge sulla protezione dei dati esistono difficoltà di demarcazione: Alla luce dell'art. 40 DPA, l'applicazione della teoria dei due livelli significherebbe che il trattamento dei dati fino all'aggiudicazione e quello successivo sarebbero soggetti a regimi giuridici diversi. Tuttavia, una separazione così rigida del trattamento dei dati comporta notevoli difficoltà (tecniche) nella pratica.

35 Nell'ottica di una soluzione non solo pragmatica, ma anche costituzionalmente giustificabile, si dovrebbe quindi ipotizzare un'applicazione globale delle disposizioni più restrittive in materia di protezione dei dati per gli organi federali alle procedure di gara. Anche in questo ambito, lo Stato che agisce in base al diritto privato non deve essere trattato con leggerezza e deve essere completamente equiparato ai privati.

V. CASISTICA

36 La sentenza "SwissPass" del Tribunale amministrativo federale è un esempio della procedura descritta sopra per esaminare l'esistenza di un'azione privata ai sensi dell'art. 40 LPD. In questo caso, il tribunale ha dovuto valutare se il rilascio di uno SwissPass e il relativo trattamento dei dati da parte delle FFS fossero soggetti al diritto pubblico o privato.

37 In primo luogo, è rilevante il regolamento giuridico speciale per il settore del trasporto passeggeri, secondo il quale le imprese di trasporto - a prescindere dalla loro forma giuridica - sono soggette alle disposizioni per gli organi federali per le loro attività autorizzate e concesse e, in caso di azioni di diritto

privato, a quelle per le persone private (art. 54 PBG). Ne consegue che anche le imprese di trasporto possono agire in base al diritto privato nell'area autorizzata e, in tal modo, devono rispettare le norme sulla protezione dei dati per i privati.

Secondo il Tribunale Amministrativo Federale, il rilascio dello SwissPass non ha una funzione diretta di trasporto passeggeri autorizzato, in quanto può essere rilasciato anche senza servizi di trasporto pubblico. Tuttavia, poiché lo SwissPass è un ausilio per la stipula di un contratto di trasporto passeggeri, il tribunale ha comunque tenuto conto della sua natura giuridica. Applicando il pluralismo dei metodi e in particolare la teoria delle funzioni, il tribunale ha qualificato il contratto di trasporto passeggeri come diritto civile e ne ha dedotto che le FFS erano soggette alle norme sulla protezione dei dati per i privati quando emettevano lo SwissPass. 38

Di conseguenza, la sentenza è corretta e l'azione di diritto privato delle FFS appare consentita e pertinente nel caso specifico. Vanno poi sottolineati due punti: 39

- Da un lato, il tribunale ha incluso nelle sue considerazioni anche il criterio dell'"adempimento di un compito pubblico", che non trova spazio in un'interpretazione rigorosa dell'art. 40 LPD. Secondo la formulazione, la norma si basa esclusivamente sulla forma giuridica dell'azione. I due concetti di "compito pubblico" e "azione privata o sovrana" devono essere separati per principio.
- Nonostante questo principio, nel caso in esame si sostiene che una pura attenzione alla natura giuridica del rapporto di base tra l'interessato e l'ente pubblico può portare a un'elusione delle norme di diritto pubblico imperative. Le azioni e, nel presente contesto, il trattamento dei dati personali da parte degli organi federali non possono essere misurati solo in base alla scelta della forma di azione. L'azione deve essere inserita in un contesto costituzionale più ampio. Pertanto, l'art. 40 LPD non è nemmeno applicabile se non riguarda un organo federale, compresi i privati che svolgono funzioni pubbliche. Nel presente parere, la valutazione del contratto di trasporto da parte del Tribunale amministrativo federale sulla base del pluralismo dei metodi e talvolta della teoria delle funzioni è quindi coerente e impedisce l'elusione dei principi di diritto pubblico.

BIBLIOGRAFIA

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.

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 41 LPD

Un commentario di Sarah Bischof

CITAZIONE SUGGERITA

Sarah Bischof, Commentario all'art. 41 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Bischof, art. 41 LPD N. XXX.

Art. 41 Pretese e procedura

[1] Chi ha un interesse degno di protezione può esigere che l'organo federale responsabile:

a. si astenga dal trattamento illecito dei pertinenti dati personali;

b. elimini le conseguenze di un trattamento illecito;

c. accerti il carattere illecito del trattamento.

[2] Il richiedente può in particolare esigere che l'organo federale:

a. rettifichi, cancelli o distrugga i pertinenti dati personali;

b. comunichi a terzi o pubblichi la sua decisione, in particolare la rettifica, la cancellazione o la distruzione dei dati, l'opposizione alla

comunicazione ai sensi dell'articolo 37 o la menzione del carattere contestato dei dati secondo il capoverso 4.

[3] Invece di cancellare o distruggere i dati personali, l'organo federale ne limita il trattamento se:

a. la persona interessata contesta l'esattezza dei dati personali ma né la loro esattezza né la loro inesattezza possono essere accertate;

b. lo esigono interessi preponderanti di terzi;

c. lo esige un interesse pubblico preponderante, in particolare la salvaguardia della sicurezza interna o esterna della Svizzera; o

d. la cancellazione o la distruzione dei dati rischia di compromettere un'indagine, un'istruzione o un procedimento amministrativo o giudiziario.

[4] Se non possono essere accertate né l'esattezza né l'inesattezza dei dati personali, l'organo federale aggiunge agli stessi una menzione che ne indica il carattere contestato.

[5] La rettifica, cancellazione o distruzione di dati personali non può essere chiesta in riferimento a fondi di biblioteche, istituti d'insegnamento, musei, archivi accessibili al pubblico e altre istituzioni pubbliche della memoria collettiva. Il richiedente che rende verosimile un interesse preponderante può chiedere che l'istituzione limiti l'accesso ai dati contestati. I capoversi 3 e 4 non sono applicabili.

[6] La procedura è retta dalla PA. Le eccezioni previste dagli articoli 2 e 3 PA non sono applicabili.

STRUTTURA

In breve 524
I. Generalità 524
A. Osservazioni preliminari 524
B. Storia dell'origine 525
II. Reclamo e requisiti procedurali 525
III. Le richieste 526
A. Presupposto di illegittimità 526
B. Diritto a un provvedimento ingiuntivo (cpv. 1 lett. a e cpv. 2 lett. a) 527
1. Generale 527
2. Rettifica e conferma (cpv. 4) 527
C. Diritto alla cancellazione (cpv. 1 lett. b) 528
D. Diritto a una sentenza dichiarativa (cpv. 1 lett. c) 529
E. Limitazione del trattamento (cpv. 3) 530
IV. Disposizioni di esenzione (cpv. 5) 531
V. Diritto processuale amministrativo (cpv. 6) 531
Bibliografia 532
I Materiali 532

IN BREVE

Se una persona ritiene che un organo federale violi le disposizioni applicabili della LPD nel trattamento dei dati personali, l'art. 41 LPD (insieme al diritto all'informazione ai sensi dell'art. 25 LPD) le conferisce i diritti necessari per far valere un trattamento dei dati lecito nei confronti dell'organo federale responsabile. In particolare, può chiedere che l'organismo federale si **astenga** dal trattamento illegale dei dati, **ponga rimedio** alle conseguenze del trattamento illegale o **stabilisca** l'illegalità del trattamento (art. 41 cpv. 1 LPD). L'articolo prevede eccezioni, come in particolare la limitazione del trattamento (art. 41 cpv. 3 LPD). La decisione dell'organo federale di rifiutare o accogliere o respingere tali richieste viene presa sotto forma di ordinanza, che a sua volta, se sono soddisfatti i requisiti necessari, può essere impugnata secondo le norme dell'amministrazione federale generale della giustizia.

I. GENERALITÀ

A. Osservazioni preliminari

1 Il trattamento di dati personali da parte di un organo federale costituisce una violazione del diritto fondamentale all'autodeterminazione informativa dell'interessato ai sensi dell'art. 13 cpv. 2 Cost. e dell'art. 8 CEDU. Per questo motivo, le autorità federali possono trattare i dati personali solo in misura limitata, nel rispetto dei principi di trattamento ai sensi dell'art. 6 LPD e in particolare degli artt. 34 e segg. LPD. In particolare, è necessaria una base giuridica.

2 Il trattamento dei dati da parte di un'autorità federale costituisce in genere un vero e proprio atto. L'art. 41 LPD concede alla persona interessata (nonché a eventuali terzi, cfr. n. 8) una serie di diritti con i quali può chiedere il ripristino della legittimità del trattamento dei dati o almeno l'accertamento dell'illegittimità. Almeno nel caso di una decisione (parzialmente) negativa, l'interessato ottiene così un provvedimento impugnabile.

3 La protezione giuridica individuale di cui all'art. 41 LPD, che entra in vigore solo in caso di reclamo attivo da parte dell'interessato, deve essere distinta dai diritti di controllo dell'Incaricato federale della protezione dei dati e delle informazioni (si vedano i commenti agli artt. 49 e segg. LPD). Nell'ambito dei

suoi poteri di vigilanza, l'IFPDT è autorizzato a condurre indagini d'ufficio e a emettere sentenze, il che tutela anche le persone che non possono o non vogliono intraprendere un'azione legale contro un organo federale inadempiente (ad esempio perché non sono a conoscenza dell'illegalità o del trattamento dei dati stesso).

B. Storia dell'origine

Secondo il messaggio del Consiglio federale sulla LPD originale del 1992, il sistema giuridico proposto doveva essere modellato sulle azioni di diritto privato dell'art. 28a del CC da un lato, ma dall'altro doveva essere integrato nel diritto processuale amministrativo in vigore all'epoca. I Consigli non hanno successivamente messo in discussione il concetto proposto dal Consiglio federale e hanno apportato solo alcune modifiche. 4

La disposizione ha subito alcune modifiche a seguito della revisione, che è entrata in vigore il 1° settembre 2023. In particolare, sono stati inseriti un diritto esplicito alla cancellazione e la limitazione del trattamento. Le modifiche e le integrazioni proposte dal Consiglio federale sono state adottate dai Consigli senza ulteriori modifiche. 5

II. RECLAMO E REQUISITI PROCEDURALI

Il **destinatario** del reclamo è l'**organo federale** responsabile che tratta o fa trattare i dati per adempiere al proprio mandato legale. Sono considerati organi federali non solo le autorità federali, ma anche i soggetti privati che adempiono a compiti di diritto pubblico della Confederazione (cfr. spiegazioni sull'art. 5 lett. i LPD). Ciò significa, ad esempio, che i reclami derivanti da un trattamento illecito dei dati nei confronti di una cassa pensioni organizzata come fondazione di diritto privato, ma che offre una previdenza professionale obbligatoria ai sensi della LPP ed è quindi considerata un ente federale, devono essere fatti valere ai sensi dell'art. 41 LPD (e non dell'art. 32 LPD). 6

Si noti che l'esecuzione di un reclamo nei confronti di un organo federale non ha alcun effetto vincolante su altri organi federali (si veda il n. 21 sulla notifica a terzi o la pubblicazione); essi devono pertanto essere fatti valere individualmente nei confronti di ciascun organo federale responsabile del trattamento dei dati. 7

8 Ogni persona che abbia un **interesse meritevole di protezione** ha il diritto di presentare un reclamo. L'esistenza di tale interesse viene valutata in base ai principi generali della procedura amministrativa. L'interesse degno di tutela non è limitato agli interessi personali e non deve necessariamente coincidere con l'interesse protetto dalla norma violata. L'unico requisito è che il richiedente abbia un interesse attuale, di diritto o di fatto, all'esito del procedimento che ha avviato e che questo possa portargli un beneficio diretto e concreto. Il richiedente deve avere un rapporto particolare con l'oggetto della controversia e quindi essere più interessato rispetto al pubblico in generale.

9 Nel caso dell'interessato, in genere esiste un interesse degno di tutela. Tuttavia, sono possibili eccezioni, ad esempio se l'organo federale non tratta più i dati, il che renderebbe la richiesta irrilevante. In alcune costellazioni, è anche possibile che terze parti i cui dati non vengono elaborati affatto possano dimostrare un interesse degno di protezione. Tuttavia, ciò avviene generalmente solo se il terzo è un parente stretto o un amico della persona interessata (deceduta) e può invocare la protezione della memoria riconosciuta dal Tribunale federale.

III. LE RICHIESTE

A. Presupposto di illegittimità

10 Ai sensi dell'art. 41 cpv. 1 LPD, il richiedente può chiedere l'**omissione di un** trattamento illecito dei dati, l'**eliminazione delle conseguenze** di un trattamento illecito dei dati o l'**accertamento** dell'illiceità del trattamento dei dati.

11 Ciò che accomuna queste richieste è che presuppongono che il trattamento dei dati sia **illecito** . Ciò è in contrasto con l'obiezione alla divulgazione di dati personali ai sensi dell'art. 37 LPD; in questo caso, è determinante solo un interesse della persona interessata degno di protezione, ma non l'illegalità della divulgazione (si veda il commento all'art. 37 LPD).

12 L'illegittimità può consistere, tra l'altro, nel fatto che l'ente federale **non dispone di una base giuridica sufficiente** per il relativo trattamento dei dati. Ad esempio, il Tribunale amministrativo federale ha stabilito che un istituto di previdenza che invia i certificati di previdenza non sigillati

direttamente al datore di lavoro agisce illegalmente perché tale divulgazione non è necessaria per l'attuazione della previdenza professionale in conformità con la LPP e nessun'altra base giuridica (in particolare l'art. 86a LPP, che regola la divulgazione dei dati nell'ambito della LPP) la legittimerebbe. Inoltre, il **trattamento di dati errati** è illegittimo anche se l'organo federale responsabile non adempie al proprio obbligo di verifica in materia (cfr. commento all'art. 6 cpv. 5 LPD).

B. Diritto a un provvedimento ingiuntivo (cpv. 1 lett. a e cpv. 2 lett. a)

1. Generale

La richiesta di un provvedimento inibitorio presuppone che, al momento della richiesta, vi sia il **serio timore** che l'organo federale responsabile effettui in un prossimo futuro un trattamento illecito dei dati. Tale serio timore può sussistere, da un lato, se l'organo federale sta già effettuando il trattamento dei dati e questo è in corso, oppure se vi sono indizi concreti che i dati saranno trattati illegalmente in un certo modo nel prossimo futuro. Solo in questo caso, secondo la giurisprudenza del Tribunale federale, è possibile affermare l'interesse giuridico attuale a un provvedimento ingiuntivo. 13

Se queste condizioni sono soddisfatte, tuttavia, l'interessato non può solo chiedere che l'ente federale si astenga dal trattamento illegale dei dati. Può anche chiedere il **ripristino della legalità**, in particolare chiedendo la rettifica, la cancellazione o la distruzione dei dati in questione ai sensi dell'art. 41 cpv. 2 lett. a LPD. 14

2. Rettifica e conferma (cpv. 4)

Il trattamento di dati personali inesatti è illegale solo se l'inesattezza è dovuta a una **violazione dell'obbligo di verifica** ai sensi dell'art. 6 cpv. 5 LPD. Un organismo federale che tratta dati deve quindi adottare d'ufficio misure adeguate per garantire l'esattezza dei dati sin dalla loro raccolta o durante il periodo di trattamento (cfr. commento all'art. 6 cpv. 5 LPD). Anche in tal caso, il trattamento dei dati diventa illecito almeno nel momento in cui la persona interessata si rivolge all'organo federale con una richiesta di rettifica e quest'ultimo non chiarisce nuovamente in modo sufficiente l'esattezza o l'inesattezza. 15

16 Se l'esattezza o l'inesattezza dei dati non può essere stabilita, o non può essere stabilita senza ulteriori tentativi, nonostante la richiesta di rettifica motivata della persona interessata, l'organo federale deve limitare il trattamento ai sensi dell'art. 41 cpv. 3 LPD per la durata dei chiarimenti necessari (cfr. lettera E di seguito). Ciò significa che durante questo periodo l'organismo federale può trattare i dati solo per stabilirne l'esattezza o l'inesattezza.

17 Se l'organo federale non è in grado di dimostrare l'esattezza dei dati trattati, eventualmente nonostante ulteriori chiarimenti, ma l'interessato non è nemmeno in grado di dimostrare l'esattezza delle correzioni da lui richieste, l'organo federale deve allegare una **nota di contestazione**. Da un lato, ciò soddisfa gli interessi della persona interessata, dimostrando che non è d'accordo con la presentazione dei fatti da parte dell'organismo federale. Dall'altro, garantisce che l'organo federale non debba astenersi dal trattare i dati di cui ha bisogno per adempiere al suo mandato legale.

18 Il materiale legislativo sulla nuova restrizione introdotta con la revisione del 2023 non commenta il rapporto tra l'art. 41 cpv. 3 e il cpv. 4 LPD. Tuttavia, come spiegato in precedenza, uno degli scopi dell'avviso di conferma è quello di garantire che l'organo federale possa continuare ad adempiere ai propri compiti legali. Se il chiarimento dell'esattezza o dell'inesattezza dei dati non ha successo, l'organo federale deve avere la possibilità di revocare la limitazione del trattamento effettuata a tal fine ai sensi dell'art. 41 cpv. 3 LPD, di allegare una nota di contestazione e di trattare nuovamente e integralmente i dati in questione, almeno nella misura in cui non sia possibile astenersi completamente dal trattamento e non sussistano altri motivi di limitazione (cfr. punto E).

C. Diritto alla cancellazione (cpv. 1 lett. b)

19 L'interessato ha anche il diritto di far eliminare **le conseguenze** di un trattamento illecito dei dati mediante misure adeguate e proporzionate. Si tratta dell'effettiva eliminazione delle conseguenze negative attribuibili al trattamento illecito dei dati, ad esempio la successiva concessione di prestazioni legali. Se una compagnia di assicurazione sanitaria nell'ambito dell'assicurazione sanitaria obbligatoria (OKP) utilizzasse un questionario sulla salute per chiarire lo stato generale di salute di un assicurato e non gli offrisse determinate prestazioni OKP sulla base di questo, non ci sarebbe alcuna base

legale per questo (e sarebbe in contrasto con l'obbligo di accettare i dati ai sensi della LAMal); la raccolta dei dati sarebbe illegale e la compagnia di assicurazione sanitaria dovrebbe concedere all'assicurato le prestazioni previste dalla legge sull'assicurazione sanitaria.

Tuttavia, il diritto non consente alle persone interessate di revocare le decisioni formalmente vincolanti. Ciò è ancora possibile solo con i motivi legali di revisione ai sensi dell'art. 66 PA. Inoltre, gli interessati non possono chiedere un risarcimento o una soddisfazione ai sensi dell'art. 41 cpv. 1 lett. b LPD, in quanto tali diritti devono essere fatti valere attraverso la legge federale sulla responsabilità. 20

In pratica, la richiesta di rimozione sarà regolarmente utilizzata in caso di divulgazione illegale dei dati. In questo caso, la persona interessata può richiedere, tra l'altro, la pubblicazione della decisione sul trattamento illecito dei dati (in particolare sulla rettifica, la cancellazione o la distruzione, la nota di opposizione ma anche sull'opposizione alla divulgazione ai sensi dell'art. 37 LPD) o la sua notifica a eventuali destinatari dei dati (art. 41 cpv. 2 lett. b LPD). In questo modo il destinatario dei dati può accettare volontariamente la decisione e cancellare o correggere i dati, ma non può essere costretto a farlo. In questo caso, l'interessato non ha altra scelta che far valere eventuali diritti nei confronti del destinatario dei dati. 21

D. Diritto a una sentenza dichiarativa (cpv. 1 lett. c)

Il richiedente può anche richiedere una dichiarazione di **illegittimità** del trattamento dei dati. Questa richiesta **è** solo **sussidiaria** rispetto alla richiesta di provvedimenti ingiuntivi e di rimozione. Finché si può chiedere l'omissione di un trattamento illecito o l'eliminazione delle relative conseguenze, non vi è alcun interesse degno di tutela nell'accertamento dell'illiceità. 22

Secondo la giurisprudenza della Corte Suprema Federale, esiste un interesse a una sentenza dichiarativa se il trattamento illecito dei dati (passato) o la relativa violazione dei diritti della personalità continua ad avere un effetto dirompente e l'accertamento dell'illiceità è idoneo a eliminare questo effetto continuo. 23

E. Limitazione del trattamento (cpv. 3)

24 Con la revisione del 2023 è stato inserito l'art. 41 cpv. 3 LPD. In base ad esso, invece di cancellare o distruggere i dati, l'organo federale deve limitarne il trattamento se si verifica uno dei seguenti casi

- L'interessato contesta l'esattezza dei dati personali, ma non è possibile stabilire né l'esattezza né l'inesattezza (cfr. n. 18);
- interessi prevalenti di terzi o interessi pubblici prevalenti richiedono la conservazione dei dati;
- la cancellazione o la distruzione dei dati metterebbe a rischio un'indagine, un'inchiesta o un procedimento ufficiale o giudiziario.

25 Va notato che l'art. 18 del DSGVO prevede anche la "limitazione del trattamento". A differenza di quanto previsto dal DSGVO, quando l'interessato ha un reclamo nei confronti del responsabile del trattamento, l'art. 41 cpv. 3 LPD è concepito come un'eccezione alla cancellazione/distruzione o alla rettifica. Al momento dell'elaborazione di una richiesta di cancellazione/distruzione, ma anche di rettifica (sebbene non sia esplicitamente menzionata, la restrizione del trattamento per verificare l'esattezza o l'inesattezza dei dati ha senso da un punto di vista legale), l'organismo federale deve verificare d'ufficio se esiste uno dei motivi per una restrizione. Se la richiesta è accolta e la limitazione è confermata, l'organismo federale deve ridurre il trattamento alla finalità in conflitto con la cancellazione/distruzione o la rettifica.

26 La decisione sulla restrizione deve essere emessa come ordinanza o come ordinanza provvisoria se il procedimento non si conclude a seguito di ciò.

27 L'invio stabilisce che la restrizione deve essere attuata in modo tale che i dati contestati siano chiaramente etichettati, il che in pratica potrebbe significare che vengono temporaneamente spostati in un altro sistema di elaborazione o che i diritti di accesso sono limitati. Nell'avanzare questa argomentazione, il legislatore non ha tenuto conto del fatto che ciò comporterà regolarmente problemi di attuazione nella pratica, in quanto non si può presumere che tutti i sistemi consentano tali precauzioni per i singoli dati, cioè "sul campo", per così dire, e che non possano essere attuate senza ulteriori indugi. Se le opzioni di implementazione tecnica non sono disponibili, la restrizione deve essere garantita almeno con misure organizzative, ad esempio mediante istruzioni nel sistema, direttive o elenchi separati.

IV. DISPOSIZIONI DI ESENZIONE (CPV. 5)

La rettifica, la cancellazione o la distruzione dei dati personali non può essere richiesta in relazione alle disponibilità dei cosiddetti archivi pubblici, come in particolare biblioteche accessibili al pubblico, istituti scolastici, musei o archivi. In queste costellazioni, non è nemmeno possibile emettere un avviso di rifiuto. Lo scopo di queste istituzioni è quello di rappresentare un momento del passato, il che può essere raggiunto solo se il patrimonio è fedele all'originale e immutato. 28

Tuttavia, l'interessato può almeno chiedere che l'accesso ai dati contestati sia limitato. In linea di principio, l'interesse pubblico all'accesso libero e inalterato ai documenti ha la precedenza. Tuttavia, si deve presumere un interesse prevalente della persona interessata a limitare l'accesso se essa subirebbe notevoli svantaggi personali a causa del libero accesso, ad esempio perché il suo avanzamento professionale sarebbe limitato e il valore archivistico dei dati in questione sembra essere inferiore in confronto. Secondo il dispaccio, questa eccezione deve essere presa in considerazione in particolare per quanto riguarda la crescente pubblicazione di documenti d'archivio su Internet. 29

V. DIRITTO PROCESSUALE AMMINISTRATIVO (CPV. 6)

La procedura per far valere i diritti di cui all'art. 41 cpv. 1-2 LPD è disciplinata dalla PA. Ciò vale anche nel caso in cui la PA non si applichi effettivamente al rispettivo settore (le eccezioni di cui agli artt. 2 e 3 della PA non sono applicabili). 30

Ciò significa, in particolare, che l'organo federale deve chiarire d'ufficio i fatti del caso (principio di indagine, art. 12 PA). Tuttavia, il richiedente è soggetto a un obbligo di cooperazione (art. 13 PA); ad esempio, nell'ambito di una domanda di rettifica, il richiedente deve presentare prove che dimostrino l'accuratezza delle modifiche richieste. 31

L'organo federale può anche decidere di rifiutare, approvare o respingere la domanda. La decisione viene emessa sotto forma di sentenza, che a sua volta può essere impugnata presso il Tribunale amministrativo federale. 32

BIBLIOGRAFIA

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.

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 42 LPD

Un commentario di Sarah Bischof

CITAZIONE SUGGERITA

Sarah Bischof, Commentario all'art. 42 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Bischof, art. 42 LPD N. XXX.

Art. 42 Procedura in caso di comunicazione di documenti ufficiali che contengono dati personali

Se è in corso una procedura ai sensi della legge del 17 dicembre 2004 sulla trasparenza concernente l'accesso a documenti ufficiali che contengono dati personali, la persona interessata può, in tale procedura, far valere i diritti che le spettano in virtù dell'articolo 41 della presente legge in riferimento ai documenti oggetto della procedura di accesso.

STRUTTURA

In breve 535
I. Osservazioni preliminari 535
II. Rivendicazione di diritti ai sensi dell'art. 41 LPD nell'ambito della procedura di accesso 535
Bibliografia 536
I Materiali 537

IN BREVE

Secondo l'art. 42 LPD, i diritti di cui all'art. 41 LPD possono essere fatti valere nell'ambito di una procedura di accesso ai sensi della legge sull'accesso del pubblico se i documenti in questione contengono dati personali. La disposizione tiene quindi conto del fatto che gli scopi di tutela della LPD e della LTras, ossia l'autodeterminazione informativa nell'ambito della protezione della sfera privata da un lato e il principio della trasparenza dell'amministrazione dall'altro, possono essere in conflitto.

I. OSSERVAZIONI PRELIMINARI

L'ex art. 25bis aDSG è stato introdotto con l'entrata in vigore della Legge federale sulla pubblicità dell'amministrazione (Legge sulla pubblicità, LTras). Questa stabiliva i principi di coordinamento tra la LPD e la legge federale sulla libertà d'informazione. Nella versione riveduta della LPD del 2023, il contenuto della disposizione non è stato modificato; ora si trova nell'art. 42 LPD. 1

La disposizione garantisce che la persona interessata possa far valere i propri diritti in materia di protezione dei dati nell'ambito della procedura di accesso prevista dalla legge sull'accesso pubblico. Ciò significa che la procedura di accesso è estesa a questi problemi di protezione dei dati. 2

II. RIVENDICAZIONE DI DIRITTI AI SENSI DELL'ART. 41 LPD NELL'AMBITO DELLA PROCEDURA DI ACCESSO

La legge federale sull'accesso al pubblico stabilisce che ogni persona ha il diritto di prendere visione di documenti ufficiali e di ottenere dalle autorità informazioni sul contenuto dei documenti ufficiali (**principio dell'accesso al pubblico**, art. 6 cpv. 1 LTras). Tuttavia, l'accesso può essere limitato, rinviato o negato se la sua concessione può mettere in pericolo la privacy di terzi, a condizione che l'interesse pubblico all'accesso non prevalga (art. 7 cpv. 2 LTras). 3

Per proteggere la privacy di terzi nella procedura di accesso, i documenti ufficiali contenenti dati personali devono essere in linea di principio **resi anonimi** (art. 9 LTras). Tuttavia, se l'anonimizzazione non è possibile, ad 4

esempio perché il contenuto e il contesto del documento ufficiale non sarebbero più comprensibili o perché comporterebbe uno sforzo sproporzionato (il che richiede una ponderazione completa degli interessi da parte dell'organo federale), l'accesso può essere concesso solo a condizione dell'art. 36 LPD, che regola la divulgazione dei dati da parte degli organi federali (cfr. commento). Se l'autorità sta valutando la possibilità di concedere l'accesso, deve innanzitutto dare alla persona interessata i cui dati personali sono contenuti nei documenti in questione e la cui privacy può essere compromessa da ciò, l'opportunità di **esprimersi** entro 10 giorni. Nell'ambito di questa dichiarazione, l'interessato non può limitarsi a chiedere che i suoi dati non vengano divulgati al richiedente. L'art. 42 LPD consente piuttosto di far valere il proprio diritto all'**omissione di un** trattamento illecito dei dati, all'**eliminazione** delle conseguenze di un trattamento illecito dei dati o all'**accertamento dell** 'illiceità del trattamento dei dati (si veda il commento all'art. 41 LPD). Le richieste devono riguardare i documenti oggetto della procedura di accesso.

5 Se l'autorità intende concedere l'accesso in contrasto con il parere dell'interessato, deve informarlo (art. 11 cpv. 2 LTras). L'interessato può quindi chiedere **la mediazione** dell'IFPDT entro 20 giorni. Se la mediazione fallisce, l'IFPDT emette una raccomandazione. L'autorità deve quindi emettere un'ordinanza se non segue la raccomandazione o se l'interessato (o il richiedente) la richiede (art. 15 cpv. 1 e cpv. 2 lett. b LTras). Contro questa decisione è possibile presentare ricorso al Tribunale amministrativo federale (art. 16 cpv. 1 LTras).

6 L'art. 42 LPD mira, tra l'altro, a garantire l'efficienza della procedura, in quanto la persona interessata può venire a conoscenza del fatto che i suoi dati personali sono contenuti nei documenti ufficiali in questione solo quando viene invitata a presentare osservazioni. Di conseguenza, può essere sensato che gli aspetti della protezione dei dati siano valutati nell'ambito della procedura di accesso. Questa soluzione è stata criticata perché rende la procedura di accesso macchinosa e lunga.

BIBLIOGRAFIA

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.

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 43 LPD

Un commentario di Carl Jauslin / Danielle Schneider

CITAZIONE SUGGERITA

Carl Jauslin/Danielle Schneider, Kommentierung zu Art. 43 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Jauslin/Schneider, N. XXX zu Art. 43 DSG.

Capitolo 7:
Incaricato federale della protezione dei dati e della trasparenza

Sezione 1: Organizzazione

Art. 43 Elezione e statuto

[1] Il capo dell'IFPDT (Incaricato) è eletto dall'Assemblea federale plenaria.

[2] È eleggibile chiunque abbia diritto di voto in materia federale.

[3] Il rapporto di lavoro dell'Incaricato è retto dalla legge del 24 marzo 2000[12] sul personale federale (LPers), sempreché la presente legge non disponga altrimenti. Sino al compimento dei 65 anni l'Incaricato è assicurato presso la Cassa pensioni della Confederazione PUBLICA contro le conseguenze economiche di vecchiaia, invalidità e

morte. Su richiesta dell'Incaricato, la previdenza per la vecchiaia è mantenuta oltre il 65° anno di età e sino alla fine del rapporto di lavoro, ma al massimo sino alla fine dell'anno civile in cui egli compie 68 anni. In tal caso, l'IFPDT finanzia i contributi di risparmio del datore di lavoro.[13]

[3bis] L'Assemblea federale emana mediante ordinanza le disposizioni d'esecuzione concernenti il rapporto di lavoro dell'Incaricato.[14]

[4] L'Incaricato esercita la sua funzione in modo indipendente, senza ricevere né sollecitare istruzioni da alcuna autorità o da terzi. È aggregato amministrativamente alla Cancelleria federale.

[5] Dispone di una segreteria permanente e di un proprio preventivo. Assume il proprio personale.

[6] All'Incaricato non si applica il sistema di valutazione di cui all'articolo 4 capoverso 3 LPers.

STRUTTURA

In breve 542
I. Generale 542
II. Corpo elettorale (cpv. 1) 545
III. Eleggibilità (cpv. 2) 545
IV. Rapporto di lavoro (cpv. 3) 546
V. Disposizioni di attuazione del rapporto di lavoro (cpv. 3bis) 547
VI. Indipendenza e incarico (cpv. 4) 549
VII. Segreteria, bilancio e personale (cpv. 5) 550
VIII. Valutazione (cpv. 6) 551
Bibliografia 552
I Materiali 553

IN BREVE

L'elezione e la posizione del capo dell'IFPDT (il Commissario) sono fondamentali per l'indipendenza e la legittimità dell'attività di vigilanza. Il Commissario è eletto dall'Assemblea federale unitaria ed esercita la sua funzione in modo indipendente: Il Commissario non accetta istruzioni, non è soggetto al sistema di valutazione della LPers ed è assegnato solo amministrativamente alla Cancelleria federale. Dispone di una segreteria permanente e di un proprio budget.

L'elezione e la revoca del commissario sono di competenza dell'Assemblea federale unitaria. La Commissione giudiziaria è responsabile delle altre decisioni del datore di lavoro riguardanti il commissario. La legge federale sul personale si applica al rapporto di lavoro del commissario solo nella misura in cui la LPD e le sue disposizioni di attuazione non dispongano diversamente.

I. GENERALE

1 L'art. 43 disciplina l'elezione e la posizione del capo dell'IFPDT, che vigila sull'applicazione delle disposizioni federali in materia di protezione dei dati (art. 4 cpv. 1 LPD).

2 Dal punto di vista terminologico, occorre distinguere l'Incaricato come persona dall'IFPDT come autorità: Se la persona in questione è il capo dell'Incaricato federale della protezione dei dati e dell'informazione, si usa il termine "l'Incaricato"; se invece si intende l'autorità dell'Incaricato federale della protezione dei dati e dell'informazione in senso istituzionale, si usa l'abbreviazione "IFPDT". Oltre all'Incaricato, l'IFPDT come istituzione comprende anche la Segreteria.

3 Mentre nella legge precedente l'Incaricato era eletto dal Consiglio federale e l'elezione doveva essere approvata dall'Assemblea federale riunita (art. 26 cpv. 1 LDP), nella legge attuale l'Assemblea federale riunita è responsabile dell'elezione dell'Incaricato (art. 43 cpv. 1 LDP). L'elezione da parte dell'Assemblea federale unitaria mira a rafforzare l'indipendenza del Commissario e la sua legittimità democratica.

4 L'obiettivo di questa disposizione sull'elezione e sulla carica è garantire l'indipendenza del commissario come persona e dell'IFPDT come autorità. Il

concetto di indipendenza comprende l'indipendenza istituzionale, funzionale e sostanziale.

- L'indipendenza istituzionale significa che l'IFPDT non è subordinato a nessun'altra autorità dal punto di vista organizzativo. Tuttavia, ciò non esclude un incarico amministrativo, come nel caso dell'IFPDT presso la Cancelleria federale (FC) (cfr. art. 43 cpv. 4 seconda frase LPD).
- L'indipendenza funzionale richiede che l'IFPDT eserciti le sue funzioni e i suoi poteri in modo indipendente, senza ricevere istruzioni da alcun organismo (cfr. art. 43 cpv. 4 prima frase LDP) e che il Commissario non sia sottoposto ad alcun sistema di valutazione ai sensi dell'art. 4 cpv. 3 LDP (cfr. art. 43 cpv. 6 LDP). L'indipendenza funzionale dell'IFPDT è garantita anche dal fatto che il commissario è assunto al 100% (art. 8 dell'ordinanza sul rapporto di lavoro del commissario), il lavoro accessorio è possibile solo in misura molto limitata (artt. 46 e 47 LPD) e il commissario può essere rimosso dalla carica solo in casi eccezionali molto restrittivi (art. 44 cpv. 3 LPD).
- L'indipendenza materiale richiede che vengano create le condizioni e il quadro di riferimento affinché l'IFPDT possa esercitare i propri compiti e poteri in modo indipendente, ossia non solo sulla carta, ma abbia effettivamente la possibilità di adempiere al proprio mandato legale in modo indipendente. Questa indipendenza materiale comprende, in particolare, che l'IFPDT disponga di una segreteria e di un bilancio permanenti e che possa assumere il proprio personale in modo indipendente (cfr. art. 43 cpv. 5 LPD).

La revisione di questa disposizione sull'elezione, la posizione e il rapporto di lavoro del Commissario è avvenuta in tre fasi: 5

- In una prima fase, il Parlamento ha rafforzato l'indipendenza dell'IFPDT adottando la legge federale del 28 settembre 2018 sull'attuazione della direttiva UE 2016/680, che rientra nell'ulteriore sviluppo dell'acquis di Schengen.
- In un secondo momento, il Parlamento ha ulteriormente rafforzato l'indipendenza dell'IFPDT nell'ambito della revisione totale della legge sulla protezione dei dati del 25 settembre 2020, stabilendo che il commissario sarà ora eletto dall'Assemblea federale unitaria. La modifica dell'organo elettivo è stata introdotta solo durante il dibattito

parlamentare, contrariamente al parere del Consiglio federale, che si è attenuto alla soluzione precedente. L'iniziativa parlamentare Leutenegger Oberholzer 16.409 chiedeva già che il Commissario fosse eletto dall'Assemblea federale unitaria. Nel dibattito parlamentare, il rafforzamento dell'indipendenza e della posizione dell'IFPDT e l'accresciuta legittimità democratica sono stati addotti a sostegno di una modifica della procedura di elezione a favore dell'Assemblea federale unitaria. Il Consiglio federale e i sostenitori della soluzione precedente temevano una politicizzazione dell'elezione, che avrebbe potuto essere influenzata da vari gruppi d'interesse in Parlamento, e sottolineavano che anche nella soluzione precedente l'Assemblea federale unitaria deve approvare l'elezione da parte del Consiglio federale ed è quindi coinvolta.

- In una terza fase, i singoli aspetti del rapporto di lavoro sono stati specificati a livello legislativo e all'Assemblea federale è stata conferita la competenza di emanare disposizioni attuative sul rapporto di lavoro del commissario (iniziativa parlamentare SPK-N 21.443). Le modifiche alla LPD completamente rivista, associate all'iniziativa parlamentare SPK-N 21.443, e le nuove disposizioni di attuazione sono state adottate il 17 giugno 2022 ed entrano in vigore contemporaneamente alla revisione totale della LPD (1.9.2023). In questo modo l'indipendenza del commissario si riflette anche nel rapporto di lavoro.

6 L'art. 43 cpv. 4 e 5 LPD rimane invariato rispetto alla vecchia legge (art. 26 cpv. 4 e 5 LPD), in quanto l'art. 43 cpv. 5 LPD è stato integrato dall'art. 45 LPD sulla procedura di bilancio. L'art. 43 cpv. 3 prima frase corrisponde all'art. 26 cpv. 2 LPD ed è stato ampliato con tre frasi sul fondo pensione del Commissario.

7 L'art. 43 LPD è conforme ai requisiti del diritto europeo di cui all'art. 15 della Convenzione 108+ aggiornata del Consiglio d'Europa per la protezione delle persone fisiche con riguardo al trattamento dei dati personali, agli artt. 41 e segg. della Direttiva UE 2016/680 relativa a Schengen, nonché allo standard per un efficace controllo della protezione dei dati di cui agli artt. 51 e segg. del Regolamento generale sulla protezione dei dati UE 2016/679 in relazione alla decisione di adeguatezza della Commissione UE (art. 45 cpv. 2 lett. b del Regolamento generale sulla protezione dei dati UE).

II. CORPO ELETTORALE (CPV. 1)

L'Assemblea federale unitaria elegge il Commissario. La Commissione giudiziaria è responsabile della pubblicità della carica e della preparazione dell'elezione (art. 40a cpv. 1 lett. d e cpv. 2 prima frase LParl; cfr. anche art. 2 dell'ordinanza sul rapporto di lavoro del commissario). Il sostituto del commissario non rientra nella disposizione e non è eletto dal Parlamento. Al sostituto si applicano le disposizioni generali della legge federale sul personale. 8

L'art. 43 cpv. 1 LPD si basa sull'art. 168 cpv. 2 Cost. secondo cui una legge può autorizzare l'Assemblea federale a eleggere persone diverse da quelle di cui all'art. 168 cpv. 1 Cost. Si tratta, ad esempio, del Procuratore federale e dei Procuratori federali aggiunti, nonché dei membri dell'autorità di vigilanza sull'Ufficio del Procuratore federale (cfr. artt. 20 e 23 LOAP). 9

Il diritto europeo non prescrive la procedura di elezione dei membri dell'autorità di protezione dei dati (cfr. art. 43(1) della Direttiva (UE) 2016/680; anche art. 53(1) del Regolamento (UE) 2016/679). In base a questi atti giuridici, spetta agli Stati membri garantire che la nomina avvenga secondo una procedura trasparente e prevedere una nomina da parte del Parlamento, del Governo, del Capo dello Stato o di un organismo indipendente incaricato di tale compito ai sensi della legislazione dello Stato membro. 10

III. ELEGGIBILITÀ (CPV. 2)

Ai sensi del cpv. 2, è eleggibile a commissario chiunque abbia diritto di voto in materia federale. Ai sensi dell'art. 136, cpv. 1, della Cost. hanno diritto di voto in materia federale tutti i cittadini svizzeri che hanno compiuto 18 anni e che non sono incapaci di intendere e di volere. In particolare, la cittadinanza svizzera è di conseguenza un requisito per la carica di commissario. 11

Questa disposizione sull'eleggibilità, che si basa sul diritto di voto, si ritrova per analogia in altre leggi federali. Corrisponde, ad esempio, all'art. 20 cpv. 1bis LOAP per l'elezione del Procuratore federale e dei Sostituti procuratori federali o all'art. 5 cpv. 2 VGG per l'elezione dei giudici del Tribunale amministrativo federale. 12

I requisiti per l'idoneità fattuale e personale dell'incaricato non sono esplicitamente indicati nella LPD. Tuttavia, essi derivano dal diritto del 13

personale federale, che rimane sussidiariamente applicabile alla persona nominata ai sensi dell'art. 43 cpv. 3 LDP, in particolare dall'obbligo di pubblicizzare la posizione pubblicamente (cfr. art. 7 LPers in combinato disposto con l'art. 22 OPers). L'incaricato deve essere un esperto di comprovata esperienza nell'ambito della LPD e di LTras, dotato di integrità personale. Tuttavia, l'idoneità fattuale e personale non è un prerequisito per l'eleggibilità, ma è piuttosto responsabilità dell'autorità elettorale. La commissione giudiziaria incaricata di preparare l'elezione dell'incaricato deve già tenere conto dell'idoneità professionale e personale quando pubblicizza la posizione. Le commissioni di controllo delle imprese e la delegazione delle finanze sono tenute a esaminare l'idoneità professionale e personale dell'incaricato e a portare i loro risultati all'attenzione della commissione giudiziaria (art. 40a cpv. 6 LParl).

14 L'incaricato non è soggetto a un controllo di sicurezza personale da parte dell'Amministrazione federale (art. 29 cpv. 4 lett. eb^{is} ISG), il che significa che anche l'esame degli aspetti di sicurezza è di competenza del corpo elettorale.

IV. RAPPORTO DI LAVORO (CPV. 3)

15 Il rapporto di lavoro del commissario è disciplinato dalla RICA, a meno che la RICA non disponga diversamente. Di conseguenza, la LPers si applica sussidiariamente nel caso in cui la LPD non preveda disposizioni speciali. La LPD contiene disposizioni derogatorie o chiarificatrici nei seguenti punti:

- Art. 43 cpv. 1 e 2 LPD (elezione)
- Art. 43 cpv. 3 LPD (fondo pensione)
- Art. 43 cpv. 3bis LPD (base giuridica per le disposizioni di attuazione)
- Art. 43 cpv. 4 prima frase LPD (indipendenza e libertà di emanare direttive)
- Art. 43 cpv. 6 LPD (sistema di valutazione)
- Art. 44 cpv. 1 e 2 LPD (durata del mandato e cessazione)
- Art. 44 cpv. 3 LPD (revoca dell'incarico)
- Art. 44a LPD (avvertimento)
- Art. 46 LPD (incompatibilità)
- Art. 47 LPD (impiego secondario)

- Art. 47a LPD (ricusazione)
- Art. 72 LPD (disposizione transitoria)
- Art. 72a LPD (disposizione transitoria)

Le deroghe al diritto del personale federale sono necessarie in particolare se lo richiede l'indipendenza del commissario o la procedura elettorale speciale (elezione da parte dell'Assemblea federale unitaria).

L'art. 43 cpv. 3 contiene poi, nelle frasi 2-4, una disposizione chiarificatrice per l'incaricato in relazione alla previdenza professionale. Tale disposizione è necessaria perché, secondo il rapporto della SPK-N, la LPers non è direttamente applicabile in questo caso. L'art. 43 cpv. 3 stabilisce che la persona incaricata è assicurata presso la Cassa pensioni della Confederazione PUBLICA contro le conseguenze economiche della vecchiaia, dell'invalidità e del decesso fino all'età di 65 anni. Inoltre, la persona incaricata ha la possibilità di continuare a percepire la pensione di vecchiaia fino alla fine dell'anno in cui compie 68 anni (cfr. anche l'art. 4 cpv. 2 dell'Ordinanza sul rapporto di lavoro della persona incaricata), a condizione che il rapporto di lavoro sia continuato. Questa disposizione corrisponde nel contenuto all'art. 8 cpv. 2 e 3 dell'ordinanza dell'Assemblea federale del 1° ottobre 2010 sul rapporto d'impiego e la retribuzione del procuratore federale e dei procuratori federali aggiunti (di seguito: ordinanza sul rapporto d'impiego del procuratore federale, RS 173.712.23). L'IFPDT finanzia i contributi di risparmio del datore di lavoro. 16

V. DISPOSIZIONI DI ATTUAZIONE DEL RAPPORTO DI LAVORO (CPV. 3BIS)

Il Parlamento, e non il Consiglio federale, è responsabile dell'emanazione delle disposizioni di attuazione sul rapporto di lavoro del commissario in base alla sua posizione di organo elettorale. Il fatto che le disposizioni attuative siano emanate dall'organo elettorale è da accogliere con favore per ragioni di coerenza e di mantenimento dell'indipendenza. Il Parlamento si è occupato di questo lavoro nell'ambito dell'iniziativa parlamentare SPK-N 21.443 e il 17 giugno 2020 ha adottato l'"Ordinanza sul rapporto di lavoro del capo dell'Incaricato federale della protezione dei dati e delle informazioni". 17

18 L'ordinanza dell'Assemblea federale sul rapporto di lavoro dell'Incaricato si basa sull'art. 43 cpv. 3bis LPD. Essa stabilisce, tra l'altro, che

- le decisioni più importanti del datore di lavoro relative all'elezione del commissario e alla sua revoca sono di competenza dell'Assemblea federale unitaria (riferimento puramente dichiarativo all'art. 2 cpv. 1), mentre la Commissione giudiziaria è responsabile delle altre decisioni del datore di lavoro (ad es. annunci di lavoro) riguardanti il commissario (art. 2 cpv. 3).
- il rapporto di lavoro del commissario è stabilito da un decreto elettorale dell'Assemblea federale che richiede l'approvazione (art. 3 cpv. 1) e, a differenza di altri magistrati, il commissario non deve prestare giuramento o voto di coscienza (art. 3 cpv. 4).
- il commissario si ritira dall'incarico al più tardi alla fine dell'anno in cui compie 68 anni (art. 4 cpv. 2).
- l'incaricato è inquadrato nella classe salariale 34 ai sensi dell'art. 36 OPers (art. 5 cpv. 1) e non possono essere corrisposti né i premi di rendimento ai sensi dell'art. 49 OPers né i premi spontanei ai sensi dell'art. 49a OPers (art. 6 cpv. 1).
- l'incaricato è assicurato alla previdenza professionale nell'ambito del regime pensionistico della Confederazione (art. 7).
- il grado di occupazione del rappresentante è del 100% (art. 8) e deve essere domiciliato in Svizzera (art. 9).
- la commissione giudiziaria è responsabile dello scioglimento del segreto d'ufficio ai sensi dell'art. 320 n. 2 CP (art. 10).
- la sospensione provvisoria del commissario in carica è possibile solo alle condizioni dell'art. 14 cpv. 5 VG e sono escluse le disposizioni della Legge sul personale federale (artt. 103 e 103a OPers) (art. 11)).
- la Commissione giudiziaria può in linea di principio concedere all'incaricato un'indennità pari al massimo a un anno di stipendio in caso di cessazione del rapporto di lavoro, se il singolo caso lo giustifica (art. 12; sulle eccezioni cfr. art. 12 cpv. 3 e sull'obbligo di rimborso cfr. art. 12 cpv. 5).
- il trattamento dei dati personali dell'Incaricato nell'ambito del suo rapporto di lavoro è disciplinato dall'Ordinanza sulla protezione dei dati

personali del personale federale (OADO), fatte salve le disposizioni dell'Ordinanza sull'amministrazione parlamentare (PADO) (art. 13).

VI. INDIPENDENZA E INCARICO (CPV. 4)

Secondo la prima frase dell'art. 43 cpv. 4 LPD, l'Incaricato esercita la sua funzione in modo indipendente, senza chiedere o accettare istruzioni da un'autorità o da terzi. La libertà da istruzioni comprende due elementi: Il commissario non può né chiedere attivamente né accettare passivamente istruzioni. Ciò vale per le istruzioni provenienti da altre autorità pubbliche o da terzi privati. 19

La libertà di istruzioni dell'IFPDT tiene conto in particolare dei requisiti di diritto europeo sull'indipendenza dell'autorità di controllo della protezione dei dati di cui all'art. 12bis cpv. 4 della Convenzione 108+ aggiornata del Consiglio d'Europa e all'art. 42 cpv. 1 e 2 della Direttiva (UE) 2016/680 relativa a Schengen, nonché all'art. 52 cpv. 1 e 2 del Regolamento (UE) 2016/679 in relazione alla decisione di adeguatezza della Commissione UE (cfr. art. 45 cpv. 2 lett. b del Regolamento generale sulla protezione dei dati UE 2016/679). 20

Anche dopo la revisione totale della LOGA, il commissario e la segreteria permanente dell'IFPDT costituiscono un'unità amministrativa decentrata senza personalità giuridica (art. 2 cpv. 3 LOGA in combinato disposto con l'art. 8 cpv. 1 lit. Art. 8 cpv. 1 lett. b RVOG in combinato disposto con. Allegato 1 lit. A n. 2.1.1). Dal punto di vista amministrativo, l'IFPDT rimane assegnato come autorità alla Cancelleria federale (art. 43 cpv. 4, seconda frase), ma non è istituzionalmente subordinato ad essa. L'IFPDT deve facilitare e sostenere amministrativamente l'adempimento dei suoi compiti da parte dell'IFPDT, senza pregiudicarne l'indipendenza. Sulla base di un accordo di servizio, l'FC fornisce all'IFPDT una serie di servizi nei settori dell'amministrazione del personale, delle finanze e dell'automazione degli uffici. Tra gli esempi vi sono l'assegnazione di spazi per gli uffici, la fornitura di un'infrastruttura TIC adeguata e il supporto organizzativo per il sito web. Nonostante l'integrazione organizzativa nell'Amministrazione federale, l'IFPDT non è da considerarsi un'autorità amministrativa vera e propria, ma un'istituzione sui generis. Lo status sui generis è definito dalla LPD e da altre leggi. Garantendo la libertà di istruzioni dell'IFPDT, si garantisce la sua indipendenza istituzionale e funzionale. 21

22 L'indipendenza istituzionale e funzionale dell'IFPDT, con la contemporanea assegnazione amministrativa al FCO, si riflette anche nel canale di comunicazione prescritto. L'art. 37 cpv. 1 LDP prevede che la DFP comunichi con il Consiglio federale tramite il Cancelliere federale. Il Cancelliere federale è tenuto a trasmettere al Consiglio federale le proposte, i pareri e i rapporti senza modifiche. Tuttavia, l'IFPDT non sottopone i rapporti all'attenzione dell'Assemblea federale tramite il BK, ma direttamente tramite i servizi parlamentari (art. 37 cpv. 2 LDP).

23 È lecito chiedersi se esistano soluzioni più adatte per l'IFPDT nell'ambito del diritto dell'organizzazione amministrativa, invece dell'assegnazione amministrativa al CF. Tuttavia, un'assegnazione amministrativa dell'IFPDT ai servizi parlamentari appare artificiosa, poiché non esiste alcun legame tra i compiti dell'IFPDT e quelli dei servizi parlamentari. L'abbandono completo di un incarico amministrativo, come nel caso del Tribunale federale, ad esempio, avrebbe come conseguenza che la collaborazione tra l'IFPDT e gli organi federali non sarebbe più così stretta se il Commissario come persona o l'IFPDT come autorità non facessero più parte dell'Amministrazione federale.

VII. SEGRETERIA, BILANCIO E PERSONALE (CPV. 5)

24 Le risorse umane e finanziarie sono fondamentali per l'indipendenza materiale dell'IFPDT. L'art. 43 cpv. 5 LPD prevede pertanto che il commissario disponga di un proprio budget e di una segreteria permanente. La procedura di budget è regolata dall'art. 45 LPD.

25 L'IFPDT deve disporre di risorse umane e informatiche sufficienti per adempiere ai suoi compiti legali. A tal fine, la segreteria richiede in particolare conoscenze giuridiche, organizzative, tecniche (di sicurezza) e di comunicazione. Per quanto riguarda le relazioni della Svizzera con l'Unione europea, la disponibilità di risorse sufficienti è importante anche sotto un duplice aspetto: costituisce un elemento importante sia per quanto riguarda la decisione di adeguatezza sia per quanto riguarda l'attuazione dell'acquis di Schengen. Pertanto, l'obbligo di fornire alle autorità di controllo risorse umane, tecniche e finanziarie, locali e infrastrutture sufficienti è sancito dagli atti europei (articolo 12bis cpv. 5 del 108+ della Convenzione modernizzata del Consiglio d'Europa, articolo 42 cpv. 4, della Direttiva UE 2016/680 e articolo 52 cpv. 4 del Regolamento UE 2016/679).

L'articolo 43 cpv. 5, seconda frase della FADP prevede, come in precedenza, che il Commissario assuma il proprio personale e abbia determinate competenze in merito. Ad esempio, firma i contratti di lavoro. Tuttavia, l'incaricato non è ancora considerato un datore di lavoro per i dipendenti della Segreteria ai sensi della LPers. Secondo l'art. 3 cpv. 1 lett. a LPers, il datore di lavoro è il Consiglio federale. La questione se il Commissario debba avere lo status di datore di lavoro in futuro dovrà essere chiarita al più presto a livello giuridico formale. Ai sensi dell'art. 36 cpv. 2 LFPr, il diritto del personale federale continua pertanto ad applicarsi al rapporto di lavoro dei collaboratori della Segreteria permanente della DFP. L'UFAP, l'OPers e l'OAD continuano quindi ad applicarsi ai collaboratori della segreteria. 26

VIII. VALUTAZIONE (CPV. 6)

L'incaricato non è soggetto al sistema di valutazione di cui all'art. 4 cpv. 3 LPers. Questo sistema di valutazione ai sensi della LPers costituisce la base per la retribuzione legata alle prestazioni e per lo sviluppo orientato agli obiettivi dei collaboratori. Poiché l'IFPDT svolge la sua funzione in modo indipendente e non è soggetto ad alcuna direttiva, deve essere esonerato dal sistema di valutazione del LPers. Il fatto che le prestazioni dell'incaricato non siano valutate secondo il sistema di valutazione della LPers è di conseguenza la logica conseguenza del fatto di non essere vincolato da istruzioni e corrisponde all'altra faccia della medaglia. Chi non è vincolato da istruzioni non può essere valutato di conseguenza senza che la sua indipendenza venga compromessa. 27

Invece di una retribuzione legata ai risultati con bonus, per il capo dell'IFPDT è stato previsto uno sviluppo salariale indipendente dai risultati, secondo il modello del Procuratore federale. Secondo l'art. 5 cpv. 3 dell'ordinanza sul rapporto di lavoro, lo stipendio aumenta il 1° gennaio di ogni anno del tre per cento dell'importo massimo della categoria di stipendio fino a raggiungere tale importo massimo (cfr. art. 6 cpv. 3 dell'ordinanza sul rapporto di lavoro del Procuratore federale). 28

L'obbligo di rendicontazione dell'IFPDT (art. 57 LPD) riveste un'importanza fondamentale a fronte della mancanza di un sistema di valutazione. In caso di violazione dei doveri d'ufficio, esiste anche la possibilità di un ammonimento (art. 44a LPD). In caso di grave violazione dei doveri d'ufficio, può essere 29

presa in considerazione la rimozione dall'incarico (ultima ratio) (art. 44 cpv. 3 LPD) o la non rielezione da parte dell'Assemblea federale.

30 Il Commissario e l'istituzione dell'IFPDT non sono esenti da qualsiasi forma di controllo. Le attività dell'IFPDT sono soggette a controllo giudiziario, in quanto le sue decisioni possono essere impugnate fino al Tribunale federale. Inoltre, l'IFPDT è soggetto alla supervisione finanziaria del Controllo federale delle finanze (art. 8 cpv. 1 lett. a LFK; cfr. sui requisiti rilevanti per Schengen: Art. 42 cpv. 6 della Direttiva UE 2016/680). Le modalità di controllo finanziario devono tenere conto dell'indipendenza dell'IFPDT. Infine, l'IFPDT rimane soggetto alla vigilanza dell'Assemblea federale (art. 169 cpv. 1 Cost.). Secondo l'art. 8 cpv. 2 LF, i tribunali federali, l'Autorità federale di vigilanza sui mercati finanziari, l'Autorità federale di controllo dei revisori, l'Autorità di vigilanza del Ministero pubblico della Confederazione e il Ministero pubblico della Confederazione sono soggetti alla vigilanza finanziaria del Controllo federale delle finanze solo nella misura in cui questa serve all'esercizio della vigilanza generale dell'Assemblea federale. A nostro avviso, un'aggiunta corrispondente all'art. 8 cpv. 2 dell'AFC per includere il commissario vale almeno la pena di essere presa in considerazione al fine di rafforzare la sua indipendenza.

Il parere espresso riflette l'opinione personale degli autori e non è vincolante per l'Ufficio federale di giustizia.

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 44 LPD

Un commentario di Danielle Schneider / Carl Jauslin

CITAZIONE SUGGERITA

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 44 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Schneider/Jauslin, N. XXX zu Art. 44 DSG.

Art. 44 Durata, rielezione e cessazione del mandato

[1] Il mandato dell'Incaricato dura quattro anni e può essere rinnovato due volte. Inizia il 1° gennaio seguente l'inizio della legislatura del Consiglio nazionale.

[2] L'Incaricato può disdire il rapporto di lavoro per la fine di un mese con preavviso di sei mesi. In singoli casi, la Commissione giudiziaria può accordare all'Incaricato un termine di preavviso più breve se nessun interesse essenziale vi si oppone.

[3] L'Assemblea federale plenaria può destituire l'Incaricato prima della scadenza del mandato se questi:

a. intenzionalmente o per negligenza grave, ha violato gravemente i suoi doveri d'ufficio; o

b. ha durevolmente perso la capacità di esercitare il suo ufficio.

STRUTTURA

In breve 558
I. Aspetti generali 558
A. Scopo della legge 558
B. Contesto e storia delle origini 558
II. Durata del mandato e rielezione (cpv. 1) 560
III. Cessazione del rapporto di lavoro da parte del Commissario (cpv. 2) 560
IV. Rimozione dall'incarico (cpv. 3) 561
A. Requisiti 561
1. Grave violazione dei doveri d'ufficio 561
2. Incapacità permanente a ricoprire la carica 562
B. Procedura 562
Bibliografia 563
I Materiali 564

IN BREVE

Le disposizioni relative alla durata del mandato, alla rielezione e alla cessazione del rapporto di lavoro sono importanti per l'indipendenza del commissario sotto diversi aspetti. In particolare, occorre menzionare la limitazione della durata del mandato e le possibilità restrittive di cessazione del rapporto di lavoro. L'Assemblea Federale Unita, e non la Commissione Giudiziaria, è dichiarata responsabile di un'eventuale rimozione dall'incarico del commissario a causa dei suoi effetti drastici.

I. ASPETTI GENERALI

A. Scopo della legge

1 L'art. 44 LPD disciplina l'inizio e la durata del mandato (cpv. 1; n. 6 e segg.) nonché la cessazione del rapporto di lavoro del Commissario (cpv. 2 e 3; n. 10 e segg.). Per l'indipendenza della persona nominata, le ragioni e la procedura di cessazione del rapporto di lavoro sono di particolare importanza. In questo senso, l'art. 44 LPD contribuisce al controllo indipendente della protezione dei dati con la durata limitata del mandato del Commissario e le possibilità restrittive di rimozione dall'incarico.

B. Contesto e storia delle origini

2 La limitazione a due rielezioni (art. 44 cpv. 1 prima frase LPD; cfr. n. 6) era già stata introdotta durante la prima fase della revisione totale della LPD (disposizioni sulla protezione dei dati per la cooperazione Schengen in materia penale) nell'art. 26a cpv. 1 aDSG. Ciò ha tenuto conto dell'art. 44 cpv. 1 lett. e della Direttiva (UE) 2016/680 relativa a Schengen. In base a questa disposizione, gli Stati Schengen devono disciplinare se e - in caso affermativo - con quale frequenza i membri dell'autorità di controllo della protezione dei dati possono essere riconfermati. La modifica dell'art. 26a cpv. 1 aDSG è entrata in vigore il 1° marzo 2019.

3 Nella seconda fase della revisione totale della LPD, l'Assemblea federale unitaria è stata designata come organo di elezione del Commissario (cfr. art. 43 cpv. 1 LPD). Di conseguenza, è stato necessario adeguare anche le norme relative alla durata del mandato, alla rielezione e alla cessazione del mandato.

Tra l'altro, è stato specificato che il mandato inizia il 1° gennaio successivo all'inizio della legislatura del Consiglio nazionale (art. 44 cpv. 1 seconda frase LPD; cfr. n. 8). Inoltre, l'Assemblea federale unitaria è stata dichiarata competente a rimuovere il commissario dal suo incarico (art. 44 cpv. 3 LDP; cfr. n. 18). I motivi per la rimozione dalla carica, invece, sono rimasti sostanzialmente invariati rispetto alla legge precedente (art. 26a cpv. 3 aDSG) (cfr. n. 13 e segg.).

Infine, nell'ambito dell'iniziativa parlamentare SPK-N 21.443, la risoluzione del rapporto di lavoro su iniziativa del commissario è stata rivista nell'art. 44 cpv. 2 LPD: Invece della precedente richiesta di licenziamento, è stato sancito il diritto di recesso (unilaterale) (cfr. n. 10 s.). 4

Il Parlamento ha discusso in modo controverso se il Commissario debba ricevere un'indennità di licenziamento in caso di cessazione del rapporto di lavoro. Nella bozza della SPK-N per l'attuazione dell'iniziativa parlamentare 21.443, era previsto un nuovo art. 44 cpv. 4 LPD, che - in deroga alle disposizioni della legge federale sul personale - escludeva espressamente l'indennità di licenziamento. La giustificazione di questa disposizione era che il Commissario era meno esposto politicamente rispetto ad altre persone elette dall'Assemblea federale (come il Procuratore federale) o ad altre funzioni di alto livello dell'Amministrazione federale. Inoltre, il potenziale di conflitto in caso di cessazione del rapporto di lavoro non era così elevato da giustificare l'indennità di licenziamento. Dopo che il Consiglio federale si era espresso a favore dell'indennità di fine rapporto nella sua dichiarazione sull'iniziativa parlamentare 21.443 , nell'ottica dell'uguaglianza giuridica e dell'indipendenza del commissario, l'SPK-N ha modificato il suo progetto di decreto e ha proposto un'indennità di fine rapporto analoga a quella prevista per il Procuratore federale e il Procuratore generale. il Procuratore federale e i giudici federali di prima istanza (oggi: art. 12 dell'ordinanza dell'Assemblea federale del 17.6.2022 sul rapporto di lavoro del capo dell'Incaricato federale della protezione dei dati e delle informazioni [di seguito "ordinanza sul rapporto di lavoro dell'Incaricato"]). Le preoccupazioni relative all'indennità di licenziamento, invece, dovrebbero essere esaminate in un quadro generale (cioè non solo per l'Incaricato). Il Consiglio nazionale e il Consiglio degli Stati hanno approvato questa soluzione. 5

II. DURATA DEL MANDATO E RIELEZIONE (CPV. 1)

6 Ai sensi dell'art. 44 cpv. 1 prima frase LPD, il mandato del commissario è di quattro anni e può essere rinnovato due volte. Il commissario può quindi rimanere in carica per un massimo di dodici anni. Secondo il messaggio del Consiglio federale, questa limitazione del mandato mira a rafforzare l'indipendenza del commissario.

7 Alla scadenza del mandato quadriennale, il commissario deve essere rieletto dall'Assemblea federale unitaria se desidera continuare a esercitare la carica. A differenza della legge precedente (art. 26a cpv. 1bis aDSG) e in deroga all'art. 14 cpv. 2 lett. c BPG, non è più prevista una proroga tacita o automatica del mandato. Ciò promuove la legittimità democratica del commissario.

8 L'art. 44 cpv. 1 seconda frase LPD fissa l'inizio del mandato del commissario al 1° gennaio successivo all'inizio della legislatura del Consiglio nazionale. In questo modo, l'elezione viene trasferita al Parlamento appena composto. L'art. 72 cpv. 2 LPD prevede un'eccezione (una tantum) nel caso in cui il precedente titolare della carica sia eletto dall'Assemblea federale unita quando il commissario viene eletto per la prima volta. In questa costellazione, il nuovo mandato del Commissario inizia già il giorno successivo all'elezione (cfr. art. 72 n. 6 s.).

9 La persona nominata cessa automaticamente dal suo incarico al più tardi alla fine dell'anno in cui compie 68 anni (art. 4 cpv. 2 dell'Ordinanza sul rapporto di lavoro della persona nominata). Con l'innalzamento del limite di età a 68 anni, il Commissario viene equiparato ai giudici federali e al Procuratore federale, anch'essi eletti dall'Assemblea federale.

III. CESSAZIONE DEL RAPPORTO DI LAVORO DA PARTE DEL COMMISSARIO (CPV. 2)

10 Il commissario può risolvere il rapporto di lavoro alla fine di ogni mese con un preavviso di sei mesi (art. 44 cpv. 2, prima frase LPD). Mentre la legge precedente prevedeva solo la possibilità di chiedere il licenziamento (art. 26a cpv. 2 aDSG), ora l'incaricato può risolvere unilateralmente il rapporto di lavoro con un preavviso. Al commissario si applica quindi una normativa analoga a quella del Procuratore federale.

In singoli casi, la Commissione giudiziaria può concedere al commissario un periodo di preavviso più breve se non vi sono interessi sostanziali in conflitto (art. 44 cpv. 2, seconda frase LPD). A tal fine, deve tenere conto delle circostanze del caso specifico, come il periodo di transizione fino all'entrata in carica di un nuovo commissario o commissariamento. Può essere preso in considerazione un periodo di preavviso più breve, soprattutto in caso di motivi di salute. 11

IV. RIMOZIONE DALL'INCARICO (CPV. 3)

L'art. 44 cpv. 3 LPD disciplina la procedura di rimozione dalla carica. Dal punto di vista del contenuto, la disposizione corrisponde al precedente regolamento dell'art. 26a cpv. 3 aDSG (cfr. n. 13 e segg.). Tuttavia, la rimozione del commissario non è più di competenza del Consiglio federale, ma dell'Assemblea federale unificata (cfr. n. 18 e segg.). 12

A. Requisiti

In considerazione degli elevati requisiti di indipendenza del commissario, la rimozione dall'incarico è ammessa solo in casi gravi. I motivi sono elencati in modo esaustivo nell'art. 44 cpv. 3 LPD: Il commissario può essere rimosso dall'incarico se ha violato gravemente i doveri d'ufficio, intenzionalmente o per grave negligenza (lett. a; n. 14 e segg.) o ha perso in modo permanente la capacità di esercitare l'incarico (lett. b; n. 17). 13

1. Grave violazione dei doveri d'ufficio

Il compito principale del Commissario consiste nell'adempimento legittimo e diligente dei compiti assegnati dalla legge nell'ambito della protezione dei dati e del principio di pubblicità. Si tratta in particolare di indagare sulle violazioni delle norme sulla protezione dei dati (art. 49 e segg. LPD), ma anche di fornire consulenza agli incaricati del trattamento dei dati privati o agli organi federali e alle persone interessate (art. 58 cpv. 1 lett. a, c e d LPD), nonché di numerosi altri compiti, ad esempio in relazione alla divulgazione dei dati all'estero (art. 16 cpv. 2 LPD), alla valutazione dell'impatto sulla protezione dei dati (art. 23 LPD) o alla segnalazione di violazioni della sicurezza dei dati (art. 24 LPD). Altri doveri d'ufficio sono l'obbligo di segretezza (art. 320 CP, ma cfr. anche l'art. 20 cpv. 2 LPD), la limitazione del lavoro secondario (artt. 46 e 47 LPD) o 14

l'obbligo di residenza (art. 9 dell'ordinanza sul rapporto di lavoro del commissario).

15 La rimozione dalla carica non è ammessa per ogni violazione dei doveri d'ufficio. La violazione deve essere grave e deve essere intenzionale o gravemente negligente (art. 44 cpv. 3 lett. a LPD). Nel caso di una violazione meno grave dei doveri d'ufficio, può essere preso in considerazione un ammonimento da parte della commissione giudiziaria (cfr. art. 44a LPD).

16 In dottrina, l'inadempimento palesemente ingiustificato dei doveri di legge o (di norma) la violazione del segreto d'ufficio sono qualificati come gravi violazioni dei doveri d'ufficio. La mera critica del modo in cui viene svolto l'incarico, invece, non può giustificare la rimozione dall'incarico. La violazione dei doveri d'ufficio deve essere di natura tale da ledere irrevocabilmente la fiducia nella persona e da far apparire inaccettabile la prosecuzione dell'incarico.

2. Incapacità permanente a ricoprire la carica

17 La rimozione dalla carica è ammessa se la capacità di ricoprire la carica è venuta meno in modo permanente (art. 44 cpv. 3 lett. b LPD). Ciò dovrebbe valere solo in casi eccezionali. In particolare, devono essere presi in considerazione motivi medici o di malattia. Tuttavia, sono possibili anche motivi familiari. Infine, la capacità di ricoprire l'incarico può venire meno in modo permanente anche se l'incaricato è disperso o scomparso.

B. Procedura

18 La rimozione di un commissario dalla carica rientra, insieme alla sua elezione, tra le decisioni più importanti del datore di lavoro di competenza dell'Assemblea federale unitaria. Lo afferma non solo l'art. 44 cpv. 3 LPD, ma anche l'art. 2 cpv. 1 dell'ordinanza sul rapporto di lavoro del commissario.

19 La Commissione giudiziaria prepara un'eventuale rimozione dalla carica e presenta le necessarie mozioni all'Assemblea federale unita (art. 40a cpv. 1 lett. d ParlG e art. 2 cpv. 2 dell'ordinanza sul rapporto di lavoro del commissario). Di norma, tuttavia, la Commissione giudiziaria emette prima un ammonimento per motivi di proporzionalità (art. 44a LPD) prima di avviare il procedimento di rimozione dalla carica.

Nell'ambito del procedimento di impeachment, al commissario deve essere garantito il diritto di essere ascoltato. Nei suoi principi d'azione sulla procedura di impeachment o di non rielezione, la Commissione giudiziaria prevede, tra l'altro, che la persona interessata dal procedimento di impeachment abbia il diritto, dopo la conclusione dell'indagine e prima di riferire all'Assemblea federale riunita, di commentare per iscritto o oralmente il risultato dell'indagine e le ragioni della decisione (art. 7 cpv. 4 dei principi d'azione). Successivamente, la domanda della Commissione Giudicante all'Assemblea Federale Unificata deve contenere una riproduzione analoga del parere della persona interessata (art. 14 cpv. 2 lett. d dei Principi d'azione). 20

Nel caso in cui l'Assemblea federale unificata decida di rimuovere il commissario dal suo incarico, si pone la questione se tale decisione possa essere impugnata in tribunale. In linea di principio, non esiste un rimedio legale contro le decisioni dell'Assemblea federale unitaria (art. 189 cpv. 4 della Costituzione federale). Tuttavia, nel suo rapporto sull'iniziativa parlamentare 21.443, l'SPK-N fa riferimento alla recente prassi della Corte europea dei diritti dell'uomo, secondo cui la garanzia di ricorso legale ai sensi dell'art. 6 cpv. 1 CEDU si applica alla destituzione dei giudici. L'SPK-N ritiene ipotizzabile - a nostro avviso a ragione - che questa giurisprudenza possa essere trasferita al commissario, anch'esso dotato di una forte indipendenza. In questo caso, il commissario dovrebbe essere in grado di impugnare la rimozione dal suo incarico da parte dell'Assemblea federale unita davanti a un tribunale (Tribunale amministrativo federale, Corte suprema federale, CEDU). 21

Le opinioni espresse riflettono il parere personale degli autori e non sono vincolanti per l'Ufficio federale di giustizia.

BIBLIOGRAFIA

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.

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 44a LPD

Un commentario di Danielle Schneider / Carl Jauslin

CITAZIONE SUGGERITA

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 44a DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Schneider/Jauslin, N. XXX zu Art. 44a DSG.

Art. 44*a* Ammonimento

La Commissione giudiziaria può pronunciare un ammonimento qualora accerti che l'Incaricato ha violato i suoi doveri d'ufficio.

STRUTTURA

In breve 567
I. Aspetti generali 567
A. Storia delle origini 567
B. Scopo della norma 567
II. Misura disciplinare dell'ammonimento 568
III. Procedimento disciplinare 569
Bibliografia 570
I Materiali 570

IN BREVE

Il diritto disciplinare è disciplinato dalla legislazione speciale dell'art. 44a LPD. La disposizione limita la gamma di misure disciplinari possibili ai sensi della legge federale sul personale e mette a disposizione del commissario solo la misura dell'ammonimento. Ciò tiene conto dell'indipendenza del commissario. Allo stesso tempo, la misura disciplinare dell'ammonimento fornisce alla Commissione giudiziaria uno strumento per contestare i comportamenti del commissario che violano i suoi doveri e per proteggere la reputazione e l'affidabilità dell'autorità del DFP.

I. ASPETTI GENERALI

A. Storia delle origini

L'art. 44a LPD è stato inserito nella LPD completamente rivista nell'ambito dell'iniziativa parlamentare SPK-N 21.443. Durante i lavori per la legge di attuazione sul rapporto di lavoro del commissario, è emersa la necessità di apportare singole integrazioni alla LPD completamente rivista. In questo contesto, il legislatore ha considerato - tra le altre cose - il diritto disciplinare come una disposizione importante da chiarire a livello giuridico-formale. 1

B. Scopo della norma

L'art. 44a LPD prevede una deroga alla legge federale sul personale per il rapporto di lavoro del commissario nell'ambito del diritto disciplinare (cfr. art. 43 cpv. 3 prima frase LPD). La maggior parte delle misure disciplinari elencate nell'art. 99 cpv. 2 e 3 OPers (in combinato disposto con l'art. 25 cpv. 2 lett. b e c OPers), che possono essere adottate in caso di violazione dei doveri del diritto del lavoro, sono di fatto incompatibili con la carica di commissario o potrebbero compromettere l'indipendenza del commissario. Ciò vale in particolare per le riduzioni di stipendio e le multe, nonché per le modifiche dell'ambito delle mansioni, dell'orario o del luogo di lavoro. Tuttavia, il legislatore non ha voluto rinunciare completamente alle misure disciplinari nei confronti del commissario, in quanto tali misure possono contribuire a garantire che la carica sia esercitata in conformità alla legge. 2

3 L'art. 44a LPD deve essere inteso alla luce di questa tensione tra la salvaguardia dell'indipendenza e l'interesse all'esercizio legittimo delle funzioni ufficiali. La disposizione limita la gamma di misure disciplinari possibili ai sensi della legge federale sul personale e mette a disposizione del commissario solo la misura dell'ammonimento.

II. MISURA DISCIPLINARE DELL'AMMONIMENTO

4 Ai sensi dell'art. 44a LPD, la Commissione giudiziaria può emettere un ammonimento se ritiene che il commissario abbia violato i doveri d'ufficio. Ciò le fornisce uno strumento da utilizzare per garantire la reputazione e l'affidabilità dell'FDPIC. Con l'ammonimento, "il datore di lavoro fa capire al dipendente che non è disposto a continuare a tollerare il comportamento rimproverato e che intende adottare misure più severe se il comportamento rimproverato è ripetuto o continuato".

5 A differenza della rimozione dalla carica ai sensi dell'art. 44 cpv. 3 lett. a LPD, l'ammonimento non deve essere basato su una grave violazione dei doveri d'ufficio. La formulazione della legge sembra consentire un ammonimento per qualsiasi tipo di violazione dei doveri d'ufficio. In considerazione del principio di proporzionalità, tuttavia, l'ammonimento deve essere adeguato e necessario per ripristinare il corretto esercizio dei doveri d'ufficio da parte del commissario. Secondo le spiegazioni della SPK-N sull'iniziativa parlamentare 21.443, un ammonimento potrebbe, ad esempio, essere preso in considerazione se l'Incaricato viola le norme sul lavoro secondario (art. 47 LPD) o l'accettazione di doni o altri vantaggi (art. 1 cpv. 2 dell'Ordinanza dell'Assemblea federale del 17.6.2022 sul rapporto d'impiego del capo dell'Incaricato federale della protezione dei dati e della trasparenza [di seguito "Ordinanza sul rapporto d'impiego dell'Incaricato"] in combinato disposto con gli artt. 93 e segg. della Legge federale sulla protezione dei dati). Art. 93 f. OPERS). D'altro canto, la Commissione giudiziaria non può emettere un ammonimento se ritiene che il commissario stabilisca priorità sbagliate nell'esercizio delle sue funzioni. Ciò sarebbe incompatibile con l'indipendenza del commissario e interferirebbe nell'esercizio delle sue funzioni.

6 Come misura disciplinare, l'ammonimento presuppone sempre una colpa. Il commissario deve quindi aver agito intenzionalmente o almeno per negligenza.

III. PROCEDIMENTO DISCIPLINARE

La Commissione giudiziaria è responsabile dell'ammonimento dell'incaricato. Ciò corrisponde all'art. 2 cpv. 3 dell'ordinanza sul rapporto di lavoro del commissario, secondo cui la Commissione giudiziaria prende le decisioni sul datore di lavoro che non sono assegnate all'Assemblea federale unificata. Se la Commissione giudiziaria giunge alla conclusione che il comportamento denunciato costituisce una grave violazione dei doveri d'ufficio ai sensi dell'art. 44 cpv. 3 lett. a LPD, può chiedere all'Assemblea federale unitaria di rimuovere il commissario dal suo incarico. 7

Il procedimento disciplinare nei confronti del commissario è disciplinato dalle disposizioni (applicabili in via sussidiaria) della legge federale sul personale (art. 1 cpv. 2 dell'ordinanza sul rapporto di lavoro del commissario). 8

L'ammonimento può essere emesso solo dopo un'indagine disciplinare (art. 99 cpv. 1 OPers). L'art. 98 dell'OPers si applica all'indagine disciplinare: in base ad esso, la Commissione giudiziaria apre l'indagine disciplinare e designa la persona incaricata dell'indagine. Questa può anche essere una persona esterna (art. 98 cpv. 1 OPers). 9

Al procedimento disciplinare si applica la legge sulla procedura amministrativa (art. 98 cpv. 2 OPers). Ciò significa, in particolare, che l'accertamento dei fatti da parte della commissione giudiziaria è disciplinato anche dalle disposizioni della Legge sulla procedura amministrativa, in particolare per quanto riguarda il diritto di astensione (art. 10 PA), il principio dell'indagine e delle prove (art. 12 e art. 14 e segg. PA), l'obbligo di collaborazione del commissario (art. 13 PA) e i diritti procedurali del commissario (in particolare il diritto di consultare gli atti e di essere ascoltato; artt. 26 e segg. PA). 10

La diffida deve essere emessa come un ordine ai sensi dell'art. 5 PA (art. 34 BPG). Il commissario può impugnare la diffida della Commissione giudiziaria davanti al Tribunale amministrativo federale (art. 36 cpv. 1 BPG). 11

Il parere espresso riflette l'opinione personale degli autori e non è vincolante per l'Ufficio federale di giustizia.

BIBLIOGRAFIA

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.

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 45 LPD

Un commentario di Carl Jauslin / Danielle Schneider

CITAZIONE SUGGERITA

Carl Jauslin/Danielle Schneider, Kommentierung zu Art. 45 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Jauslin/Schneider, N. XXX zu Art. 45 DSG.

Art. 45 Preventivo

L'IFPDT presenta ogni anno, per il tramite della Cancelleria federale, un progetto di preventivo al Consiglio federale. Quest'ultimo lo inoltra senza modifiche all'Assemblea federale.

STRUTTURA

In breve 573
I. Aspetti generali 573
II. Sovranità di bilancio 574
III. Processo di bilancio 574
IV. Risoluzione sul bilancio 576
Bibliografia 577
I Materiali 577

IN BREVE

L'IFPDT elabora autonomamente il proprio bilancio e lo sottopone al Consiglio federale tramite la Cancelleria federale (CF). Il Consiglio federale lo sottopone poi senza modifiche all'Assemblea federale per l'approvazione. Questa procedura di bilancio, in cui l'FC e il Consiglio federale trasmettono il bilancio dell'IFPDT senza modifiche, rafforza l'indipendenza dell'IFPDT come autorità di vigilanza.

I. ASPETTI GENERALI

La sovranità di bilancio, la procedura di bilancio e la decisione di bilancio sono fondamentali per l'indipendenza dell'IFPDT come autorità di vigilanza (art. 43 n. 4). Solo chi decide autonomamente sul proprio bilancio è libero di svolgere i propri compiti nel quadro del mandato legale. L'indipendenza funzionale presuppone infatti una certa indipendenza finanziaria o materiale. 1

L'art. 45 descrive il processo attraverso il quale passa il bilancio dell'IFPDT. Il bilancio dell'IFPDT comprende gli stipendi del personale, che costituiscono la parte di gran lunga più consistente del bilancio, l'affitto dei locali, le spese per il materiale informatico, le spese di consulenza e altre spese operative. La disposizione si ricollega all'art. 43 cpv. 5 LPD, che già prevede, in relazione alla posizione dell'IFPDT, che il Commissario disponga di un proprio budget. 2

L'art. 45 LPD è stato inserito nella Legge federale sulla protezione dei dati con la revisione totale del 25 settembre 2020 (entrata in vigore il 1.9.2023). La disposizione è stata proposta dal Parlamento e non è ancora presente nel progetto del Consiglio federale. In particolare, l'Incaricato ritiene che il regolamento del suo bilancio debba essere allineato a quello del Controllo federale delle finanze. La vecchia legge sulla protezione dei dati del 19 giugno 1992 si limitava a prevedere, all'art. 26 cpv. 4 aDSG (ora art. 43 cpv. 5 LPD), che il Commissario disponesse di un proprio budget. Secondo la vecchia legge, il Consiglio federale non era ancora obbligato ad adottare il progetto di bilancio dell'IFPDT senza modifiche. Inoltre, l'IFPDT non aveva ancora la possibilità di rappresentare il proprio bilancio all'Assemblea federale (cfr. il nuovo art. 142, cpv. 2 e 3, terza frase, LParl). 3

II. SOVRANITÀ DI BILANCIO

4 La sovranità di bilancio significa che l'IFPDT redige il proprio bilancio in modo indipendente. La sovranità di bilancio è una componente essenziale dell'indipendenza dell'IFPDT. L'IFPDT deve determinare autonomamente le risorse di cui ha bisogno per svolgere i suoi compiti statutari. Nell'ambito della protezione dei dati, ciò riguarda le indagini sulle violazioni delle norme sulla protezione dei dati (art. 49 e segg. LPD), l'assistenza amministrativa (art. 54 e segg. LPD), i compiti relativi alla divulgazione dei dati all'estero (art. 16 LPD), la consultazione sulle valutazioni d'impatto sulla protezione dei dati (art. 23 LPD) nonché la gestione dei registri, l'informazione, la sensibilizzazione e la cooperazione (art. 56 e segg. LPD). L'assegnazione amministrativa dell'IFPDT alla Cancelleria federale riguarda solo il processo di bilancio e non influisce sulla sovranità di bilancio dell'IFPDT (art. 43 N 19 e segg.).

III. PROCESSO DI BILANCIO

5 Dopo aver elaborato autonomamente il proprio progetto di bilancio, l'IFPDT lo sottopone al Consiglio federale tramite la Cancelleria federale, alla quale è amministrativamente assegnato (art. 43 cpv. 4 seconda frase LPD). Secondo l'art. 142 cpv. 2 della Legge sul Parlamento (LParl), il Consiglio federale deve includere il progetto di bilancio e i conti dell'IFPDT senza modifiche nel suo progetto di bilancio e nei conti della Confederazione. Lo stesso vale per i preventivi e i conti dell'Assemblea federale, dei tribunali federali, del Controllo federale delle finanze, del Ministero pubblico della Confederazione e dell'autorità di vigilanza sul Ministero pubblico della Confederazione. La caratteristica comune delle istituzioni citate è la loro indipendenza dal Consiglio federale. Nelle loro azioni, le istituzioni citate sono vincolate solo dalla legge e non dalle istruzioni del Consiglio federale. La Costituzione stessa (nel caso dell'Assemblea federale e del Tribunale federale) o una legge federale (nel caso del Controllo federale delle finanze, del Ministero pubblico della Confederazione e della sua autorità di vigilanza) stabiliscono esplicitamente l'indipendenza delle unità organizzative menzionate.

6 L'art. 45 LPD si basa sulla soluzione adottata per l'autorità di vigilanza sulle attività di intelligence quando viene presentata tramite il Dipartimento (cfr. art. 4 dell'ordinanza del 16 agosto 2017 sulla vigilanza sulle attività di intelligence, VAND). Per contro, il Controllo federale delle finanze (CDF)

presenta il proprio budget annuale direttamente al Consiglio federale (cfr. art. 2 cpv. 3 LF) - senza passare per il Dipartimento federale delle finanze, da cui il CDF dipende (art. 1 cpv. 3 LF).

Inoltre, ai sensi dell'art. 142, cpv. 3, terza frase, della LParl, l'IFPDT stesso rappresenta il progetto di preventivo e di consuntivo all'Assemblea federale. In linea di principio, ciò dovrebbe essere fatto dal Commissario. In confronto, per il CDF, la delegazione finanziaria delle due Camere federali (art. 51 LParl) assume questo compito, mentre il Tribunale federale e l'autorità di vigilanza sul Ministero pubblico della Confederazione rappresentano anch'essi i loro preventivi davanti al Parlamento, così come lo stesso IFPDT davanti all'Assemblea federale (art. 142 LParl, cpv. 3). 7

Il processo di budget può essere riassunto come segue: 8

- L'IFPDT prepara un progetto di bilancio che comprende tutte le risorse necessarie per adempiere in modo coscienzioso e doveroso ai compiti che gli sono stati assegnati per legge in qualità di incaricato della protezione dei dati e dell'informazione pubblica.
- L'IFPDT presenta il suo progetto di budget alla Cancelleria federale, alla quale è amministrativamente assegnato (art. 43 cpv. 4 seconda frase LPD).
- La Cancelleria federale trasmette il progetto di bilancio dell'IFPDT al Consiglio federale.
- Il Consiglio federale trasmette il progetto di bilancio dell'IFPDT senza modifiche all'Assemblea federale per l'approvazione (art. 45 LPD). Concretamente, ciò significa che il Consiglio federale include il bilancio e i conti dell'IFPDT senza modifiche nel bilancio e nei conti della Confederazione (art. 142 LParl) e sottopone il progetto di bilancio all'Assemblea federale. Ciò avviene sotto forma di semplice decreto federale (art. 143 cpv. 3 LParl).
- Le commissioni finanziarie dei due Consigli discutono preventivamente i preventivi (art. 50 cpv. 1 LParl). L'approvazione dei Consigli è obbligatoria nel caso di preventivi (art. 73 cpv. 3 LParl).
- L'IFPDT presenta il suo progetto di bilancio all'Assemblea federale (art. 142 cpv. 3, terza frase).
- L'Assemblea federale è responsabile dell'approvazione del progetto di bilancio dell'IFPDT. Se nella procedura di composizione delle divergenze

tra i due Consigli viene respinta una proposta di accordo sulla risoluzione federale sul bilancio federale, si considera adottata la risoluzione della terza deliberazione che prevede l'importo inferiore (art. 94 LParl).

IV. RISOLUZIONE SUL BILANCIO

9 Il Parlamento è responsabile della deliberazione sul bilancio. Affinché il Parlamento possa deliberare in modo significativo sulla richiesta di bilancio dell'IFPDT, quest'ultimo deve giustificare il proprio budget.

10 Il Parlamento non può porre condizioni o requisiti all'approvazione del bilancio; non sono ammesse specifiche sull'uso dei fondi o sulla definizione di priorità. L'IFPDT può disporre liberamente dei fondi concessi nell'ambito del suo mandato legale.

11 L'articolo 15, paragrafo 6, della Convenzione del Consiglio d'Europa per la protezione delle persone fisiche con riguardo al trattamento dei dati personali (108+) modernizzata richiede che l'autorità di controllo disponga dei mezzi necessari per svolgere efficacemente le proprie funzioni ed esercitare i propri poteri. Anche la Direttiva UE 2016/680 relativa a Schengen prevede, all'art. 42(4), che ciascuna autorità di controllo debba disporre delle risorse necessarie per svolgere efficacemente le proprie funzioni ed esercitare i propri poteri, anche nell'ambito della reciproca assistenza, cooperazione e partecipazione. Inoltre, le risorse sufficienti dell'autorità di controllo della protezione dei dati sono un criterio essenziale per valutare l'adeguatezza del livello di protezione dei dati dal punto di vista del Regolamento generale sulla protezione dei dati dell'UE 2016/679 (cfr. a questo proposito l'articolo 52, paragrafo 4, in combinato disposto con l'articolo 45, paragrafo 2, lettera b)). Infine, l'efficacia della vigilanza dipende dalle risorse disponibili.

12 Un bilancio insufficiente a svolgere i compiti conferiti dalla legge mette in discussione l'indipendenza della vigilanza. Mancano meccanismi legali per la revisione dell'adeguatezza del bilancio. Allo stesso tempo, gli sforamenti di bilancio dovuti all'adempimento dei compiti previsti dalla legge non sono considerati una violazione dei doveri d'ufficio (art. 44 cpv. 3 lett. a LPD).

Il parere espresso riflette l'opinione personale degli autori e non è vincolante per l'Ufficio federale di giustizia.

BIBLIOGRAFIA

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.

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 46 LPD

Un commentario di Carl Jauslin / Danielle Schneider

CITAZIONE SUGGERITA

Carl Jauslin/Danielle Schneider, Kommentierung zu Art. 46 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Jauslin/Schneider, N. XXX zu Art. 46 DSG.

Art. 46 Incompatibilità

L'Incaricato non può essere membro dell'Assemblea federale o del Consiglio federale, né esercitare alcun'altra funzione al servizio della Confederazione.

STRUTTURA

In breve 581
I. Aspetti generali 581
II. Nessun membro dell'Assemblea federale 582
III. Nessun membro del Consiglio federale 582
IV. Nessun altro rapporto di lavoro con la Confederazione 583
Bibliografia 583

IN BREVE

Il commissario non può avere altri rapporti di lavoro con la Confederazione. In particolare, la contemporanea appartenenza all'Assemblea federale o al Consiglio federale è incompatibile con la funzione di vigilanza del commissario. Questo per evitare conflitti di interesse e rafforzare l'indipendenza dell'IFPDT.

I. ASPETTI GENERALI

L'Incaricato non può essere membro dell'Assemblea federale o del Consiglio federale e non può avere altri rapporti di lavoro con la Confederazione. Ciò al fine di escludere conflitti di interesse derivanti da funzioni diverse e contemporaneamente esercitate. 1

L'art. 144 della Cost. disciplina le incompatibilità tra le funzioni dei membri dei rami legislativo, esecutivo e giudiziario del governo ed è espressione della separazione dei poteri a livello federale. I membri del Consiglio nazionale, del Consiglio degli Stati, del Consiglio federale e i giudici del Tribunale federale non possono appartenere contemporaneamente a un'altra di queste autorità. Le norme sull'incompatibilità mirano a evitare concentrazioni di potere in una sola persona, a prevenire i conflitti di interesse, a salvaguardare l'indipendenza dei titolari delle cariche e a impedire che l'esercizio delle loro funzioni sia compromesso. Il cpv. 3 dell'art. 144 Cost. stabilisce che la legge può prevedere ulteriori incompatibilità. Per i membri del Parlamento, le disposizioni sull'incompatibilità si trovano nell'art. 14 f. LParl; per i membri del Consiglio federale e il Cancelliere federale, le incompatibilità professionali sono specificate nell'art. 60 LOGA. 2

Anche l'art. 46 LPD costituisce un'incompatibilità statutaria ai sensi dell'art. 144 cpv. 3 Cost. La disposizione sull'incompatibilità della nomina in base alla funzione corrisponde a quella dei giudici federali (art. 6 cpv. 1 LTF, art. 6 cpv. 1 LTF, art. 44 cpv. 1 LOAP) e a quella dei membri dell'autorità di vigilanza sul Ministero pubblico della Confederazione (art. 24 cpv. 1 LOAP). 3

L'art. 46 LPD è stato inserito nella Legge federale sulla protezione dei dati con la revisione totale del 25 settembre 2020 (entrata in vigore il 1.9.2023). La disposizione è stata proposta dal Parlamento e non è ancora presente nel 4

progetto del Consiglio federale. Ai sensi della vecchia legge sulla protezione dei dati del 19 giugno 1992, le questioni di incompatibilità funzionale dovevano essere valutate dal punto di vista del lavoro secondario.

5 L'incompatibilità funzionale è una conditio sine qua non per garantire l'indipendenza del commissario ed è quindi una conseguenza delle disposizioni di diritto europeo di cui all'art. 15 cpv. 5 della Convenzione del Consiglio d'Europa per la protezione delle persone fisiche con riguardo al trattamento dei dati personali (108+ modernizzata), all'art. 42 cpv. 3 della Direttiva Schengen (UE) 2016/680 e all'art. 52 cpv. 3 del Regolamento generale sulla protezione dei dati (RGPD) 2016/679 dell'Unione europea.

6 L'art. 46 LPD prevede tre incompatibilità per il Commissario, che verranno brevemente discusse di seguito. Tuttavia, le incompatibilità si applicano solo al Commissario e non ai suoi dipendenti.

II. NESSUN MEMBRO DELL'ASSEMBLEA FEDERALE

7 Il commissario non può essere contemporaneamente membro dell'Assemblea federale, cioè del Consiglio nazionale o del Consiglio degli Stati. Pertanto, in caso di elezione a commissario, la persona eletta deve porre fine a qualsiasi funzione o impiego esistente prima di assumere l'incarico.

8 I membri dell'Assemblea federale possono essere eletti come commissari, ma devono dimettersi dal Parlamento al più tardi al momento dell'entrata in carica. Ciò è già avvenuto in due delle tre elezioni del Consiglio federale. Al contrario, ai sensi dell'art. 44 cpv. 2 LPD, l'incaricato può recedere dal rapporto di lavoro alla fine di ogni mese, con un preavviso di sei mesi, e successivamente assumere una nuova funzione come membro del Parlamento (o del Consiglio federale; cfr. infra n. 9). Ai sensi dell'art. 44 cpv. 2 LPD, la Commissione giudiziaria può concedere all'incaricato un periodo di preavviso più breve in questi casi se non vi sono interessi sostanziali in conflitto.

III. NESSUN MEMBRO DEL CONSIGLIO FEDERALE

9 Il commissario non può essere contemporaneamente membro del Consiglio federale. Anche se, da un lato, il Consiglio federale non ha la facoltà di impartire direttive all'IFPDT (art. 43 cpv. 4 LPD) e, dall'altro, l'IFPDT non può esercitare la sua funzione di vigilanza attraverso il Consiglio federale (art. 4

cpv. 2 lett. b LPD), non è possibile evitare conflitti di interesse e l'indipendenza dell'IFPDT non sarebbe garantita da una tale unione personale.

IV. NESSUN ALTRO RAPPORTO DI LAVORO CON LA CONFEDERAZIONE

10 La funzione di commissario non è compatibile nemmeno con altri rapporti di lavoro che esistono contemporaneamente con la Confederazione. Gli altri rapporti di lavoro con la Confederazione devono quindi essere interrotti al momento dell'assunzione dell'incarico (cfr. n. 8). Questa incompatibilità costituisce una sorta di clausola generale sussidiaria rispetto alle due incompatibilità specifiche relative al Parlamento e al Consiglio federale. Considerata l'importanza centrale dell'indipendenza del Commissario, una norma di incompatibilità così ampia va accolta con favore.

11 Per ragioni di competenza costituzionale, l'art. 46 non contiene alcuna dichiarazione di incompatibilità con le funzioni e gli impieghi a livello cantonale o comunale. La compatibilità di tali cariche e impieghi a livello cantonale o comunale con la funzione di capo dell'IFPDT deve essere esaminata nel caso di un impiego secondario ai sensi dell'art. 47 LPD. Al contrario, un impiego secondario legato a un rapporto di lavoro con la Confederazione è già inammissibile a causa della disposizione di incompatibilità di cui all'art. 46 LPD.

Il parere espresso riflette l'opinione personale degli autori e non è vincolante per l'Ufficio federale di giustizia.

BIBLIOGRAFIA

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 47 LPD

Un commentario di Danielle Schneider / Carl Jauslin

CITAZIONE SUGGERITA

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 47 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Schneider/Jauslin, N. XXX zu Art. 47 DSG.

Art. 47 Attività accessorie

[1] L'Incaricato non può esercitare alcuna attività accessoria.

[2] La Commissione giudiziaria può autorizzare l'Incaricato a esercitare un'attività accessoria sempreché non siano pregiudicati il pieno adempimento della funzione, nonché l'indipendenza e la reputazione dell'IFPDT. La decisione è pubblicata.

STRUTTURA

In breve 587
I. Generalità 587
A. Scopo della norma 587
B. Storia delle origini 587
II. Principio: divieto di lavoro secondario (cpv. 1) 588
III. Eccezione: autorizzazione al lavoro secondario (cpv. 2) 588
A. Requisiti relativi al contenuto 588
B. Responsabilità 589
Bibliografia 590
I materiali 590

IN BREVE

In linea di principio, il commissario non può esercitare un'attività lavorativa secondaria (art. 47 cpv. 1 LPD). Questo divieto contribuisce a rafforzare l'indipendenza. Per essere considerata un'attività secondaria, un'attività deve essere di una certa qualità e intensità. Non importa se l'attività è remunerata o meno. In via eccezionale, la Commissione giudiziaria può consentire al commissario di esercitare un'attività secondaria, a condizione che non vengano compromessi né l'esercizio della funzione, né l'indipendenza, né la reputazione della LPD (art. 47 cpv. 2 LPD). In considerazione degli elevati requisiti di indipendenza del commissario, è opportuno adottare uno standard rigoroso. Qualsiasi impiego secondario del commissario deve essere pubblicato per tener conto dell'esigenza di trasparenza.

I. GENERALITÀ

A. Scopo della norma

L'art. 47 LPD prevede che il commissario non possa, in linea di principio, esercitare un'attività lavorativa secondaria (art. 47 cpv. 1; n. 4 s.). Questa norma giuridica speciale, più severa della legge federale generale sul personale (art. 23 LFPr in combinato disposto con l'art. 91 UFPP), tiene conto dell'indipendenza dell'incaricato. Nell'esercizio delle sue funzioni, l'incaricato non deve entrare in conflitto di interessi che potrebbero compromettere la sua indipendenza e mettere in dubbio la credibilità della carica. 1

B. Storia delle origini

Il divieto fondamentale di svolgere un'attività lavorativa secondaria per il commissario era già stato introdotto nella prima fase della revisione totale della LPD all'art. 26b aLPD (disposizioni sulla protezione dei dati per la cooperazione Schengen in materia penale). Per quanto riguarda l'impiego secondario, sono stati decisivi i requisiti dell'art. 42 cpv. 3 della Direttiva (UE) 2016/680. Le disposizioni sono entrate in vigore il 1° marzo 2019. 2

Il contenuto dell'art. 47 LPD non è cambiato da allora. Tuttavia, la competenza per l'autorizzazione all'impiego secondario del commissario è stata adeguata due volte: Nella versione della LPD completamente rivista del 3

15 settembre 2020, il compito è stato trasferito all'Assemblea federale unificata. In seguito sono sorti timori che la ripartizione dei compiti non fosse adeguata ai livelli e che la procedura potesse rivelarsi troppo macchinosa nella pratica. Nell'ambito dell'iniziativa parlamentare SPK-N 21.443, la Commissione giudiziaria è stata quindi dichiarata responsabile (art. 47 cpv. 2; cfr. n. 11 e segg.).

II. PRINCIPIO: DIVIETO DI LAVORO SECONDARIO (CPV. 1)

4 L'art. 47 cpv. 1 LPD vieta al commissario di svolgere un'attività secondaria. Ciò vale indipendentemente dal fatto che tale attività sia remunerata o meno. Il divieto fondamentale di svolgere un'attività secondaria va quindi oltre la regola dell'incompatibilità sancita dall'art. 46 LPD e riguarda in particolare anche le cariche o gli incarichi cantonali e comunali.

5 La LPD non definisce il termine "impiego secondario". Tuttavia, dalla documentazione emerge chiaramente che non tutte le attività che il commissario svolge in aggiunta alla sua carica sono da considerarsi inammissibili. L'occupazione secondaria deve invece essere di una certa qualità e intensità. In particolare, le attività di svago o gli hobby non sono considerati un'occupazione secondaria.

III. ECCEZIONE: AUTORIZZAZIONE AL LAVORO SECONDARIO (CPV. 2)

6 Sono possibili eccezioni al divieto di svolgere un'attività secondaria alle condizioni dell'art. 47 cpv. 2 LPD: la Commissione giudiziaria può autorizzare il commissario a svolgere un'attività secondaria (cfr. n. 11 e segg.), a condizione che non vengano compromessi né l'esercizio della funzione, né l'indipendenza, né la reputazione dell'IFPD (cfr. n. 7 e segg.). I suddetti requisiti devono essere intesi in modo cumulativo. Nel concedere l'autorizzazione, la Commissione giudiziaria tiene conto in particolare del contenuto dell'impiego secondario, del tempo necessario e dell'importo dell'eventuale compenso.

A. Requisiti relativi al contenuto

7 In primo luogo, l'impiego secondario non deve interferire con lo svolgimento delle funzioni dell'incaricato. L'adempimento dei doveri non deve essere

limitato dall'assenza o dall'indisponibilità dell'incaricato. A questo proposito, va notato che la carica di commissario può essere esercitata solo a tempo pieno - a differenza della legge precedente, in cui non era previsto un grado di occupazione specifico (art. 8 dell'ordinanza dell'Assemblea federale del 17 giugno 2022 sul rapporto di lavoro del capo dell'Incaricato federale della protezione dei dati e delle informazioni). Ciò è legato alle esigenze dell'ufficio, che sono aumentate in particolare a causa della digitalizzazione, nonché ai nuovi compiti e alle nuove competenze che l'IFPD riceverà nell'ambito della revisione totale della LPD (ad esempio, i nuovi poteri di indagine e di disposizione ai sensi degli artt. 49 e segg. LPD).

In secondo luogo, l'impiego secondario non deve compromettere l'indipendenza della DFP. Un conflitto di interessi o la semplice parvenza di un conflitto di interessi deve essere esclusa dal punto di vista giuridico e fattuale. 8

In terzo luogo, l'impiego secondario non deve pregiudicare la reputazione dell'FDPIC. Questo vale tanto più che la funzione dell'FDPIC è altamente personalizzata e una percezione negativa dell'incaricato o degli incaricati può avere un impatto sull'autorità dell'FDPIC. 9

Esempi: 10

- La carica di membro del comitato esecutivo, del consiglio di amministrazione o dei revisori dei conti di una società può compromettere di norma l'indipendenza dell'incaricato (e, a seconda della portata dell'attività, anche limitare la disponibilità alla carica).
- Inoltre, le attività per associazioni i cui obiettivi mettono in discussione la protezione dei dati o la vigilanza da parte dell'IFPDT sarebbero inammissibili, in quanto metterebbero a repentaglio la reputazione dell'IFPDT.
- La possibilità di approvare un incarico di insegnamento (ad esempio come docente universitario) dipende dalle circostanze del singolo caso. In ogni caso, sarebbe possibile solo un carico di lavoro ridotto.

B. Responsabilità

La commissione giudiziaria è responsabile del rilascio dell'autorizzazione al lavoro secondario (per la storia delle origini dell'art. 47 cpv. 2 LPD, cfr. n. 2 s.). 11

12 Sulla base delle informazioni presentate dal commissario, la commissione giudiziaria esamina in ogni singolo caso se sono soddisfatti i criteri per un'eccezione al divieto fondamentale del lavoro accessorio. In considerazione delle elevate esigenze di indipendenza del commissario, è opportuno adottare uno standard rigoroso. Tuttavia, se i requisiti dell'art. 47 cpv. 2 LPD sono chiaramente soddisfatti, sarebbe arbitrario che la Commissione giudiziaria rifiutasse di concedere all'incaricato una deroga.

13 La decisione della Commissione giudiziaria viene pubblicata (art. 47 cpv. 2 seconda frase LPD). Ciò contribuisce alla trasparenza dell'ufficio del commissario.

Le opinioni espresse riflettono il parere personale degli autori e non sono vincolanti per l'Ufficio federale di giustizia.

BIBLIOGRAFIA

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.

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 47a LPD

Un commentario di Danielle Schneider / Carl Jauslin

CITAZIONE SUGGERITA

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 47a DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Schneider/Jauslin, N. XXX zu Art. 47a DSG.

Art. 47a Ricusazione

Se la ricusazione dell'Incaricato è contestata, decide il presidente della corte del Tribunale amministrativo federale competente in materia di protezione dei dati.

STRUTTURA

In breve 595
I. Storia delle origini 595
II. Motivi di ricusazione del commissario 596
III. Decisione sulla ricusazione 596
Bibliografia 597
Materiali 597

IN BREVE

L'art. 47a LPD chiarisce la questione di chi decide sulla ricusazione del commissario in caso di controversia. Il compito è assegnato al presidente della sezione del Tribunale amministrativo federale competente per la protezione dei dati. Questa soluzione preserva l'indipendenza dell'Incaricato e il fatto che non è vincolato da istruzioni.

I. STORIA DELLE ORIGINI

L'art. 47a LPD è stato inserito nella LPD completamente rivista nell'ambito dell'iniziativa parlamentare SPK-N 21.443. Durante la stesura delle disposizioni di attuazione sul rapporto di lavoro del commissario, il Parlamento ha notato che non era chiaro chi avrebbe deciso sulla ricusazione del commissario in caso di controversia. 1

Le consuete competenze previste dal diritto del personale federale (superiore ai sensi dell'art. 94a cpv. 3 dell'UFAP) e dal diritto processuale amministrativo (autorità di vigilanza o autorità collegiale che esclude il membro interessato ai sensi dell'art. 10 cpv. 2 della PA) erano fuori questione a causa della posizione speciale del commissario. Anche l'Assemblea federale unitaria o la Commissione giudiziaria, che in linea di principio sono responsabili delle decisioni del datore di lavoro nei confronti dell'Incaricato (cfr. art. 2 dell'ordinanza dell'Assemblea federale del 17 giugno 2022 sul rapporto di lavoro del capo dell'Incaricato federale della protezione dei dati e delle informazioni; di seguito "ordinanza sul rapporto di lavoro dell'Incaricato"), erano fuori questione come organi decisionali a causa dell'indipendenza dell'Incaricato o del fatto che non è vincolato da istruzioni. 2

Il Parlamento ha colmato questa lacuna affidando al presidente della sezione del Tribunale amministrativo federale competente per la protezione dei dati la decisione su un licenziamento contestato del commissario. Questa competenza è ovvia, dal momento che il presidente della prima divisione del Tribunale amministrativo federale svolgeva già compiti speciali nel settore della protezione dei dati ai sensi della legge precedente (cfr. art. 30 cpv. 2 e art. 33 cpv. 2 aDPR). 3

II. MOTIVI DI RICUSAZIONE DEL COMMISSARIO

4 I motivi di ricusazione dell'Incaricato sono disciplinati in linea di principio dalla legge federale sul personale (art. 43 cpv. 3, prima frase, LPD in combinato disposto con. Art. 1 cpv. 2 dell'Ordinanza sul rapporto di lavoro del Commissario). Secondo l'art. 94a cpv. 1 dell'UFAP, il commissario deve astenersi dall'agire se potrebbe essere parziale in una questione a causa di un interesse personale o per altri motivi. È sufficiente l'apparenza di parzialità (art. 94a cpv. 1 UFAP). L'art. 94a cpv. 2 UFAP elenca (in modo non esaustivo) i seguenti motivi di parzialità:

- il particolare rapporto di prossimità o di amicizia o inimicizia personale con persone fisiche e giuridiche coinvolte o interessate da una transazione o da un processo decisionale (lett. a) e
- l'esistenza di un'offerta di lavoro da parte di una persona fisica o giuridica coinvolta o interessata da una transazione o da un processo decisionale (lett. b).

5 Per contro, nel contesto di un'indagine su una violazione delle disposizioni in materia di protezione dei dati, si applicano le disposizioni del diritto processuale amministrativo e quindi i motivi di ricusazione di cui all'art. 10 cpv. 1 LPD sono applicabili (art. 94a cpv. 4 UFAP e art. 52 cpv. 1 LPD). Questi includono, tra l'altro

- un interesse personale nella questione (art. 10 cpv. 1 lett. a LPD),
- il matrimonio, l'unione domestica registrata o la convivenza di fatto con una parte (art. 10 cpv. 1 lett. b LDP),
- parentela o affinità con una parte (art. 10 cpv. 1 lett. bbis APA), e
- la rappresentanza di una parte o l'agire per una parte nella stessa questione (art. 10 cpv. 1 lett. c APA).

III. DECISIONE SULLA RICUSAZIONE

6 I motivi di ricusazione sono di natura obbligatoria. Il delegato deve pertanto tenerne conto di propria iniziativa e portarli a conoscenza delle persone coinvolte. Se il delegato si ritira, il suo sostituto assume la direzione dei lavori.

Se invece la ricusazione del commissario è contestata, il presidente della divisione del Tribunale amministrativo federale competente per la protezione dei dati decide in merito (art. 47a LDP). La decisione può essere impugnata con un ricorso in materia di diritto pubblico al Tribunale federale (artt. 82 e segg. e art. 92 LFK). 7

Le opinioni espresse riflettono il parere personale degli autori e non sono vincolanti per l'Ufficio federale di giustizia.

BIBLIOGRAFIA

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.

MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 48 LPD

Un commentario di Carl Jauslin / Danielle Schneider

CITAZIONE SUGGERITA

Carl Jauslin/Danielle Schneider, Kommentierung zu Art. 48 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Jauslin/Schneider, N. XXX zu Art. 48 DSG.

Art. 48 Autocontrollo dell'IFPDT

Per mezzo di misure di controllo adeguate, in particolare in riferimento alla sicurezza dei dati, l'IFPDT assicura che al suo interno sia garantita l'esecuzione conforme delle norme federali sulla protezione dei dati.

STRUTTURA

In breve 601
I. Aspetti generali 601
II. Misure di controllo 603
A. Sicurezza dei dati in particolare 603
B. Applicazione legalmente conforme delle norme sulla protezione dei dati in generale 604
Bibliografia 605
I Materiali 605

IN BREVE

Il rispetto delle norme sulla protezione dei dati da parte dell'IFPDT è un obbligo legale che deriva già dalla sua qualità di organo federale. Poiché l'IFPDT non è sottoposto a un controllo esterno in materia di protezione dei dati, il legislatore lo obbliga ad autocontrollarsi: ai sensi dell'art. 48 LPD, l'IFPDT deve garantire l'esecuzione conforme alla legge mediante misure di controllo adeguate. L'art. 40 LADP specifica che l'IFPDT deve redigere un regolamento di trattamento per tutte le sue operazioni di trattamento automatizzato dei dati, indipendentemente dal fatto che tratti dati personali sensibili o che effettui una profilazione. Ciò garantisce che il rispetto delle norme sulla protezione dei dati sia monitorato anche all'interno dell'IFPDT, il che rafforza la credibilità dell'IFPDT come autorità di controllo nei confronti di terzi.

I. ASPETTI GENERALI

L'art. 48 LPD si rivolge all'IFPDT - ma non nella sua funzione di autorità di controllo, bensì di organo federale che tratta dati personali. Esso obbliga l'IFPDT ad assicurare misure di controllo adeguate per garantire la sicurezza dei dati in particolare e l'applicazione legalmente conforme delle norme federali sulla protezione dei dati in generale, anche all'interno della sua istituzione. Poiché non è previsto alcun controllo esterno sulla protezione dei dati per l'IFPDT in quanto autorità di vigilanza, con questa disposizione il legislatore obbliga l'IFPDT ad autocontrollare il trattamento dei dati personali. 1

L'IFPDT tratta i dati personali, compresi quelli particolarmente sensibili, per le seguenti finalità (art. 39 LDP): 2

- svolgere la propria attività di vigilanza (lett. a),
- per svolgere la propria attività di consulenza (lett. b),
- per la cooperazione con altre autorità (lett. c),
- per l'adempimento dei propri compiti nell'ambito delle disposizioni penali della LPD (lett. d),
- per l'adempimento dei suoi doveri ai sensi della Legge sull'informazione pubblica (lett. e-g),

- per informare la vigilanza parlamentare (lett. h), per informare il pubblico (lett. i) e per svolgere le proprie attività di formazione (lett. j).

L'IFPDT tratta dati personali sia nella sua funzione di commissario per la protezione dei dati che in quella di commissario per le informazioni pubbliche. In particolare, gestisce un sistema di amministrazione aziendale (art. 57h LOGA), un sistema di amministrazione del personale, un elenco di consulenti in materia di protezione dei dati (art. 10 cpv. 3 lett. d LPD; art. 10 cpv. 4 LPD in combinato disposto con l'art. 27 cpv. 2 LPD), l'elenco delle attività di trattamento degli organi federali (art. 12 cpv. 4 LPD) nonché un portale di segnalazione delle violazioni della sicurezza dei dati (art. 24 LPD). In particolare, nell'ambito dei suoi compiti legali, l'IFPDT può trattare dati personali dei suoi collaboratori, dati personali di altri collaboratori della Confederazione, nonché dati di terzi, compresi quelli di persone giuridiche (art. 57r LOGA).

3 L'IFPDT non è soggetto ad alcun controllo esterno sulla protezione dei dati, per cui è obbligato ad autocontrollarsi. La disposizione dell'art. 48 LPD chiarisce che anche l'IFPDT, in quanto autorità di controllo nel settore della protezione dei dati, non è al di sopra della legge sulla protezione dei dati e deve garantirne il rispetto anche all'interno della propria autorità. Il controllo esterno dell'IFPDT limiterebbe in modo sproporzionato la sua indipendenza rispetto al rischio piuttosto basso di abuso dei dati.

4 In quanto organo federale, l'IFPDT è vincolato non solo dalle disposizioni generali di cui agli articoli 5-13 e 16-29, ma anche dalle disposizioni speciali sul trattamento dei dati da parte degli organi federali di cui agli articoli 33 e seguenti. LPD. L'art. 48 LPD stabilisce che l'IFPDT deve prevedere misure di controllo adeguate per garantire il rispetto di questi obblighi. Questo obbligo di autocontrollo è dovuto al fatto che non esiste un corrispondente controllo esterno sulla protezione dei dati per l'IFPDT. Gli obblighi primari non sono quindi diversi da quelli degli altri organi federali; l'art. 48 LPD riguarda solo l'obbligo dell'IFPDT di controllare il rispetto di questi obblighi primari. In particolare, l'IFPDT deve adottare tutte le misure di controllo che normalmente esegue nell'ambito della sua attività di vigilanza nei confronti di altri organi federali, nella misura in cui queste si rivelano idonee anche nel caso dell'autocontrollo. Ciò rafforza la credibilità dell'IFPDT nella sua attività di vigilanza nei confronti degli organi federali e dei privati.

La disposizione dell'art. 48 LPD sull'autocontrollo da parte dell'IFPDT è stata integrata nella Legge federale sulla protezione dei dati con la revisione totale del 25 settembre 2020 (entrata in vigore il 1° settembre 2023). 5

II. MISURE DI CONTROLLO

A. Sicurezza dei dati in particolare

L'art. 48 LPD obbliga l'IFPDT a stabilire misure di controllo adeguate per garantire la sicurezza dei dati all'interno della propria istituzione. Ai sensi dell'art. 5 lett. h LPD, per violazione della sicurezza dei dati si intende "una violazione della sicurezza che comporta la perdita, la cancellazione, la distruzione o l'alterazione involontaria o illecita di dati personali, oppure la loro divulgazione o accessibilità a persone non autorizzate". 6

L'obbligo di garantire la sicurezza dei dati per l'IFPDT deriva già in modo generale dall'art. 8 LPD. Ai sensi di questa disposizione, i responsabili e gli incaricati del trattamento devono garantire una sicurezza dei dati adeguata al rischio mediante misure tecniche e organizzative adeguate. Le misure messe in atto devono consentire non solo di individuare a posteriori le violazioni della sicurezza dei dati, ma anche di prevenirle. La sicurezza dei dati è specificata nel DPO. In particolare, l'art. 3 del RGPD elenca una serie di misure tecniche e organizzative per raggiungere gli obiettivi di sicurezza dei dati ai sensi dell'art. 2 del RGPD, come ad esempio i controlli sull'accesso, sull'utente, sull'immissione e sulla divulgazione. Anche le disposizioni sul trattamento dei dati per gli organi federali ai sensi dell'art. 6 LADP servono a garantire la sicurezza dei dati. 7

In questo contesto, il Consiglio federale ha specificato l'obbligo di autocontrollo dell'IFPDT all'art. 40 della LDP. L'IFPDT deve redigere un regolamento di trattamento per tutti i trattamenti automatizzati, indipendentemente dal fatto che si tratti, ad esempio, di dati personali sensibili, di profilazione o che lo scopo del trattamento o il modo in cui i dati sono trattati possa comportare una grave interferenza con i diritti fondamentali della persona interessata. In effetti, l'art. 40 della legge sul trattamento dei dati personali dichiara inapplicabile l'art. 6 cpv. 1 della legge sul trattamento dei dati personali e le condizioni ivi contenute per la creazione di un regolamento sul trattamento dei dati nel caso dell'IFPDT. 8

9 Oltre all'obbligo di redigere un regolamento sul trattamento, l'art. 40 LADP non menziona altre misure nell'ambito dell'autoregolamentazione dell'IFPDT. Nelle note esplicative all'art. 40 LDT, l'Ufficio federale di giustizia afferma che anche l'IFPDT, come gli altri organi federali, deve prevedere processi interni corrispondenti che attuino le norme sul trattamento e ne verifichino la conformità. Tuttavia, la disposizione legale dell'art. 48 LPD parla in termini più generali di "misure di controllo adeguate, in particolare per quanto riguarda la sicurezza dei dati". Di conseguenza, la creazione, l'attuazione, la revisione e l'adeguamento regolare delle norme sul trattamento ai sensi dell'art. 40 LPD non esonera l'IFPDT dall'obbligo più generale di cui all'art. 48 LPD di prevedere misure di controllo più ampie, a condizione che queste siano giudicate adeguate e appropriate.

B. Applicazione legalmente conforme delle norme sulla protezione dei dati in generale

10 L'art. 48 LPD obbliga l'IFPDT a stabilire misure di controllo per garantire l'applicazione conforme alla legge delle disposizioni federali in materia di protezione dei dati. Questo obbligo va oltre la creazione e l'attuazione delle norme sul trattamento ai sensi dell'art. 40 LDP. In particolare, richiede che le operazioni di trattamento dei dati pianificate siano regolarmente controllate per verificarne la conformità con le disposizioni federali in materia di protezione dei dati. È proprio nell'ambito del sistema di controllo interno (SCI) che l'IFPDT deve prevedere ulteriori misure per garantire la conformità ai requisiti della LPD.

11 A differenza dell'obbligo di redigere un regolamento sul trattamento, tuttavia, le misure di controllo che vanno oltre sono necessarie solo se, da un lato, sono idonee a garantire il rispetto delle disposizioni sulla protezione dei dati e, dall'altro, sono proporzionate al rischio di abuso dei dati e alla minaccia per i diritti fondamentali della persona interessata. In particolare, l'obbligo dell'IFPDT non deve rendere impossibili o sproporzionatamente difficili i suoi compiti statutari di controllo e consulenza. Detto questo, l'IFPDT può tenere conto delle risorse umane necessarie nel contesto dell'autoregolamentazione nella sua richiesta di bilancio.

Il parere espresso riflette l'opinione personale degli autori e non è vincolante per l'Ufficio federale di giustizia.

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 49 LPD

Un commentario di Michael Reinle

CITAZIONE SUGGERITA

Michael Reinle, Kommentierung zu Art. 49 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Reinle, N. XXX zu Art. 49 DSG.

Sezione 2:
Inchiesta per violazione delle disposizioni sulla protezione dei dati

Art. 49 Inchiesta

[1] L'IFPDT apre, d'ufficio o su denuncia, un'inchiesta nei confronti di un organo federale o di un privato se indizi sufficienti lasciano presumere che un trattamento di dati potrebbe violare le disposizioni sulla protezione dei dati.

[2] Può rinunciare ad aprire un'inchiesta se la violazione delle disposizioni sulla protezione dei dati è di poca importanza.

[3] L'organo federale o il privato fornisce all'IFPDT tutte le informazioni e i documenti necessari per l'inchiesta. Il diritto di rifiutare di fornire

informazioni è retto dagli articoli 16 e 17 PA; è fatto salvo l'articolo 50 capoverso 2 della presente legge.

[4] Se la persona interessata ha sporto denuncia, l'IFPDT la informa sul seguito dato alla denuncia e sull'esito di un'eventuale inchiesta.

STRUTTURA

In breve 610
I. Generalità 610
A. Scopo e contesto normativo 610
B. Storia delle origini 610
II. Indagine 612
A. Differenza rispetto al diritto precedente 612
B. Apertura dell'indagine (cpv. 1) 613
C. Rinuncia alle indagini (cpv. 2) 614
D. Obbligo di cooperazione (cpv. 3) 615
E. Informazioni sull'interessato (cpv. 4) 617
Bibliografia 617
I materiali 618

IN BREVE

Questa disposizione è di fondamentale importanza per il rafforzamento delle competenze dell'FDPIC. Particolarmente importanti sono gli obblighi di collaborazione degli organi federali e delle persone private. La novità, anch'essa significativa, è che l'IFPDT può avviare un'indagine nei confronti di persone private se vi sono sufficienti indizi di una violazione delle norme sulla protezione dei dati. Con la precedente LPD, la competenza di indagare su persone private era più limitata.

I. GENERALITÀ

A. Scopo e contesto normativo

1 Mentre l'art. 4 LDP stabilisce in termini generali che l'IFPDT è responsabile della vigilanza sull'applicazione della legislazione federale in materia di protezione dei dati, l'art. 49 LDP disciplina una delle competenze più importanti dell'IFPDT in relazione a tale vigilanza, ossia l'indagine su eventuali violazioni della protezione dei dati da parte di organi federali e di privati.

2 Uno degli obiettivi più importanti della revisione della LADP è stato quello di rafforzare le competenze di vigilanza della DFP. Questo anche perché la precedente LDP era considerata poco incisiva per quanto riguarda la supervisione del trattamento dei dati da parte di privati (art. 29 dell'ALPD).

3 Inoltre, i precedenti poteri investigativi dell'IFPDT erano al di sotto degli standard internazionali, motivo per cui si temeva che, senza il rafforzamento dei poteri investigativi dell'IFPDT, una decisione positiva di adeguatezza dell'UE potesse essere messa in pericolo.

B. Storia delle origini

4 Nel concetto normativo per la revisione della legge sulla protezione dei dati, il rafforzamento delle competenze dell'IFPDT è stato indicato come una delle esigenze principali della revisione della LDP e, tra le altre cose, sono stati discussi l'introduzione di una procedura di indagine preliminare e il rafforzamento dei poteri investigativi.

Nell'art. 41 LDP sono state attuate diverse misure del concetto di norma: ad esempio, sono stati riuniti in un'unica disposizione i poteri investigativi nei confronti degli organi federali e delle persone private, precedentemente contenuti negli artt. 27 e 29 LDP, ed è stata regolamentata la procedura informale di indagine preliminare. Mentre l'art. 29 dell'ALPD consentiva l'apertura di indagini nei confronti di persone private solo a condizioni limitate, in futuro queste restrizioni sarebbero state eliminate. Ciò è stato giustificato anche dal fatto che le precedenti restrizioni dell'art. 29 aLPD non avrebbero soddisfatto i requisiti dell'E-SEV 108. I nuovi poteri investigativi dell'FDPIC sono stati un elemento cruciale anche per quanto riguarda l'art. 45 del Regolamento (UE) 2016/679 per garantire che la Commissione europea rinnovi o confermi la decisione di adeguatezza nei confronti della Svizzera. L'art. 41 VE-DSG è stato oggetto di una vivace discussione durante la consultazione. Mentre alcuni partecipanti alla consultazione hanno accolto con favore il rafforzamento dei poteri investigativi, altri hanno ritenuto che si spingesse troppo oltre. 5

Il contenuto dell'art. 43 della bozza di legge sulla protezione dei dati si basa sull'art. 41 della bozza di legge sulla protezione dei dati. Tuttavia, la procedura di indagine preliminare non è stata menzionata. Anche le misure d'indagine esplicitamente menzionate nell'art. 41 cpv. 3 LPD sono state omesse o copiate in un'altra disposizione. Nel messaggio sulla revisione della LDP è stato nuovamente sottolineato che la nuova regolamentazione dei poteri d'indagine dell'IFPDT è importante perché i suoi poteri di vigilanza nei confronti del settore privato non soddisfano attualmente i requisiti del progetto di decreto 108. L'art. 43 E-DSA è stato omesso o copiato in un'altra disposizione. 6

L'art. 43 E-DSA è stato oggetto di consultazioni parlamentari. In Consiglio nazionale, la discussione si è concentrata principalmente sui requisiti per l'apertura di un'indagine. La minoranza "Romano" voleva aumentare i requisiti minimi per l'apertura di un'indagine. La motivazione addotta era che semplici indizi di violazione delle norme sulla protezione dei dati non avrebbero soddisfatto i requisiti di una procedura basata sullo Stato di diritto. Si temeva inoltre che l'IFPDT potesse essere sovraccaricato se i requisiti fossero stati troppo bassi. La maggioranza, invece, non vuole "ammanettare" l'IFPDT. Il Consigliere federale Keller-Sutter ha sottolineato che la proposta della maggioranza - devono esserci indizi sufficienti e non solo segni di una violazione della protezione dei dati - non rappresenta un cambiamento 7

sostanziale rispetto all'art. 43 dell'e-DSA. Tuttavia, è critico nei confronti di un ulteriore aumento dei requisiti. La mozione di minoranza "Romano" comporterebbe un certo grado di incertezza giuridica nelle procedure dell'IFPDT. Inoltre, l'aumento dei requisiti per l'avvio della procedura metterebbe a rischio l'adeguatezza del livello svizzero di protezione dei dati in un settore particolarmente importante per l'UE. Né la Convenzione 108+ né gli atti giuridici dell'UE prevedono una tale limitazione dei poteri investigativi delle autorità di controllo della protezione dei dati. Il Consiglio nazionale ha seguito l'opinione della maggioranza.

8 Il Consiglio degli Stati ha condiviso la decisione del Consiglio nazionale in merito all'art. 43 cpv. 1 del progetto di legge sulla protezione dei dati. Il Consiglio degli Stati ha discusso principalmente l'art. 43 cpv. 3 del progetto di legge sulla protezione dei dati. Il dibattito ha riguardato la protezione del segreto professionale. Sebbene l'art. 43 cpv. 3 E-DSA protegga già il segreto professionale di avvocati e medici, la commissione del Consiglio degli Stati ha chiesto che la riserva del segreto professionale sia nuovamente menzionata in modo esplicito. L'onorevole Keller-Sutter ha difeso la proposta del Consiglio federale. Ha sottolineato che il segreto professionale è già sufficientemente protetto dalle leggi procedurali in vigore. Secondo il Consiglio federale, ribadire il segreto professionale tenderebbe a creare incertezze giuridiche. Ci si chiederebbe perché non siano stati citati nuovamente e in modo esplicito anche altri importanti motivi di rifiuto previsti dal diritto processuale generale. Tuttavia, il Consiglio degli Stati ha seguito la sua commissione. Il Consiglio nazionale ha seguito la decisione del Consiglio degli Stati.

II. INDAGINE

A. Differenza rispetto al diritto precedente

9 Finora le indagini contro gli organi federali e le persone private erano disciplinate da disposizioni diverse (artt. 27 e 29 dell'ALPD). Anche i requisiti per l'apertura di un'indagine erano diversi. L'art. 27 cpv. 2 dell'ALPD non prevedeva una soglia speciale per l'apertura di indagini contro gli organi federali. Secondo l'art. 29 cpv. 1 aLPD, invece, l'IFPDT poteva aprire un'indagine nei confronti di persone private solo se i metodi di trattamento potevano violare la personalità di un gran numero di persone (errore di sistema), se le raccolte di dati dovevano essere registrate o se sussisteva un

obbligo di informazione ai sensi dell'art. 6 cpv. 3 aLPD. Tuttavia, questi requisiti previsti dall'art. 29 cpv. 1 dell'ALPD non soddisfano gli standard internazionali.

I precedenti requisiti per l'apertura di un'indagine contro persone private sono stati eliminati. Inoltre, si applicano regole uniformi per l'apertura di indagini contro organi federali e persone private. Ciò comporta un rafforzamento dell'FDPIC. 10

B. Apertura dell'indagine (cpv. 1)

Ai sensi dell'art. 49 cpv. 1 LDP, l'IFPDT avvia un'indagine d'ufficio o su segnalazione se vi sono sufficienti indizi che un trattamento di dati possa violare le disposizioni in materia di protezione dei dati. 11

La segnalazione può essere fatta da terzi o dalla persona interessata, quindi in linea di principio da chiunque. Tuttavia, la persona che effettua la segnalazione non ha lo status di parte nel procedimento (art. 52 cpv. 2 LADP e contrario). La segnalazione può essere fatta anche in forma anonima. Poiché l'IFPDT deve avviare un'indagine solo se vi sono sufficienti indizi di una violazione della protezione dei dati, una segnalazione anonima può avere un impatto negativo su questa decisione. Il fatto che la segnalazione venga fatta o meno, ad esempio da una persona che ha un legame stretto con il trattamento dei dati segnalato, è quindi certamente rilevante ai fini di questa valutazione. 12

L'IFPDT può attivarsi anche se i comunicati stampa riferiscono di possibili violazioni della protezione dei dati, il che corrisponde già alla prassi attuale. 13

Le norme sulla protezione dei dati ai sensi dell'art. 4 cpv. 1 LADP non sono solo le norme della LADP, ma anche le norme settoriali sulla protezione dei dati della Confederazione. Sono comprese le disposizioni rilevanti per la protezione dei dati contenute in altri decreti federali e nei trattati internazionali specifici per la legge sulla protezione dei dati. Questa estensione oltre la LPD è rilevante soprattutto per gli organi federali. 14

Un'indagine può essere avviata solo se vi sono sufficienti indizi di una violazione delle disposizioni sulla protezione dei dati. Questo requisito è stato introdotto dal Parlamento (cfr. n. 7). Sulla base delle deliberazioni parlamentari, non è possibile trovare linee guida troppo chiare su cosa debba essere considerato un indizio sufficiente. Una minoranza del Consiglio 15

nazionale ha voluto che l'articolo 43 della legge sulla protezione dei dati elettronici fosse formulato come segue: "In caso di sospetto fondato, l'Incaricato apre un'indagine d'ufficio o su reclamo fondato contro un organo federale o una persona privata se vi sono chiari indizi che un'operazione di trattamento dei dati possa violare le disposizioni sulla protezione dei dati". Tuttavia, questi requisiti più severi - in particolare il requisito della presenza di chiari indizi - sono stati respinti. Gli indizi sufficienti non devono essere chiari indizi o ragionevoli sospetti ai sensi del diritto processuale penale. Secondo l'onorevole Keller-Sutter, gli indizi sufficienti non dovrebbero costituire un cambiamento sostanziale rispetto alla proposta del Consiglio federale, che parlava semplicemente di indizi. In fondo, anche il Consiglio federale non voleva che l'IFPDT esaurisse le sue risorse con indagini a tappeto. Devono esserci indicazioni che giustifichino l'impiego delle risorse dell'IFPDT. Le delibere parlamentari e in particolare i voti della maggioranza dimostrano che all'IFPDT doveva essere concesso un potere discrezionale in questo senso.

C. Rinuncia alle indagini (cpv. 2)

16 Ai sensi dell'art. 49 cpv. 2 LDP, l'IFPDT può rinunciare a un'indagine formale se la violazione delle disposizioni in materia di protezione dei dati è di scarsa importanza. Secondo il messaggio, questo sarebbe il caso, ad esempio, se un'associazione sportiva o culturale invia un messaggio e-mail a tutti i suoi membri senza nascondere l'identità dei destinatari. Secondo il messaggio, il paragrafo 2 può essere applicato anche se l'IFPDT ritiene che la consulenza fornita alla persona responsabile sia sufficiente per porre rimedio a una situazione di per sé poco problematica.

17 Secondo Rosenthal, una deroga dovrebbe essere possibile anche se, nel caso di notifiche di violazioni di dati, è evidente che la violazione non è grave o che il responsabile ha la situazione sotto controllo.

18 D'altro canto, vi sono argomenti contrari a una deroga se il trattamento dei dati in questione riguarda un gran numero di persone e vi è quindi un interesse generale da parte del pubblico.

19 L'IFPDT deve agire se ritiene che l'interesse pubblico sia sufficiente per un'indagine. D'altro canto, dovrebbe astenersi da un'indagine se è interessata solo la privacy di un individuo. In quest'ultimo caso, la persona interessata ha

la possibilità di intentare un'azione contro il privato davanti a un tribunale civile o di impugnare la decisione dell'organo federale davanti all'organo di reclamo competente.

Art. 49 cpv. 1 in combinato disposto con. L'art. 49 cpv. 1 in combinato disposto con l'art. 49 cpv. 2 LADP è una "disposizione facoltativa", che lascia all'IFPDT un certo margine di manovra nel decidere se aprire un'indagine o astenersi dal farlo. Il Parlamento ha lasciato questo margine di manovra all'IFPDT (cfr. n. 7). Spetta all'IFPDT decidere sull'opportunità di tale indagine. Pertanto, il whistleblower non ha ancora diritto allo svolgimento di un'indagine formale. 20

L'IFPDT ha già chiarito che continuerà a condurre contatti informali, ossia indagini preliminari. Se questi contatti informali dimostrano che la persona responsabile riconosce le carenze che sono state portate alla sua attenzione e vi pone rimedio entro un periodo di tempo ragionevole, l'IFPDT si asterrà dall'avviare un'indagine formale. A causa delle risorse limitate dell'IFPDT, si può generalmente presumere che continuerà a dare priorità alla gestione dei reclami anche dopo l'entrata in vigore della nuova FADP, in conformità con il principio di opportunità. 21

D. Obbligo di cooperazione (cpv. 3)

L'art. 49 cpv. 3 LDP disciplina l'obbligo di collaborazione della persona privata e dell'organo federale nell'ambito di un'indagine formale da parte dell'IFPDT, con il quale è stata adottata la maggior parte delle norme di cui agli artt. 27 cpv. 3 e 29 cpv. 2 aLPD. 22

La parte in causa deve fornire all'IFPDT tutte le informazioni e i documenti che l'IFPDT richiede per l'indagine. Ai sensi dell'art. 49 cpv. 3 LADP, una parte non è tenuta a fare di più che fornire informazioni e consegnare documenti. La collaborazione può essere richiesta in modo informale. Ulteriori misure nell'ambito dell'indagine sono disciplinate dagli artt. 50 e 52 della FADP. 23

Ai sensi dell'art. 49 cpv. 3 LADP, gli organi federali e il privato devono collaborare. Come nel diritto previgente, l'IFPDT può richiedere la collaborazione anche degli incaricati del trattamento dei dati con responsabilità primaria presso l'organo federale o la persona privata interessata, nonché di altri dipendenti, incaricati del trattamento, persone 24

ausiliarie e terzi che sono coinvolti nel trattamento dei dati da indagare o che possono fornire informazioni rilevanti al riguardo.

25 Gli obblighi di collaborazione di cui all'art. 49 cpv. 3 LADP possono riguardare informazioni su un caso specifico, ma possono anche essere di natura fondamentale. Essi riguardano tutti i documenti che possono essere rilevanti per la valutazione da parte dell'IFPDT.

26 Affinché le persone obbligate a collaborare non debbano incriminarsi, esiste anche il diritto di rifiutare informazioni nell'ambito dell'indagine dell'IFPDT. Il diritto di rifiutare informazioni si basa sugli articoli 16 e 17 della PA.

27 L'art. 16 cpv. 1 PA fa riferimento all'art. 42 cpv. 1 e 3 della Legge federale del 4 dicembre 1947 sulla procedura civile federale per quanto riguarda il diritto di rifiutare di testimoniare. Ai sensi dell'art. 42 commi 1 e 3 della legge federale sulla procedura civile, le persone interrogate possono rifiutarsi di testimoniare se rispondere alle domande può esporle al rischio di un procedimento penale. Ciò riguarda le persone soggette all'obbligo legale di segretezza ai sensi degli articoli 321, 321bis e 321ter CP. Ciò significa che i medici possono rifiutarsi di fornire all'IFPDT i dati personali dei loro pazienti se questi non acconsentono alla divulgazione. Lo stesso vale per gli avvocati e i loro clienti. L'art. 90 del GDPR prevede anche la possibilità di stabilire tali diritti di rifiuto nel diritto nazionale.

28 L'art. 50 cpv. 2 DPA prevede una disposizione derogatoria che rimane riservata. Questa stabilisce solo che il segreto professionale è riservato. Questa riserva è stata inserita durante la consultazione parlamentare (cfr. n. 8). Si tratta di un'enfasi che di per sé non sarebbe stata necessaria, dal momento che i segreti professionali legali sono già presi in considerazione attraverso la legge sulla procedura PA. La riserva del segreto professionale era già prevista dalla legge precedente. Tuttavia, il segreto professionale può essere opposto all'FDPIC solo se la persona protetta dal segreto professionale non libera la persona obbligata a collaborare dall'obbligo del segreto.

29 Il segreto d'ufficio non può essere opposto all'FDPIC.

30 Le persone obbligate a collaborare non possono inoltre invocare segreti aziendali e commerciali o obblighi di segretezza contrattuale.

31 Nel caso di indagini preliminari informali che precedono l'avvio di un'indagine formale, le persone private non sono tenute a fornire

informazioni all'IFPDT. L'art. 49 cpv. 3 LDP si applica solo dopo l'apertura di un procedimento formale. Tuttavia, può essere sensato per i responsabili del trattamento dei dati collaborare volontariamente con l'IFPDT se esiste la possibilità di chiarire la questione senza un procedimento formale.

Va notato che i documenti forniti all'IFPDT nell'ambito di un'indagine preliminare informale sono soggetti alla legge sull'accesso pubblico. L'indagine preliminare informale non rientra nell'art. 3 LTras. Secondo la sua stessa dichiarazione, l'IFPDT non può garantire alcuna restrizione o rifiuto di accesso da parte di terzi ai sensi dell'art. 7 LTras. Le informazioni particolarmente riservate e, ad esempio, i dati personali di terzi devono quindi essere elaborati prima della divulgazione. Inoltre, nel caso di informazioni particolarmente riservate, ad esempio informazioni sulle misure di sicurezza dei dati, può essere consigliabile non fornire le informazioni all'IFPDT per iscritto, ma presentargliele oralmente in loco durante un'ispezione o mostrargliele, ad esempio in occasione di una videoconferenza con schermo diviso. 32

E. Informazioni sull'interessato (cpv. 4)

L'interessato non è parte del procedimento (art. 52 cpv. 2 LDP e contrario). Ciò vale anche se l'interessato ha presentato un reclamo. L'interessato non ha quindi diritto di accedere al fascicolo. 33

Ai sensi dell'art. 49 cpv. 4 LDP, se l'interessato ha presentato un reclamo, l'IFPDT deve almeno informare l'interessato sulle ulteriori azioni da intraprendere e sull'esito dell'indagine. 34

L'interessato può quindi far valere i propri diritti attraverso i rimedi giuridici applicabili, ossia può adire un tribunale civile se il responsabile è una persona privata, oppure può presentare ricorso contro la decisione dell'organo federale competente. 35

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 50 LPD

Un commentario di Reto Fanger / Isabelle Oehri

CITAZIONE SUGGERITA

Reto Fanger/Isabelle Oehri, Kommentierung zu Art. 50 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Fanger/Oehri, N. XXX zu Art. 50 DSG.

Art. 50 Attribuzioni

[1] Se l'organo federale o il privato non ottempera all'obbligo di collaborare, l'IFPDT può, nell'ambito dell'inchiesta, ordinare in particolare:

a. l'accesso alle informazioni, ai documenti, ai registri delle attività di trattamento e ai dati personali necessari per l'inchiesta;

b. l'accesso ai locali e agli impianti;

c. l'interrogatorio di testimoni;

d. perizie di esperti.

[2] È fatto salvo il segreto professionale.

[3] Per eseguire i provvedimenti di cui al capoverso 1, l'IFPDT può far capo ad altre autorità federali o a organi di polizia cantonali o comunali.

STRUTTURA

I. Scopo e storia della norma 622
II. Il diritto all'informazione dell'FDPIC 624
A. Ordinazione di misure investigative 624
B. Ambito di applicazione personale e materiale 625
C. Limiti, in particolare la riserva del segreto professionale 626
III. Diritto Processuale 628
A. Panoramica 628
B. Il termine "ordine" 628
C. Ricorso legale 631
D. Esecuzione 631
E. Nessun compenso 632
Bibliografia 633
I Materiali 635

I. SCOPO E STORIA DELLA NORMA

1 Se l'IFPD conduce un'indagine su sospette violazioni della protezione dei dati da parte di un organo federale o di una persona privata, in linea di principio deve fornire tutte le informazioni e i documenti necessari all'indagine ai sensi dell'art. 49 cpv. 3 LPD. Per garantire che le attività di controllo possano essere svolte efficacemente anche se i responsabili non adempiono ai loro obblighi di collaborazione, l'art. 50 LPD conferisce all'IFPD alcuni poteri di indagine e di intervento al fine di chiarire i fatti in modo completo, rapido e preciso.

2 L'art. 50 LPD intende soddisfare i requisiti attuali e futuri del diritto internazionale, che la Svizzera deve rispettare in quanto Stato membro della Convenzione ETS 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati personali e in quanto Stato Schengen. L'art. 15 cpv. 2 lett. a del Protocollo di modifica del 18 maggio 2018 alla Convenzione ETS 108 prevede che gli Stati membri dotino le proprie autorità di controllo della protezione dei dati di poteri di indagine e di intervento. Analogamente, l'art. 47 cpv. 1, della Direttiva (UE) 2016/680 prevede che gli Stati dell'UE e di Schengen prevedano effettivi poteri di indagine per le loro autorità di controllo, in particolare il potere di accedere a tutti i dati personali trattati e a tutte le informazioni necessarie per lo svolgimento dei loro compiti.

3 Alla luce dell'art. 45 del Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati, GDPR), secondo cui il trasferimento di dati personali dall'UE a Paesi terzi può essere effettuato solo se il Paese terzo in questione offre un livello di protezione adeguato conformemente a una decisione della Commissione europea, il legislatore svizzero ritiene che i nuovi poteri d'indagine dell'IFPDT siano un elemento cruciale per garantire che l'UE mantenga la sua decisione di adeguatezza nei confronti della Svizzera.

4 Rispetto alla legge sulla protezione dei dati del 1992 (aLPD), l'art. 50 LPD rappresenta un chiarimento e un rafforzamento della posizione dell'IFPD. L'art. 27 cpv. 3 dell'aLPD (nell'ambito della vigilanza sugli organi federali) e l'art. 29 cpv. 3 dell'aLPD (nel settore privato) prevedevano già la possibilità di richiedere fascicoli, ottenere informazioni e far elaborare dati nell'ambito di indagini conoscitive. Le persone responsabili erano tenute a collaborare, fatto salvo il diritto di rifiutarsi di testimoniare che si applica, mutatis mutandis, ai

sensi dell'art. 16 PA (cfr. art. 27 cpv. 3 aDSG e art. 34 cpv. 2 lett. b aDSG). Tuttavia, se i responsabili non collaborano di propria iniziativa, l'IFPDT non ha a disposizione misure coercitive dirette per ottenere informazioni (ad esempio, la possibilità di sequestrare informazioni o accedere a luoghi, impianti o sistemi anche contro la volontà della persona autorizzata). In caso di rifiuto a collaborare da parte di un organo federale, l'IFPDT può rivolgersi solo a un'unità di livello superiore con il diritto di impartire istruzioni allo stesso; nel settore privato, l'unica opzione a sua disposizione è infatti quella di presentare una denuncia penale per violazione dell'obbligo di collaborazione (art. 34 cpv. 2 lett. b aLPD). Nei casi più gravi di rifiuto a collaborare da parte di un organo federale o di un privato, egli può anche informare il pubblico ai sensi dell'art. 30 cpv. 2 dell'ALPD.

I limitati poteri investigativi dell'IFPD ai sensi dell'ALPD sono stati talvolta oggetto di critiche da parte di accademici e professionisti della protezione dei dati. Nel 2014, ad esempio, il gruppo di accompagnamento per la revisione della LPD ha suggerito di ampliare i poteri di raccolta di informazioni dell'IFPD. Di conseguenza, il rafforzamento della posizione dell'IFPDT nelle sue attività investigative è una risposta ai requisiti internazionali (cfr. n. 2 f. sopra) e alle debolezze individuate dalla dottrina e dalla prassi. 5

La pratica dimostrerà se il nuovo regime dei poteri d'indagine della DFP, insieme ai suoi poteri correttivi cautamente ampliati (cfr. OK-Fanger/Oehri sull'art. 51 LPD), garantisce un'attività di vigilanza efficace. Oltre alla corrispondente ripartizione delle competenze, una vigilanza efficace richiede anche che la DFP sia dotata di risorse adeguate. A questo proposito, in letteratura sono state espresse alcune critiche sulle risorse, considerate troppo scarse e che, nonostante un aumento già avvenuto, probabilmente continueranno a costringere l'IFPDT a procedere secondo il principio di opportunità nelle sue attività di vigilanza. Anche i valutatori Schengen 2018 sono stati critici a questo proposito e hanno raccomandato di assegnare all'FDPIC risorse finanziarie e umane sufficienti per consentirgli di svolgere tutti i suoi compiti nel contesto Schengen. 6

II. IL DIRITTO ALL'INFORMAZIONE DELL'FDPIC

A. Ordinazione di misure investigative

7 Se l'IFPD avvia un'indagine nei confronti di un organo federale o di una persona privata ai sensi dell'art. 49 cpv. 1 LPD a causa di una sospetta violazione della protezione dei dati, spetta in linea di principio all'organo federale o alla persona privata interessata fornire all'IFPD tutte le informazioni e i documenti necessari per l'indagine (art. 49 cpv. 3 LPD). Se la persona responsabile non adempie agli obblighi di collaborazione di cui all'art. 49 cpv. 3 LPD, l'art. 50 cpv. 1 LPD conferisce all'IFPDT la competenza di ordinare misure per ottenere informazioni. L'ordine di tali misure è subordinato alla collaborazione della persona responsabile e presuppone quindi che l'IFPDT abbia avviato un'indagine e abbia cercato invano di ottenere le informazioni e i documenti necessari.

8 L'elenco delle misure possibili per ottenere informazioni di cui all'art. 50 cpv. 1 LPD si basa su quello dell'art. 12 PA e non è esaustivo. In particolare, l'IFPDT può chiedere l'accesso a tutte le informazioni, i documenti, gli elenchi delle attività di trattamento e i dati personali necessari per l'indagine (lett. a), nonché ai locali e agli impianti (lett. b), e può ordinare l'esame di testimoni (lett. c) e le perizie di esperti (lett. d).

9 Per consentire un'indagine mirata, il concetto di accesso (art. 50 cpv. 1 lett. a e lett. b LPD) deve essere inteso in senso ampio. Pertanto, l'accesso ai documenti comprende non solo la loro ispezione, ma anche il loro sequestro, se necessario. Per quanto riguarda le misure di accesso di cui all'art. 50 cpv. 1 lett. a e lett. b LPD, il regolamento si basa essenzialmente sulle disposizioni pertinenti del GDPR (art. 58 cpv. 1 lett. e e lett. f GDPR). Di norma, le informazioni vengono raccolte tramite un questionario e tutti i documenti rilevanti per l'indagine vengono registrati. Ai sensi dell'art. 12 cpv. 1 LPD, l'elenco delle attività di trattamento deve essere redatto e conservato dal responsabile del trattamento e dall'incaricato del trattamento indipendentemente da qualsiasi indagine sulla protezione dei dati, tranne nei casi eccezionali di cui all'art. 12 cpv. 5 LPD, che tuttavia sono molto estesi in Svizzera in quanto paese di PMI e quindi saranno probabilmente la regola. Anche in questo caso, l'ordine di cui all'art. 50 cpv. 1 LADP riguarda l'ispezione e, se necessario, il sequestro, ma non la corretta tenuta dei registri. Quest'ultima può essere oggetto di un ordine basato sui risultati dell'indagine

ai sensi dell'art. 51 LPD. Se necessario, può essere ordinata anche la divulgazione dei dati personali necessari per l'indagine, ai sensi dell'art. 50 cpv. 1 lett. a LPD. L'accesso ai locali e alle strutture può essere necessario se le misure tecniche e organizzative (TOM) sono oggetto dell'indagine. Menzionando l'esame di testimoni e perizie, l'art. 50 cpv. 1 LPD va oltre il GDPR, che non contiene alcuna norma esplicita al riguardo.

Rispetto all'ALPD, l'elenco esemplare delle possibili misure investigative di cui all'art. 50 cpv. 1 LPD comporta un'espansione selettiva dei poteri di informazione (cfr. n. 4 sopra). Tuttavia, l'ampliamento essenziale della posizione dell'IFPDT in materia di acquisizione di informazioni consiste principalmente nel rafforzamento dei meccanismi di esecuzione (cfr. infra, n. 18 e segg.). 10

B. Ambito di applicazione personale e materiale

Affinché l'IFPDT possa adempiere ai suoi compiti di vigilanza legale, i diritti di raccolta di informazioni che gli spettano devono essere strutturati in modo completo. 11

In termini personali, le informazioni sono ottenute in primo luogo dall'organo federale o dalla persona privata interessata, ma possono comprendere anche altri organi o persone coinvolti nel trattamento dei dati in questione (ad esempio, collaboratori, ausiliari, agenti, partner di outsourcing) o terzi che possono fornire informazioni rilevanti (ad esempio, persone interessate, autorità, ex collaboratori, partner commerciali). Nell'ambito dell'ALPD, il gruppo di persone da cui l'FDPIC può ottenere informazioni nel corso delle sue indagini era già ampiamente definito. L'inclusione esplicita delle audizioni di testimoni e delle perizie nell'art. 50 cpv. 1 LPD rende ora chiaro nel testo giuridico anche il possibile coinvolgimento di terzi. Mentre il dovere della persona responsabile di collaborare come parte si basa sull'art. 49 cpv. 3 LPD e sull'art. 13 cpv. 1 lett. c PA, quello di terzi si basa sugli artt. 15 e 17 PA. Restano riservati i diritti di rifiuto applicabili nei singoli casi (cfr. infra, n. 14 e segg.). 12

Anche il diritto all'informazione dell'IFPDT deve essere interpretato in senso lato da un punto di vista fattuale. L'art. 50 cpv. 1 lett. a LPD menziona specificamente tutte le informazioni, i documenti, gli elenchi delle attività di trattamento e i dati personali necessari per l'indagine. Pertanto, il diritto 13

all'informazione si estende a tutte le informazioni relative a un caso specifico o di natura generale che siano rilevanti e necessarie per una valutazione legale della presunta violazione della protezione dei dati. Ciò include tutti i documenti e le informazioni che potrebbero dire se, quando e come gli organismi responsabili rispettano i requisiti della legge sulla protezione dei dati, in particolare quelli che possono essere utilizzati per valutare l'accuratezza dei dati, la liceità del loro trattamento e il rispetto dei diritti degli interessati. Sono inclusi anche documenti e informazioni sul personale, sulle misure tecniche e organizzative, sulla documentazione relativa alle procedure, ai programmi e ai sistemi, nonché su tutte le basi giuridiche (ad es. direttive, linee guida, opuscoli, contratti) relative all'attuazione delle disposizioni sulla protezione dei dati.

C. Limiti, in particolare la riserva del segreto professionale

14 Il diritto all'informazione dell'IFPDT e il relativo dovere di collaborazione da parte degli organi federali e delle persone private oggetto di indagine, nonché di terzi, non sono ovviamente illimitati. Trovano i loro limiti nei relativi diritti di rifiuto. A questo proposito, l'art. 49 cpv. 3 LDP stabilisce che il diritto di rifiutare informazioni da parte degli organi federali e delle persone private è disciplinato dagli artt. 16 e 17 LDP, a meno che l'art. 50 cpv. 2 LDP non disponga diversamente. L'art. 16 e l'art. 17 PA si applicano anche ai terzi.

15 Secondo l'ordinamento applicabile, che risulta dall'interazione tra la LPD e la Legge sulla procedura amministrativa e dal riferimento parziale alla Legge federale sulla procedura civile e al Codice penale, le informazioni e anche altre forme di cooperazione, ad esempio sotto forma di consegna di documenti, possono essere rifiutate in ogni caso:

- se il collaboratore esporrebbe se stesso o una persona vicina al rischio di un procedimento penale o di un grave danno all'onore o causerebbe un danno patrimoniale diretto a se stesso o a una persona vicina (art. 16 cpv. 1 PA in combinato disposto con l'art. 42 cpv. 1 lett. a BZP);
- se il collaboratore può invocare la protezione delle fonti per i professionisti dei media (art. 16 cpv. 1 PA in combinato disposto con l'art.

42 cpv. 1 lett. a BZP). Art. 42 cpv. 1 lit. abis BZP in combinato disposto con. Art. 28a SCC);

- se il collaboratore può invocare un segreto professionale ai sensi dell'art. 321 n. 1 CP e la persona avente diritto al segreto non ha acconsentito alla divulgazione del segreto (art. 16 cpv. 1 PA in combinato disposto con l'art. 42 cpv. 1 lett. abis BZP in combinato disposto con l'art. 28a CP). Art. 42 cpv. 1 lett. b BZP in combinato disposto con. Art. 321 cpv. 1 CP);
- se la corrispondenza proviene da un avvocato (art. 17 PA in combinato disposto con l'art. 51a BZP).

D'altra parte, invocare segreti di fabbricazione o commerciali, obblighi di segretezza contrattuale o segreto d'ufficio non esime una persona dal partecipare a un'indagine dell'IFPDT. L'IFPDT, dal canto suo, è vincolato dalle disposizioni di legge applicabili - in particolare in materia di protezione dei dati e di tutela dei segreti industriali e commerciali - ed è soggetto al segreto d'ufficio ai sensi dell'art. 22 dell'UFAP, che, secondo il legislatore, garantisce il trattamento confidenziale delle informazioni ottenute nel corso delle sue indagini. 16

Secondo la prassi dell'aLPD, i detentori di altri segreti professionali, ad esempio le persone soggette al segreto bancario (art. 47 della legge sulle banche), al segreto professionale nella ricerca medica (art. 321bis CP) o al segreto postale e delle telecomunicazioni (art. 321ter CP), non potrebbero invocare il diritto di rifiutare di collaborare alle indagini in base alla legge sulla protezione dei dati, ai sensi dell'art. 16 cpv. 2 PA in combinato disposto con l'art. 42 cpv. 2 BZV. Art. 42 cpv. 2 BZP. La questione è se la riserva esplicita del segreto professionale nel nuovo art. 50 cpv. 2 LPD cambi qualcosa a questo proposito. Questa disposizione è stata inserita solo durante il dibattito parlamentare. Tuttavia, il dibattito parlamentare in questione suggerisce, secondo l'opinione espressa in questa sede, che l'esplicita menzione del segreto professionale sia solo una precisazione e non significhi un cambiamento della situazione giuridica e della prassi. 17

III. DIRITTO PROCESSUALE

A. Panoramica

18 Mentre il contenuto del diritto all'informazione dell'IFPD ai sensi dell'art. 50 cpv. 1 LPD è stato probabilmente ampliato solo sotto certi aspetti rispetto al vecchio diritto (cfr. n. 7 e segg.), la posizione dell'IFPD in merito alla sua applicazione è stata notevolmente rafforzata. In base all'ALPD, l'IFPD poteva disporre misure investigative, ma non poteva imporle in caso di controparte non collaborativa (cfr. n. 4). La raccolta di informazioni da parte dell'IFPDT è ora regolata in tre fasi:

- In primo luogo, avviene attraverso una richiesta informale dell'IFPDT all'organo federale o alla persona privata contro cui è stata aperta un'indagine. Ai sensi dell'art. 49 cpv. 3 LPD, la persona responsabile è tenuta a fornire informazioni e a consegnare documenti, nella misura in cui ciò sia necessario per l'indagine, se non può far valere il diritto di rifiutare la propria collaborazione.
- In subordine, se l'ottenimento di informazioni attraverso la sola comunicazione di informazioni e la consegna di documenti da parte dell'organo federale o della persona privata interessata è infruttuoso o insufficiente, l'IFPD può "ordinare" misure investigative ai sensi dell'art. 50 cpv. 1 LPD (cfr. infra, n. 19 e segg.).
- Infine, l'IFPD può coinvolgere altre autorità federali e le autorità di polizia cantonali o comunali per eseguire le misure ordinate ai sensi dell'art. 50 cpv. 1 LPD, conformemente all'art. 50 cpv. 3 LPD.

B. Il termine "ordine"

19 La legge e la documentazione non indicano esplicitamente cosa si intenda con il termine "ordine" o in quale forma debba essere emesso. Mentre nel contesto delle misure amministrative che l'IFPD può emettere in base all'art. 51 LPD dopo la conclusione di un'indagine, la facoltà dell'IFPD di emettere un'ordinanza è discussa in modo preponderante sia nel messaggio che nella ricezione della nuova disposizione nella letteratura (cfr. OK-Fanger/Oehri sull'art. 51 LPD, n. 1 e segg.), per quanto riguarda le misure d'indagine ai sensi dell'art. 50 LPD non si discute se anche la loro ordinanza abbia il carattere di

ordinanza o se debba essere qualificata come un vero e proprio atto dell'autorità.

Le disposizioni della PA applicabili al procedimento d'indagine ai sensi dell'art. 50 LDP in virtù del rinvio di cui all'art. 52 cpv. 1 LDP, in particolare gli artt. 12-19 LDP, nonché gli artt. 37, 39-41 e 43-61 LDP, anch'essi applicabili in virtù dell'ulteriore rinvio di cui all'art. 19 LDP, tutti rilevanti per l'accertamento dei fatti nel procedimento amministrativo, non determinano espressamente la forma in cui devono essere disposti i provvedimenti d'indagine. 20

Secondo l'opinione espressa in questa sede e spiegata in dettaglio qui di seguito, la disposizione di provvedimenti istruttori deve assumere la forma di un'ordinanza processuale (provvisoria). 21

A differenza di quanto avviene nel settore della procedura civile, le ordinanze di prova vera e propria non sono comuni nei procedimenti amministrativi, nei quali prevale la massima istruttoria. Tuttavia, le misure probatorie o investigative sono generalmente ordinate sotto forma di ingiunzioni in molti settori amministrativi. Sebbene la giurisprudenza non si occupi quasi mai in dettaglio della natura giuridica delle ordinanze in questione, nella maggior parte di queste decisioni la corte giudicante assume un'ordinanza senza ulteriori considerazioni sull'oggetto della contestazione. 22

Nelle decisioni in cui la Corte Suprema Federale ha dovuto affrontare specificamente la questione se l'ordine di una misura investigativa in un caso specifico si qualifichi o meno come un ordine (contestabile), il quadro non è uniforme: a volte un ordine corrispondente è classificato come un ordine provvisorio procedurale, a volte come un atto ufficiale reale. Nella sua giurisprudenza più recente, la Corte Suprema Federale sembra assumere sempre più spesso che l'ordinanza sia di natura ingiuntiva. Tuttavia, non si possono trarre affermazioni generali per tutti i settori amministrativi. 23

In riferimento al fatto che l'ordine di misure probatorie nell'ambito dell'obbligo di cooperazione crea sempre un obbligo legale, la dottrina sostiene - giustamente secondo l'opinione qui rappresentata - la qualificazione come ordine. In alcuni casi, si distingue se l'adempimento dell'obbligo di cooperazione può essere imposto mediante sanzioni (coercizione diretta, ammenda, ecc.). Nella misura in cui ciò è previsto dalla legge e quindi si tratta di un vero e proprio obbligo legale, l'ordine di 24

collaborare a questo proposito deve essere strutturato come un ordine provvisorio se la minaccia di astenersi è così specifica da poter essere eseguita.

25 Se un atto amministrativo interferisce fortemente con la posizione giuridica del destinatario, è opportuna un'ingiunzione, in modo che il destinatario possa avviare un riesame da parte di una corte d'appello, se necessario. È improbabile che l'ente federale o il privato, in quanto parte in causa in un'indagine ai sensi della legge sulla protezione dei dati, accetti di ordinare misure investigative: Dopo che il responsabile del trattamento non ha voluto o non ha potuto fornire le informazioni necessarie per la valutazione di una possibile violazione della protezione dei dati nell'ambito dell'indagine informale dell'IFPD, si può presumere che non sarà improvvisamente in grado o disposto a collaborare sufficientemente di sua iniziativa, nemmeno in risposta a un ordine ai sensi dell'art. 50 cpv. 1 LPD. In considerazione del diritto a un equo processo, è ancora più importante che egli abbia la possibilità di far riesaminare l'ordinanza contestata da un tribunale, ai sensi dell'art. 52 cpv. 1 LPD in combinato disposto con la legge sulla procedura amministrativa. Inoltre, l'IFPDT può eseguire le misure investigative ordinate, nella misura in cui possono essere eseguite coattivamente, con l'aiuto di altre autorità federali e delle autorità di polizia cantonali e comunali ai sensi dell'art. 50 cpv. 3 LPD. La mancata collaborazione è punita dall'art. 60 LPD. In altre parole, le misure investigative ai sensi dell'art. 50 cpv. 1 LPD danno regolarmente luogo a veri e propri obblighi giuridici per la parte processuale, motivo per cui devono essere ordinate per decreto.

26 Lo stesso vale per l'obbligo di collaborazione di terzi, che può essere eseguito (art. 50 cpv. 3 LPD) e la cui inosservanza può avere anche conseguenze penali (art. 52 cpv. 1 LPD in combinato disposto con l'art. 60 PA). Se vengono convocati come testimoni o viene loro richiesto di modificare documenti o di concedere l'accesso a locali e impianti, ciò costituisce un'interferenza sostanziale contro la quale deve essere disponibile un rimedio legale prima dell'esecuzione forzata o della sanzione della mancata collaborazione.

27 Dal punto di vista dell'economia procedurale, si può certamente obiettare che, a seconda delle circostanze del singolo caso, la disposizione di misure investigative può portare a procedimenti investigativi molto lunghi e costosi. Tuttavia, ciò è accettabile per ragioni di Stato di diritto. L'IFPDT non deve imporre requisiti eccessivi alla giustificazione delle misure investigative, in

modo che un'ordinanza sotto forma di decreto non comporti una spesa aggiuntiva significativa rispetto a un atto puramente reale. La procedura rischia di essere ritardata se è possibile un ricorso indipendente (art. 52 cpv. 1 LPD in combinato disposto con l'art. 46 cpv. 1 PA), cosa che nel presente contesto avverrà solo in casi eccezionali (cfr. in dettaglio infra n. 28). Inoltre, se necessario, l'IFPDT può revocare l'effetto sospensivo di un ricorso (art. 52 cpv. 1 LPD in combinato disposto con l'art. 55 cpv. 2 PA). Infine, soprattutto in caso di indagini complesse con procedimenti lunghi, a volte può essere necessaria l'ordinanza cautelare di misure amministrative ai sensi dell'art. 51 LPD (cfr. OK-Fanger/Oehri sull'art. 51 LPD, n. 22 e segg.).

C. Ricorso legale

Se si concede all'ordinanza di misure investigative il carattere di ingiunzione, essa può essere impugnata ai sensi dell'art. 52 cpv. 1 LPD in combinato disposto con l'art. 46 cpv. 1 VwG. L'art. 46 cpv. 1 PA può essere impugnato autonomamente con un ricorso al Tribunale amministrativo federale. 28

Il ricorso dovrebbe essere possibile soprattutto se l'ordinanza può causare un danno irreparabile ai sensi dell'art. 46 cpv. 1 lett. a PA. Questo è il caso se vengono sollevate obiezioni contro le misure probatorie ordinate che non possono essere sollevate senza svantaggio impugnando la decisione finale. L'art. 46 cpv. 1 lett. b PA, secondo il quale il ricorso è ammissibile anche se la sua approvazione porterebbe immediatamente a una decisione definitiva e quindi a un notevole risparmio di tempo o di costi per un lungo procedimento probatorio, difficilmente sarà rilevante per quanto riguarda gli atti di indagine ai sensi della legge sulla protezione dei dati. 29

Se il ricorso è ammissibile, la decisione del Tribunale amministrativo federale può essere successivamente impugnata davanti al Tribunale federale mediante un ricorso in materia di diritto pubblico (art. 82 lett. a in combinato disposto con l'art. 86 cpv. 1 lett. a LTF). In questo caso, oltre al destinatario dell'ordinanza, anche l'IFPDT ha il diritto di ricorrere (art. 52 cpv. 3 LPD). 30

D. Esecuzione

L'art. 50 cpv. 3 LPD prevede che l'IFPD possa coinvolgere altre autorità federali e le autorità di polizia cantonali o comunali nell'esecuzione delle misure di cui all'art. 50 cpv. 1 LPD. L'art. 54 cpv. 2 lett. c LPD stabilisce inoltre 31

che l'IFPD può comunicare alle autorità consultate le informazioni e i dati personali necessari per l'adempimento dei loro compiti legali.

32 L'art. 50 cpv. 3 LPD è stato modificato nel corso dell'iter legislativo. Fino alla LPD del 2017, la disposizione in questione conferiva esplicitamente all'IFPD la facoltà di ordinare misure cautelari per la durata dell'inchiesta e di farle eseguire da un'autorità federale o dagli organi di polizia cantonali o comunali (art. 44 cpv. 2 LPD [2017]). La versione finale della disposizione non contiene più alcuna menzione diretta di misure cautelari (cfr. sulla possibilità di ordinare misure cautelari durante la durata di un'indagine sulla protezione dei dati, OK-Fanger/Oehri sull'art. 51 LPD, n. 22 e segg.).

33 Per quanto riguarda l'esecuzione, si applicano inoltre le norme della legge sulla procedura amministrativa (LPD), in particolare gli artt. 39-43 LPD, nella misura in cui l'art. 50 FADP non disponga altrimenti. Di conseguenza, l'esecuzione richiede che non sia disponibile alcun rimedio legale con effetto sospensivo contro l'ordinanza (art. 52 cpv. 1 LPD in combinato disposto con l'art. 39 PA). Per quanto riguarda i possibili mezzi di coercizione (cfr. art. 52 cpv. 1 LPD in combinato disposto con l'art. 41 PA), l'accesso coercitivo e la perquisizione di locali e impianti, nonché il sequestro di impianti, documenti, elenchi di attività di trattamento e dati personali svolgeranno principalmente un ruolo nella pratica. Può essere presa in considerazione anche la minaccia di una pena (cfr. art. 60 LPD e art. 52 cpv. 1 LPD in combinato disposto con l'art. 60 PA). Per contro, la produzione obbligatoria di parti per fornire informazioni o di testimoni non dovrebbe quasi mai essere presa in considerazione, soprattutto perché il principio di proporzionalità si applica sempre per quanto riguarda i mezzi di coercizione utilizzati (Art. 52 cpv. 1 LPD in combinato disposto con l'Art. 42 PA).

E. Nessun compenso

34 L'art. 59 cpv. 1 lett. d LPD stabilisce che l'IFPD riscuote una tassa dai privati per l'emissione di misure cautelari e di misure (amministrative) ai sensi dell'art. 51 LPD. Per quanto riguarda la procedura d'inchiesta, ciò significa al contrario che, in assenza di una base legale corrispondente, non è possibile imporre alcun emolumento a un organo federale in nessun caso. Inoltre, secondo il messaggio relativo all'e-DSA (2017), si dovrebbe concludere che non vengono riscossi emolumenti per le indagini contro persone private che si concludono senza ordinare misure cautelari o amministrative.

La prevista esenzione dalle tasse è convincente per i procedimenti d'indagine in cui il chiarimento dei fatti è formalmente semplice, ossia può essere effettuato senza un'ordinanza formale di misure investigative solo grazie alla collaborazione di una persona responsabile che collabora pienamente, e d'altra parte ha un effetto liberatorio, ossia non porta a misure amministrative. Si può anche sostenere che l'ordine di misure investigative su terzi, nella misura in cui queste non siano state rese necessarie da una mancanza di cooperazione da parte del responsabile del trattamento, non dovrebbe comportare alcuna conseguenza finanziaria per quest'ultimo. Tuttavia, l'art. 50 LPD non si limita a queste fattispecie, ma si applica in particolare se il responsabile non collabora sufficientemente alla procedura di indagine (cfr. art. 50 cpv. 1 LPD). Secondo l'opinione qui espressa, l'ordine di misure investigative, che si sono rese necessarie solo perché la persona responsabile non ha adempiuto ai suoi doveri di collaborazione senza giustificazione, dovrebbe in ogni caso avere conseguenze di costo nella sfera privata, anche se, dopo il completo svolgimento dell'indagine, che è stata aperta in risposta a indicazioni sufficienti ai sensi dell'art. 49 cpv. 1 LPD, risulta che non vi è stata alcuna violazione delle disposizioni sulla protezione dei dati e quindi non è necessario ordinare misure amministrative ai sensi dell'art. 51 LPD. 35

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 51 LPD

Un commentario di Reto Fanger / Isabelle Oehri

CITAZIONE SUGGERITA

Reto Fanger/Isabelle Oehri, Kommentierung zu Art. 51 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Fanger/Oehri, N. XXX zu Art. 51 DSG.

Art. 51 Provvedimenti amministrativi

[1] Se sono state violate le disposizioni sulla protezione dei dati, l'IFPDT può ordinare di adeguare, sospendere o cessare del tutto o in parte il trattamento nonché di cancellare o distruggere del tutto o in parte i dati personali.

[2] L'IFPDT può sospendere o vietare la comunicazione di dati personali all'estero se questa è contraria alle condizioni di cui agli articoli 16 o 17 oppure alle disposizioni di altre leggi federali riguardanti la comunicazione di dati personali all'estero.

[3] L'IFPDT può segnatamente disporre che l'organo federale o il privato:

a. lo informi conformemente agli articoli 16 capoverso 2 lettere b e c nonché 17 capoverso 2;

b. adotti i provvedimenti di cui agli articoli 7 e 8;

c. informi le persone interessate conformemente agli articoli 19 e 21;

d. proceda a una valutazione d'impatto sulla protezione dei dati conformemente all'articolo 22;

e. lo consulti conformemente all'articolo 23;

f. lo informi o, se del caso, informi la persona interessata, conformemente all'articolo 24;

g. fornisca alla persona interessata le informazioni di cui all'articolo 25.

4 Può inoltre disporre che il titolare privato del trattamento con sede o domicilio all'estero designi un rappresentante secondo l'articolo 14.

5 Se durante l'inchiesta l'organo federale o il privato ha adottato i provvedimenti necessari per ristabilire il rispetto delle disposizioni sulla protezione dei dati, lo IFPDT può limitarsi a pronunciare un ammonimento.

STRUTTURA

I. Scopo e storia della norma 640
II. Misure amministrative 642
A. Misure contro il trattamento dei dati in violazione delle norme sulla protezione dei dati (art. 51 cpv. 1, 2 e 4 LPD) 643
B. Misure di accompagnamento in caso di violazione delle disposizioni normative o degli obblighi nei confronti degli interessati (art. 51 cpv. 3 LPD) 644
III. Diritto procedurale 646
A. Generalità 646
B. Misure cautelari 647
Bibliografia 649
I materiali 650

I. SCOPO E STORIA DELLA NORMA

1 L'art. 51 LPD descrive le misure amministrative che l'IFPD può adottare in caso di violazione delle disposizioni sulla protezione dei dati. Il potere di emanare ordinanze conferito all'IFPDT dall'art. 51 LPD è una novità della nuova legge sulla protezione dei dati. Con questo ampliamento dei poteri dell'IFPD, il legislatore risponde ai suggerimenti dei valutatori di Schengen del 2014, che avevano criticato il fatto che, ai sensi della vecchia legge federale sulla protezione dei dati del 1992 (aLPD), l'IFPD poteva solo formulare raccomandazioni. La valutazione Schengen del 2018 ha inoltre raccomandato di rafforzare i poteri esecutivi dell'IFPDT in modo che possa prendere direttamente decisioni giuridicamente vincolanti. L'articolo 51 LPD attua ampiamente l'articolo 47 cpv. 2, della direttiva (UE) 2016/680, specificato nell'articolo 58 cpv. 2, del regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati, GDPR). Allo stesso modo, i requisiti dell'articolo 15 cpv. 2, lett. c del Protocollo di modifica del 18 maggio 2018 alla Convenzione ETS 108 del Consiglio d'Europa sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali sono ampiamente soddisfatti.

2 Per contro, la revisione della LPD si è astenuta dall'ampliare i poteri sanzionatori della LPD al di là della facoltà di emettere ordinanze, nonostante una raccomandazione in tal senso dell'Unione europea e nonostante la corrispondente menzione nell'art. 15 cpv. 2 lett. c del Protocollo di modifica del 18 maggio 2018 alla Convenzione ETS 108. A differenza delle autorità di protezione dei dati di diversi altri Paesi - come le autorità di controllo nel campo di applicazione territoriale del GDPR - l'IFPDT non è quindi ancora in grado di imporre sanzioni amministrative agli organi federali. Anche nel caso dei privati, l'IFPD non ha il potere di imporre sanzioni dirette, ma almeno diverse violazioni dei doveri sono punite nel capitolo 8 della LPD. In particolare, l'IFPDT può imporre una minaccia di pena ai sensi dell'art. 63 LPD sulle sue decisioni di misure amministrative contro privati ai sensi dell'art. 51 LPD. Secondo il legislatore, questo sistema a due livelli è più conforme alla tradizione giuridica svizzera rispetto a una competenza sanzionatoria diretta dell'IFPDT ed è sufficientemente efficace.

3 A differenza del nuovo regime, l'IFPD non aveva la competenza di emettere misure giuridicamente vincolanti ai sensi dell'ALPD. Se nel corso di

un'indagine nei confronti di un organo federale o di una persona privata l'IFPD aveva scoperto una violazione delle norme sulla protezione dei dati, poteva solo raccomandare alla persona responsabile di modificare o di astenersi dal trattamento dei dati (art. 27 cpv. 4 aLPD [per gli organi federali] o art. 29 cpv. 3 aLPD [per le persone private]). Se il responsabile si opponeva alla raccomandazione dell'IFPDT, rifiutandola formalmente o semplicemente non seguendola nei fatti, l'IFPDT doveva presentare la sua raccomandazione al dipartimento o alla Cancelleria federale (nel settore pubblico) o direttamente al Tribunale amministrativo federale (nel settore privato) per ottenere una valutazione giuridicamente vincolante. La decisione emessa dal Dipartimento o dalla Cancelleria federale poteva essere impugnata davanti al Tribunale amministrativo federale dall'organo federale interessato e - dall'introduzione di un corrispondente diritto di ricorso con la revisione della LFPr del 2006 - anche dalla LPD. In ultima istanza, le decisioni del Tribunale amministrativo federale possono essere impugnate davanti al Tribunale federale in materia pubblica e privata (art. 82 lett. a in combinato disposto con l'art. 86 cpv. 1 lett. a LTF). Oltre a questo percorso formale in più fasi attraverso la raccomandazione e il suo eventuale rinvio, l'IFPD poteva conferire forza de facto alle sue ordinanze non vincolanti informando l'Assemblea federale e il Consiglio federale e pubblicandole con un corrispondente effetto reputazionale (art. 30 aLPD).

In pratica, sotto l'ALPD, l'IFPD ha emesso solo poche raccomandazioni, sia nel settore privato che soprattutto in quello pubblico; l'applicazione tramite reclamo è stata ancora più rara. In molti casi, i responsabili avevano già preso le misure necessarie per rimediare alle irregolarità rivelate nel corso della procedura d'indagine, con l'aiuto dei consigli dell'IFPD (art. 28 e art. 31 cpv. 1 lett. aLPD). Se l'IFPDT ha comunque formulato una raccomandazione, questa è stata di solito seguita senza ulteriori indugi. 4

Tuttavia, la mancanza di autorità dell'IFPDT per imporre misure efficaci e, se necessario, sanzioni, è stata e continua a essere criticata nell'insegnamento e nella pratica della protezione dei dati. Anche nel dibattito politico e legislativo sull'ALPD sono state individuate le relative debolezze e si è discusso di un possibile rafforzamento della posizione dell'IFPD. Tuttavia, le opinioni divergono sulla forma concreta che questa posizione più forte dovrebbe assumere e in particolare sulla questione se l'IFPDT debba avere poteri sanzionatori. Ad esempio, nel 2014, un'iniziativa parlamentare che chiedeva 5

l'introduzione di poteri sanzionatori amministrativi per l'FDPIC non ha avuto seguito. L'espansione moderatamente contenuta della posizione della LPD intrapresa con la revisione della FADP riflette l'opinione della politica, della dottrina e della pratica, nonché la pressione dovuta ai requisiti internazionali (cfr. n. 1 f. sopra).

6 La pratica dimostrerà se il nuovo regime, con il potere dell'IFPDT di emettere ordini ma senza poteri sanzionatori diretti, garantisce un'attività di vigilanza efficace. Oltre alla corrispondente ripartizione delle competenze, una vigilanza efficace richiede anche che l'FDPIC sia dotato di risorse adeguate. A questo proposito, in letteratura sono state espresse alcune critiche sulle risorse, considerate troppo scarse e che, nonostante un aumento già avvenuto, probabilmente costringeranno l'FDPIC a procedere secondo il principio di opportunità nelle sue attività di vigilanza anche in futuro. Anche i valutatori Schengen 2018 sono stati critici a questo proposito e hanno raccomandato di assegnare all'FDPIC risorse finanziarie e umane sufficienti per consentirgli di svolgere tutti i suoi compiti nel contesto Schengen.

II. MISURE AMMINISTRATIVE

7 L'art. 51 LPD lascia all'IFPD un ampio margine di manovra: in caso di violazione delle disposizioni in materia di protezione dei dati, l'IFPD può ordinare misure volte a porre rimedio alla situazione illecita, ma non è obbligato a farlo. L'elenco delle misure non è esaustivo. Nel decidere se emettere un ordine e, in caso affermativo, quale, si applica il principio di proporzionalità: devono essere ordinate le misure necessarie a (ri)garantire la legittimità del trattamento dei dati nel caso specifico. Il principio di proporzionalità è anche esplicitamente ancorato nell'art. 51 cpv. 5 LPD: se l'organo federale o la persona privata ha già adottato le misure necessarie durante l'indagine per ripristinare l'osservanza delle disposizioni in materia di protezione dei dati, l'art. 51 cpv. 5 LPD prevede che l'IFPD possa limitarsi a emanare un ammonimento. Inoltre, dato che l'art. 51 LPD è una disposizione facoltativa, nell'interesse di una prassi mirata e adeguata al singolo caso, secondo l'opinione espressa in questa sede, dovrebbe essere possibile per l'IFPD limitarsi, in caso di carenze minori, a consigliare i responsabili su come rimediare alle carenze nell'ambito della sua attività di consulenza (art. 58 cpv. 1 lett. a LPD), invece di emettere un ordine di misure. È prevedibile che, solo per ragioni di efficienza, l'IFPDT si adoperi affinché i responsabili del

trattamento dei dati adottino le misure necessarie per ripristinare la liceità del trattamento dei dati senza essere costretti a emettere un ordine.

Il potere dell'IFPD di emettere un'ingiunzione ai sensi dell'art. 51 LPD è molto ampio in termini di contenuto. È limitato solo, ma almeno, dal fatto che dipende dalla violazione delle disposizioni in materia di protezione dei dati: l'IFPDT non può, ovviamente, ordinare nulla di diverso o di più ampio di quanto sarebbe comunque richiesto dalle disposizioni legali in materia di protezione dei dati. 8

Le misure elencate nell'art. 51 LPD possono essere suddivise in due categorie: I cpv. 1, 2 e 4 prevedono misure contro il trattamento dei dati che viola le disposizioni in materia di protezione dei dati. Il cpv. 3 contiene misure di accompagnamento in caso di violazione di disposizioni normative o di obblighi nei confronti della persona interessata. L'IFPDT può, se necessario, imporre una sanzione per le misure amministrative ordinate contro privati ai sensi dell'art. 63 LPD (cfr. n. 2 sopra). 9

A. Misure contro il trattamento dei dati in violazione delle norme sulla protezione dei dati (art. 51 cpv. 1, 2 e 4 LPD)

La prima categoria di provvedimenti riguarda il trattamento dei dati in violazione delle norme sulla protezione dei dati e mira a ripristinare la conformità alle norme violate. A seconda della costellazione, l'IFPDT può emanare le necessarie ordinanze ai sensi dell'art. 51 cpv. 1, 2 o 4 LPD. 10

A titolo di clausola generale, l'art. 51 cpv. 1 LPD conferisce all'IFPD il potere, in caso di trattamento dei dati che viola le norme sulla protezione dei dati, di ordinare la rettifica, l'interruzione o la cessazione parziale o totale, nonché la cancellazione o la distruzione parziale o totale dei dati personali in questione. 11

L'art. 51 cpv. 2 e cpv. 4 LPD disciplina inoltre separatamente due casi specifici di trattamento dei dati in violazione delle norme sulla protezione dei dati, ossia la divulgazione illecita di dati all'estero e la mancata designazione di una rappresentanza svizzera per gli incaricati del trattamento all'estero ai sensi dell'art. 14 LPD. 12

Se i dati vengono divulgati all'estero in violazione delle norme, l'IFPD può ordinarne la sospensione o il divieto (art. 51 cpv. 2 LPD). Ciò comprende, da un lato, le violazioni degli artt. 16 e 17 LPD, che regolano l'esportazione di dati 13

dalla Svizzera, e, dall'altro, le violazioni delle disposizioni relative alla divulgazione di dati personali all'estero contenute in altre leggi federali. L'inclusione delle violazioni di altre leggi federali è stata lasciata invariata nonostante le relative critiche in sede di consultazione. In pratica, tuttavia, non dovrebbe avere un significato indipendente, poiché tali esportazioni di dati violano regolarmente il principio della liceità del trattamento dei dati (art. 6 cpv. 1 LPD) e potrebbero quindi essere incluse anche nella clausola generale dell'art. 51 cpv. 1 LPD.

14 In caso di violazione dell'art. 14 LPD, l'IFPD può ordinare la designazione di una rappresentanza svizzera da parte dei titolari del trattamento residenti o domiciliati all'estero (art. 51 cpv. 4 LPD).

B. Misure di accompagnamento in caso di violazione delle disposizioni normative o degli obblighi nei confronti degli interessati (art. 51 cpv. 3 LPD)

15 La seconda categoria di misure riguarda i casi di mancato rispetto delle disposizioni normative o degli obblighi nei confronti degli interessati. Non è necessario che si sia verificata una violazione della protezione dei dati. L'art. 51 cpv. 3 LPD contiene un elenco non esaustivo di possibili provvedimenti. Queste vanno lette insieme agli obblighi che la LPD impone agli organi federali e ai privati nel secondo e terzo capitolo.

16 La maggior parte delle misure elencate nell'art. 51 cpv. 3 LPD sono ordini di informazione e consultazione che impongono al responsabile del trattamento di informare o consultare l'IFPDT e/o le persone interessate dal trattamento dei dati in relazione a determinati processi (art. 51 cpv. 3 lett. a, c, e, f e g LPD). In particolare, l'IFPDT può chiedere ai responsabili del trattamento di farlo mediante un'ordinanza,

- di informarlo preventivamente delle clausole o garanzie pertinenti se è prevista la divulgazione di dati all'estero senza un'adeguata protezione ai sensi dell'art. 16 cpv. 1 LPD e la protezione dei dati deve essere assicurata mediante clausole contrattuali di protezione dei dati ai sensi dell'art. 16

cpv. 2 lett. b LPD o mediante garanzie specifiche elaborate dall'organo federale competente (art. 16 cpv. 2 lett. c LPD) (art. 51 cpv. 3 lett. a LPD);

- informarlo, ai sensi dell'art. 17 cpv. 2 LPD, dei casi di divulgazione di dati all'estero che rientrano nelle norme di esenzione di cui all'art. 17 cpv. 1 lett. b n. 2, lett. c e lett. d LPD (art. 51 cpv. 3 lett. a LPD);
- rispettare l'obbligo di informare gli interessati quando ottengono dati personali (art. 19 LPD) e quando prendono decisioni individuali automatizzate (art. 21 LPD) (art. 51 cpv. 3 lett. cpv. LPD);
- consultarlo ai sensi dell'art. 23 LPD nei casi in cui la valutazione d'impatto sulla protezione dei dati effettuata riveli ancora un rischio elevato per la personalità o i diritti fondamentali degli interessati nonostante le misure di protezione previste (art. 51 cpv. 3 lett. e LPD);
- di segnalarle le violazioni della sicurezza dei dati ai sensi dell'art. 24 LPD e, alle condizioni di cui all'art. 24 cpv. 4 e 5 LPD, di informarne gli interessati (art. 51 cpv. 3 lett. f LPD);
- adempiere all'obbligo di fornire informazioni agli interessati ai sensi dell'art. 25 LPD (art. 51 cpv. 3 lett. g LPD).

Le altre misure elencate nelle lettere b e d dell'art. 51 cpv. 3 LPD sono ordini di agire. Di conseguenza, l'IFPDT può chiedere alla parte responsabile, mediante un ordine, di 17

- di adottare le necessarie misure tecniche e organizzative (TOM) per il trattamento dei dati, nel rispetto delle disposizioni sulla protezione dei dati (art. 7 cpv. 1 e 2 LPD) e garantendo un'adeguata sicurezza dei dati ai sensi dell'art. 8 LPD e degli artt. 1 e segg. LPD. LPD (art. 51 cpv. 3 lett. b LPD);
- utilizzare impostazioni predefinite rispettose della protezione dei dati in conformità all'art. 7 cpv. 3 LPD (art. 51 cpv. 3 lett. b LPD);
- effettuare una valutazione dell'impatto sulla protezione dei dati ai sensi dell'art. 22 LPD (art. 51 cpv. 3 lett. d LPD).

III. DIRITTO PROCEDURALE

A. Generalità

18 I provvedimenti sono emessi dall'IFPDT sotto forma di ordinanza: Dal punto di vista procedurale, alle misure amministrative ai sensi dell'art. 51 LPD si applicano le disposizioni della legge sulla procedura amministrativa (art. 52 cpv. 1 LPD). Ai sensi dell'art. 52 cpv. 2 LPD, solo l'organo federale o la persona privata contro cui è stata aperta un'indagine ha lo status di parte. Le persone interessate da un'operazione di trattamento dei dati non sono quindi parti in causa, anche se l'indagine è stata avviata con la loro notifica ai sensi dell'art. 49 cpv. 1 LDP. In linea di principio, l'IFPDT emette le sue decisioni esclusivamente nei confronti dei destinatari. Solo in casi di interesse generale informa il pubblico (art. 57 cpv. 2 LPD). L'IFPDT deve motivare sufficientemente le sue decisioni in modo che le persone responsabili siano in grado di valutare e attuare le misure ordinate o di presentare ricorso contro di esse. In altre parole, il contenuto dell'ordine deve essere in ogni caso un'istruzione concreta per l'azione che può essere eseguita come tale. Ordini generici in cui si afferma che il destinatario dell'ordine deve adeguare il proprio trattamento dei dati in modo da soddisfare i requisiti di protezione dei dati della LPD non sarebbero quindi sufficientemente precisi. Se a seguito di un'indagine non vengono ordinate misure o se viene emesso solo un avvertimento ai sensi dell'art. 51 cpv. 5 LPD, la procedura di indagine deve comunque essere formalmente conclusa dall'IFPDT.

19 Le decisioni dell'IFPD ai sensi dell'art. 51 LPD possono essere impugnate dinanzi al Tribunale amministrativo federale dall'organo federale o dalla persona privata contro cui sono dirette secondo le norme generali dell'amministrazione della giustizia federale (cfr. art. 52 cpv. 1 LPD in combinato disposto con gli artt. 44 e segg. PA). Le decisioni di appello del Tribunale amministrativo federale sono impugnabili in materia di diritto pubblico presso il Tribunale federale (art. 82 lett. a in combinato disposto con l'art. 86 cpv. 1 lett. a LTF). Oltre al destinatario dell'ordinanza, anche l'IFPD ha diritto di ricorso (art. 52 cpv. 3 LPD). In assenza della qualità di parte (cfr. art. 52 cpv. 2 LPD e n. 18 supra), tuttavia, gli interessati non sono legittimati a ricorrere contro le decisioni dell'IFPDT e contro le decisioni di appello.

Per quanto riguarda l'esecuzione delle misure amministrative ordinate, si applicano inoltre gli articoli 39-43 della legge sulla procedura amministrativa, in virtù del riferimento di cui all'art. 52 cpv. 1 LPD. 20

A differenza di quanto previsto dall'aLPD, in base al quale non poteva essere richiesto alcun emolumento alla persona responsabile dell'emanazione di una raccomandazione (cfr. art. 33 aLPD), l'art. 59 cpv. 1 lett. d LPD prevede ora che possa essere richiesto un emolumento a persone private per l'emanazione di provvedimenti ai sensi dell'art. 51 LPD (cfr. anche art. 44 LPD). Per le ordinanze contro gli organi federali, in assenza di una base giuridica corrispondente, non si continua a riscuotere alcuna tassa (art. 59 cpv. 1 lett. d LPD e contrario; cfr. Messaggio 2017, pag. 7098). 21

B. Misure cautelari

Nella LPD 2017 era previsto che un paragrafo dell'articolo relativo alla procedura d'indagine autorizzasse esplicitamente l'IFPD a ordinare misure cautelari per la durata dell'indagine e a farle eseguire da un'autorità federale o dagli organi di polizia cantonali o comunali (art. 44 cpv. 2 LPD [2017]). Tuttavia, dopo che il Parlamento ha eliminato questo paragrafo dall'art. 50 LDP, la versione finale dell'art. 44 DST, la LPD non conferisce più direttamente all'IFPDT il potere di emettere ordinanze cautelari per la durata delle sue indagini. Ora la competenza dell'IFPD di emettere misure cautelari deriva solo indirettamente dall'articolo sulle tasse, che all'art. 59 cpv. 1 lett. d LPD dichiara che l'emissione di misure cautelari da parte dell'IFPD nei confronti di persone private è soggetta a una tassa. Tuttavia, come già accadeva sotto l'ALPD, l'emanazione di misure cautelari o addirittura superprovvisorie nell'ambito di indagini sulla protezione dei dati deve essere possibile in ogni caso; la soppressione della disposizione in questione deve essere interpretata come una svista legislativa e non come un silenzio qualificato. 22

Mentre nella vecchia legge l'IFPDT doveva ricorrere al Tribunale amministrativo federale (art. 33 cpv. 2 aLPD) per l'emanazione di provvedimenti provvisori a causa dell'assenza di una propria competenza a emettere ordini, ora può emetterli autonomamente. 23

Tuttavia, l'art. 33 cpv. 2 aLPD, che non è più applicabile con la nuova legge, non solo attribuiva al Tribunale amministrativo federale la competenza a 24

emettere misure cautelari nell'ambito di indagini sulla protezione dei dati, ma ne disciplinava anche i requisiti e la procedura. Nel primo contesto, l'art. 33 cpv. 2 aDSG richiedeva che le persone interessate fossero minacciate da un danno non facilmente rimediabile. In termini di procedura, la disposizione dichiarava applicabili, mutatis mutandis, gli artt. 79-84 BZP.

25 Dopo l'omissione dell'art. 33 cpv. 2 dell'ALPD, non esistono più regole procedurali e prerequisiti espliciti per la tutela legale provvisoria. Di conseguenza, la valutazione sostanziale delle misure provvisorie nelle indagini sulla protezione dei dati non dovrebbe cambiare di molto. La legge sulla procedura amministrativa (PA), applicabile al procedimento di indagine ai sensi dell'art. 52 cpv. 1 LPD, contiene solo disposizioni sull'emissione di misure cautelari nel procedimento di appello (cfr. in particolare gli artt. 55 e 56 PA), ma non nel procedimento amministrativo a monte. Tuttavia, l'ammissibilità delle misure cautelari nei procedimenti amministrativi è riconosciuta, in quanto deriva direttamente dall'esigenza di applicare il diritto sostanziale. Affinché l'IFPDT possa emettere misure cautelari nei procedimenti d'indagine, si deve innanzitutto presumere che sia previsto uno svantaggio non facilmente rimediabile. Contrariamente a quanto previsto dall'ALPD, questo non deve necessariamente minacciare le persone interessate dal trattamento dei dati, anche se in pratica è probabile che venga regolarmente attribuito loro. Inoltre, l'ordine immediato deve essere urgente e deve apparire adeguato, necessario e proporzionato in base alle circostanze complessive, al fine di tutelare interessi pubblici o privati prevalenti. In quanto ordinanze provvisorie, le misure provvisorie non possono pregiudicare né rendere impossibile la situazione che si intende regolare. Nel momento in cui si discutono le ordinanze provvisorie, l'esito dell'indagine sulla protezione dei dati è solitamente ancora incerto e si può procedere solo a un esame sommario della situazione di fatto e di diritto. Di conseguenza, nel corso dell'esame delle misure cautelari deve essere formulata una prognosi sul caso principale, ma ciò ostacola un'ordinanza provvisoria solo se è chiaramente negativa.

26 Per quanto riguarda il contenuto, è probabile che le ordinanze si basino sul catalogo delle misure amministrative di cui all'art. 51 LPD. Spesso si tratterà di utilizzare le ordinanze provvisorie per vietare il trattamento dei dati potenzialmente in violazione della protezione dei dati per la durata del procedimento, al fine di evitare ulteriori danni che potrebbero derivare dalla

continuazione immutata del trattamento in questione durante un'indagine talvolta complessa e lunga.

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 52 LPD

Un commentario di Nicolas Winkelmann

CITAZIONE SUGGERITA

Nicolas Winkelmann, Commentario all'art. 52 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Winkelmann, art. 52 LPD N. XXX.

Art. 52 Procedura

[1] La procedura d'inchiesta e le decisioni di cui agli articoli 50 e 51 sono rette dalla PA.

[2] È parte soltanto l'organo federale o il privato oggetto dell'inchiesta.

[3] L'IFPDT può impugnare le decisioni su ricorso pronunciate dal Tribunale amministrativo federale.

STRUTTURA

In breve 655
I. Indicazioni generali sulla procedura 655
II. Rinvio alla PA (cpv. 1) 657
A. Procedimento secondo la PA contro privati 657
B. Procedura secondo la PA contro organi federali 657
C. Delimitazioni 660
1. Sulla «indagine preliminare informale» 660
2. L'«intervento a bassa soglia» 661
3. La campagna 662
4. Informazione del pubblico in merito alle constatazioni e alle decisioni 663
5. Consulenza 664
D. Disposizioni speciali rispetto alla PA 664
III. Parti della procedura (cpv. 2) 665
A. Panoramica 665
B. Privati come parti 665
C. Organi federali come parti 667
IV. Legittimazione ad adire l'IFPDT (cpv. 3) 667
Bibliografia 668
I materiali 669

IN BREVE

L'art. 52 cpv. 1 LPD stabilisce le regole secondo le quali l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) conduce le procedure formali. La disposizione è una norma di rinvio e stabilisce che le indagini ai sensi dell'art. 49 LPD e le decisioni ai sensi degli art. 50 e 51 LPD sono regolate dalle norme della PA. E contrario, gli altri atti dell'IFPDT non sono soggetti alla PA, in particolare gli accertamenti preliminari informali, gli interventi a bassa soglia o le attività di consulenza e di sorveglianza. È degno di nota il fatto che anche per le procedure contro organi federali si rimanda alla PA e che l'IFPDT può «decidere» contro organi federali secondo le norme della PA. 1

Capovers. 2 stabilisce che solo l'organo federale o la persona privata contro cui è stata avviata un'indagine hanno la qualità di parte. Ciò restringe la cerchia delle parti possibili nelle procedure formali dell'IFPDT rispetto alle disposizioni della PA. 2

Capovers. 3 costituisce la base legale che conferisce all'IFPDT il diritto di ricorso al Tribunale federale contro le decisioni del Tribunale amministrativo federale. 3

I. INDICAZIONI GENERALI SULLA PROCEDURA

In base alla aDSG, dal 1993 al 2023 l'IFPDT ha condotto cosiddette accertamenti di fatto, che ha concluso con una relazione finale e raccomandazioni. A causa della mancanza di competenza decisionale dell'IFPDT, la PA non era applicabile a queste procedure. Se una **raccomandazione del preposuto** non veniva seguita o veniva respinta, l'IFPDT poteva sottoporre la questione al Tribunale amministrativo federale per una decisione. 4

Con la revisione totale della LPD, entrata in vigore il 1° settembre 2023, l'IFPDT ha ottenuto una competenza decisionale, motivo per cui, dall'entrata in vigore della LPD riveduta, conclude una procedura formale con una decisione. In occasione della Giornata internazionale della protezione dei dati, nel gennaio 2025 l'IFPDT ha pubblicato per la prima volta un bilancio intermedio in cifre. Secondo tale bilancio, dal 1° settembre 2024 al 21 gennaio 5

2025 l'IFPDT ha ricevuto complessivamente 1'406 segnalazioni di violazioni della LPD, di cui 479 erano in corso di trattamento al momento della pubblicazione. Gli **atti di vigilanza** si sono ripartiti come segue:

- Interventi di base: 116
- Di questi, seguiti volontariamente dai responsabili: circa il 90%
- Indagini preliminari: 16
- Indagini in corso / pendenti dinanzi al TAF: 8 / 2
- Campagne 2

6 I dati pubblicati mostrano che gli atti di vigilanza dell'IFPDT portano solo in casi isolati all'apertura di un'indagine formale e che l'**intervento a bassa intensità costituisce lo strumento principale della vigilanza**. In pratica, dopo aver ricevuto una denuncia, l'IFPDT interviene quindi di norma senza aprire un'indagine formale.

7 I presupposti per l'**apertura di un'indagine** sono stabiliti all'art. 49 cpv. 1 LPD. Secondo tale disposizione, l'IFPDT avvia d'ufficio o su denuncia un'indagine se sussistono indizi sufficienti che un trattamento di dati possa violare le disposizioni sulla protezione dei dati. Non appena l'IFPDT avvia un'indagine ai sensi dell'art. 49 LPD, è applicabile la PA. Ciò avviene non appena ha deciso internamente di avviare una procedura. Ciò può avvenire già prima di un intervento informale dell'IFPDT, durante o dopo.

8 Di prassi, l'avvio della procedura viene comunicato alla parte mediante una **lettera di apertura**. L'avvio della procedura non costituisce una decisione impugnabile. La procedura si conclude infine con una decisione ai sensi dell'articolo 51 LPD o viene archiviata.

9 Dal punto di vista del responsabile del trattamento, è importante sapere se è stata avviata o meno una procedura. Dopo l'avvio della procedura, le parti sono soggette all'**obbligo di collaborazione** (art. 60 cpv. 2 LPD), punibile con sanzioni penali. E contrario, la collaborazione prima dell'avvio di un'indagine non è obbligatoria. In caso di rifiuto o di collaborazione insufficiente dei responsabili nell'ambito di un'indagine preliminare o di un intervento a bassa soglia, sono tuttavia regolarmente soddisfatti i requisiti di cui all'art. 49 cpv. 1 LPD, cosicché i fatti possono essere accertati in base all'obbligo di collaborazione (art. 49 cpv. 3 LPD) o con l'ausilio di mezzi

coercitivi (art. 50 cpv. 1 LPD). Per tali atti l'IFPDT può esigere il pagamento di emolumenti (art. 59 cpv. 1 lett. d LPD), motivo per cui è regolarmente nell'interesse del responsabile cooperare volontariamente con l'IFPDT prima dell'apertura di un'indagine.

Il principio del **diritto di essere sentiti**, sancito dall'art. 29 cpv. 2 Cost. e concretizzato dagli art. 29 segg. PA, garantisce alle parti un diritto di partecipazione alla procedura che riguarda la loro personalità. Esse devono poter esprimere il proprio parere sulla questione prima che sia emanata la decisione, fornire prove rilevanti, collaborare all'assunzione delle prove o almeno esprimersi sul risultato delle prove. In altre parole, la parte interessata deve avere la possibilità di prendere posizione sui punti essenziali prima che sia presa una decisione. Ciò comprende in primo luogo i fatti rilevanti previsti. Di conseguenza, prima dell'emanazione di una decisione, le parti possono pronunciarsi solo sui fatti previsti; non è invece compreso nel diritto di essere sentiti il diritto di conoscere la valutazione giuridica prevista. Solo in casi eccezionali – ad esempio quando l'IFPDT prevede di applicare disposizioni speciali inaspettate – il diritto di essere sentiti può comprendere anche le disposizioni applicabili previste e la motivazione giuridica prevista. La valutazione giuridica dell'IFPDT viene comunicata alle parti nella decisione motivata. Se una parte non è d'accordo con la motivazione giuridica dell'IFPDT, può presentare ricorso. 10

II. RINVIO ALLA PA (CPV. 1)

A. Procedimento secondo la PA contro privati

La PA si applica, in base all'art. 1 cpv. 1 e cpv. 2 lett. c PA, alle procedure dell'IFPDT in cui quest'ultimo emette una decisione in prima istanza. Non sussiste un'eccezione ai sensi dell'art. 2 segg. PA. L'art. 52 cpv. 1 LPD costituisce quindi una **norma di rinvio dichiarativa** nei confronti dei privati e serve a fini di chiarimento. 11

B. Procedura secondo la PA contro organi federali

Prima della revisione totale della LPD, la sorveglianza sugli organi federali e sui privati era disciplinata in due disposizioni separate, che differivano in particolare per quanto riguarda i presupposti per l'apertura di un'indagine. Nella LPD riveduta, l'indagine sulle violazioni delle norme sulla protezione 12

dei dati è ora disciplinata in un'unica sezione (art. 49 segg.) per gli organi federali e i privati. È da notare che, salvo piccole eccezioni, non sono state legiferate **norme diverse per i procedimenti contro organi federali o privati**.

13 Secondo la giurisprudenza e la dottrina costanti, sono considerate decisioni ai sensi dell'articolo 5 PA le disposizioni autorevoli, unilaterali, individuali e concrete di un'autorità, emanate in applicazione del diritto amministrativo, volte a produrre effetti giuridici, vincolanti e esecutive. La procedura per l'adozione di una decisione presuppone un rapporto di sovranità tra un'autorità e un privato. Le disposizioni dell'IFPDT nei confronti di altri organi federali non soddisfano quindi tutte le caratteristiche strutturali del concetto di decisione, data l'assenza di un rapporto tra autorità e privato. Pertanto, quando l'IFPDT conduce una procedura contro un organo federale, la procedura «si basa» sull'art. 49 LPD in combinato disposto con la PA, per cui in questo ambito l'art. 52 cpv. 1 LPD corrisponde a una **norma di rinvio costitutiva** e le disposizioni della PA si applicano *per analogia*.

14 La **competenza decisionale dell'IFPDT nei confronti degli organi federali** deriva, da un lato, dal testo di numerose disposizioni legislative che si riferiscono espressamente agli organi federali e ai privati e operano una distinzione significativa tra organi federali e privati. D'altro canto, il legislatore ha volutamente uniformato le procedure nei confronti dei privati e degli organi federali, che secondo il diritto precedente erano ancora diverse. Infine, il legislatore ha adeguato i poteri d'indagine e le misure amministrative alle disposizioni europee, al fine di garantire che la Commissione europea rinnovi o mantenga la decisione di adeguatezza nei confronti della Svizzera, il che è di fondamentale importanza soprattutto per l'economia svizzera.

15 Oltre all'IFPDT, non è individuabile nessun'altra unità amministrativa che possa disporre nei confronti di altre unità amministrative secondo le norme della PA. Il **Controllo federale delle finanze**, in quanto autorità di vigilanza comparabile, può sì richiedere e far eseguire misure nei confronti di altre autorità federali che non sono gerarchicamente subordinate ad esso, ma non secondo le norme della PA.

16 Secondo il parere qui espresso, un'ordinanza dell'IFPDT ai sensi dell'articolo 51 LPD nei confronti di organi federali corrisponde a una «**finta decisione**», poiché da un lato non sono soddisfatti i requisiti materiali di una decisione ai

sensi dell'articolo 5 PA, ma dall'altro lato agli organi federali sono imposti *per analogia* gli stessi diritti e doveri dei destinatari privati di una decisione. Con la norma di rinvio costitutiva, il legislatore ha disciplinato in modo pragmatico le norme procedurali che l'IFPDT, in qualità di autorità di sorveglianza, deve seguire per condurre un'indagine nei confronti degli organi federali e per emanare e far rispettare ordinanze vincolanti.

È degno di nota il fatto che nel **progetto di revisione della legge sulla protezione dei dati** del 2014 si faceva ancora una distinzione tra inchieste nei confronti di privati e organi federali. In esso veniva proposto un modello secondo cui l'IFPDT avrebbe dovuto prima formulare una raccomandazione agli organi federali e solo dopo il suo rifiuto o la sua inosservanza avrebbe potuto emanare una decisione. Questa variante ritarda la procedura con passaggi intermedi inutili. Già nel rapporto esplicativo relativo al progetto preliminare di revisione totale della LPD del 2016 non si fa più distinzione tra procedure contro privati o organi federali. 17

Le procedure dell'IFPDT ai sensi dell'articolo 49 LPD contro organi federali devono essere distinte dall'**assistenza amministrativa**. Le autorità federali che collaborano nell'ambito dell'assistenza amministrativa sono organicamente equivalenti, motivo per cui non sussiste alcun rapporto di subordinazione tra loro e la collaborazione avviene su base paritaria. Se l'IFPDT avvia una procedura contro un organo federale in base all'articolo 49 LPD e richiede documenti all'organo federale oggetto dell'indagine, ciò non rientra nell'assistenza amministrativa, motivo per cui l'articolo 36a LTF non è applicabile. Nell'ambito di una procedura, le autorità federali oggetto di indagine sono soggette all'obbligo di collaborare, il che in tali casi crea un rapporto di subordinazione, poiché solo in questo modo l'IFPDT può controllare e garantire efficacemente il rispetto delle norme sulla protezione dei dati da parte delle autorità federali. 18

L'applicazione analogica delle disposizioni della PA alle procedure contro organi federali comporta in particolare le seguenti differenze rispetto alle procedure nei confronti dei privati: 19

La **violazione dell'obbligo di collaborazione** non è punibile per gli organi federali secondo il testo dell'art. 60 cpv. 2 LPD, che si rivolge espressamente solo ai privati. Questa esclusione è sensata, poiché un'applicazione agli organi federali sarebbe del tutto contraria al sistema. 20

21 L'IFPDT non può esigere **tasse** dagli organi federali, in particolare per l'ordinanza di misure provvisorie e di misure ai sensi dell'art. 51 LPD. Secondo il testo dell'art. 59 cpv. 1 LPD, l'esazione di tasse è riservata esclusivamente ai privati. Anche questa esclusione è coerente, poiché l'esazione di tasse dagli organi federali sarebbe anch'essa contraria al sistema.

22 Secondo il testo della legge, l'IFPDT può anche ricorrere ad altre autorità federali nonché ad organi di polizia cantonali o comunali per poter eseguire o far eseguire le disposizioni di cui all'art. 50 cpv. 1 LPD. Poiché le autorità federali godono dei diritti previsti dalla LPD e dalla PA e l'IFPDT può informare il pubblico in merito alla constatazione di un'inosservanza da parte di un organo federale ai sensi dell'art. 57 cpv. 2 LPD, questa possibilità troverà probabilmente applicazione solo in situazioni eccezionali. Per quanto riguarda l'**uso di mezzi coercitivi** ai sensi dell'art. 50 cpv. 3 LPD, non vi è quindi alcuna differenza rispetto ai privati, per cui, secondo il parere qui espresso, l'IFPDT può ricorrere a mezzi coercitivi anche nei confronti degli organi federali.

23 Per quanto riguarda la **legittimazione ad agire** degli organi federali, si vedano le considerazioni relative al cpv. 2.

C. Delimitazioni

1. Sulla «indagine preliminare informale»

24 Prima di avviare un'indagine ai sensi dell'articolo 49 LPD e di applicare le disposizioni della PA, l'IFPDT interviene spesso in via informale. Il punto di partenza è di norma una denuncia o una segnalazione dei media, che però **non contengono sufficienti indizi** per l'avvio diretto di un'indagine. Pertanto, l'IFPDT può verificare in una prima fase se sussistono indizi sufficienti per l'apertura di un'indagine. A tal fine può avvalersi di tutte le fonti di informazione possibili e, ad esempio, esaminare fonti pubbliche o interrogare il responsabile, le persone interessate o terzi in merito ai fatti. La fase dell'indagine preliminare è classificata come «atto amministrativo informale», nel quale l'IFPDT deve attenersi ai principi dello Stato di diritto (cfr. art. 5 Cost.) e non può agire in modo arbitrario o in violazione del principio di uguaglianza. Durante l'accertamento preliminare informale, il responsabile non è soggetto ad alcun obbligo di collaborazione e la norma penale di cui all'art. 60 cpv. 2 LPD non trova applicazione – tali disposizioni

sono applicabili solo dopo l'apertura di un'indagine formale ai sensi dell'art. 49 LPD.

L'inchiesta preliminare informale può portare alla confutazione degli indizi di una presunta violazione della protezione dei dati, rendendo superfluo un ulteriore intervento dell'IFPDT. Ciò accade regolarmente, ad esempio quando i fatti sono stati riportati in modo impreciso nella denuncia. In alternativa, può essere avviato un intervento a bassa soglia o un'indagine. 25

2. L'«intervento a bassa soglia»

L'accertamento preliminare informale va distinto dallo strumento dell'«intervento a bassa soglia». Il termine «intervento a bassa soglia» non figura nella legge, ma è stato coniato dall'IFPDT. Mentre l'accertamento informale mira a stabilire i fatti per valutare se sussistono indizi sufficienti per l'apertura di un'indagine ai sensi dell'articolo 49 LPD, l'intervento a bassa soglia persegue uno scopo diverso. Con l'intervento a bassa soglia si cerca di ripristinare la **situazione giuridicamente corretta mediante misure di economia amministrativa**, come una semplice lettera, in modo che il responsabile adotti volontariamente le misure necessarie. Tuttavia, come nel caso dell'accertamento informale, non viene avviata un'indagine ai sensi dell'articolo 49 LPD, per cui anche l'intervento a bassa soglia è da qualificarsi come atto amministrativo informale e non si applicano le disposizioni della PA. Secondo l'esperienza dell'IFPDT, in molti casi gli adeguamenti necessari verrebbero così attuati in tempo utile. In linea di principio si mira così a una procedura orientata alla soluzione e che risparmi risorse. 26

Ad esempio, l'IFPDT può essere informato tramite una segnalazione che un responsabile non ha risposto a una richiesta di informazioni presentata dalla persona segnalante. Sulla base di una o più segnalazioni di questo tipo, l'IFPDT può contattare il responsabile del trattamento e invitarlo a trattare la richiesta di informazioni concreta della persona segnalante e a fornire una presa di posizione sul modo in cui vengono trattate in generale le richieste di informazioni. Se dalla risposta del responsabile si può dedurre che in futuro le richieste di informazioni saranno trattate correttamente ed entro i termini previsti dalla legge, non è necessario avviare un'indagine. 27

Se l'intervento a bassa intensità non porta al rispetto della protezione dei dati, di norma sussistono indizi sufficienti per avviare un'indagine formale. Ciò vale 28

ad esempio quando, dopo un intervento a bassa soglia, l'IFPDT riceve nuovamente segnalazioni relative allo stesso caso. Indipendentemente da un eventuale intervento al di fuori di un'indagine, l'IFPDT può avviare un'indagine non appena sussistono indizi sufficienti.

3. La campagna

29 Oltre a svolgere inchieste ai sensi dell'articolo 49 LPD, l'IFPDT esercita anche attività di sorveglianza in base all'articolo 4 cpv. 1 in combinato disposto con l'articolo 57 cpv. 1 lett. a, c e g LPD. L'IFPDT definisce tali attività «campagne». Dal punto di vista dei responsabili, le **indagini sono condotte in base a casi specifici**, mentre i contatti da parte dell'autorità di protezione dei dati possono avvenire **nell'ambito di campagne senza un motivo specifico**. Nell'ambito delle campagne, l'IFPDT non interviene sulla base di segnalazioni relative a una violazione concreta della protezione dei dati da parte di un responsabile specifico, ma perché in un settore della protezione dei dati sono stati riscontrati ripetutamente problemi identici o simili. Al fine di garantire un controllo e un'applicazione efficaci delle norme sulla protezione dei dati, l'IFPDT può rivolgersi contemporaneamente a più responsabili, segnalare i problemi generali riscontrati in un determinato settore e ricordare i requisiti applicabili. È anche possibile annunciare future attività di vigilanza in un determinato settore.

30 L'IFPDT non ha ancora avviato alcuna campagna. Uno sguardo alla Germania mostra come potrebbe essere una campagna di questo tipo: nell'ambito della sua attività di vigilanza, l'Ufficio bavarese per la protezione dei dati (BayLDA) effettua diversi controlli mirati sulla protezione dei dati, ovvero controlli senza motivo specifico che hanno un focus particolare. Ad esempio, sono state verificate le norme in materia di protezione dei dati applicabili alle candidature di potenziali inquilini. A tal fine, sono stati **selezionati casualmente** alcuni responsabili e controllati in modo mirato per quanto riguarda i requisiti di protezione dei dati nella ricerca di inquilini, chiedendo loro di rispondere a un questionario entro un termine legale. L'intervento si basa in particolare sull'art. 58 cpv. 1 lett. a RGPD, secondo cui devono essere fornite tutte le informazioni necessarie per l'adempimento dei compiti legali.

31 L'attività di vigilanza del BayLDA descritta al punto precedente può essere qualificata, a seconda della sua configurazione concreta, come **chiarimento**

preliminare informale o intervento a bassa soglia, che tuttavia si rivolge **contemporaneamente a più responsabili** in un determinato settore.

A differenza delle autorità europee di protezione dei dati, che in base all'art. 58 cpv. 1 lett. a RGPD possono richiedere tutte le informazioni necessarie all'adempimento dei *compiti legali*, l'IFPDT può, in base all'art. 50 cpv. 1 lett. a LPD, solo l'accesso a tutte le informazioni, ai documenti, agli elenchi delle attività di trattamento e ai dati personali, nella misura in cui sono necessari per l'*indagine*. Sebbene l'art. 50 LPD debba soddisfare i requisiti europei, la suddetta **disposizione della LPD è stata limitata rispetto alle disposizioni europee**. Nell'ambito delle attività di sorveglianza dell'IFPDT, i responsabili del trattamento non sono soggetti all'obbligo di collaborazione sancito dall'art. 60 cpv. 2 in combinato disposto con l'art. 49 cpv. 3 LPD e non sono tenuti al pagamento di emolumenti (art. 59 cpv. 1 LPD e contrario). 32

4. Informazione del pubblico in merito alle constatazioni e alle decisioni

Ai sensi dell'art. 57 cpv. 2 LPD, l'IFPDT informa il pubblico delle sue constatazioni e delle sue decisioni nei casi di interesse generale. Poiché la procedura amministrativa si conclude con la notifica della decisione, le disposizioni della PA non sono più applicabili in base all'art. 52 cpv. 1 LPD. La **pubblicazione** ufficiale di una **decisione** rientra nell'attività amministrativa effettiva e non è quindi impugnabile in quanto **atto reale**. Se l'IFPDT e la parte non sono d'accordo sulla forma o sul tipo di pubblicazione e se la parte è lesa nei suoi interessi meritevoli di tutela, deve essere emanata una decisione impugnabile in applicazione dell'art. 25a PA. Questa decisione di pubblicazione costituisce quindi una decisione ai sensi dell'art. 5 cpv. 1 lett. c PA, che obbliga la parte a tollerare la pubblicazione nella misura disposta. 33

Una parte è lesa nei suoi **interessi meritevoli di tutela** se fa valere **segreti d'ufficio** o **segreti commerciali** che, secondo la valutazione dell'IFPDT, non costituiscono tali segreti e non devono quindi essere resi anonimi o pubblicati. A tal proposito occorre fare riferimento alla definizione di cui all'art. 7 cpv. 1 lett. g LTras. 34

Per la **divulgazione di dati personali o di dati di persone giuridiche** devono essere soddisfatti i presupposti legali corrispondenti. 35

5. Consulenza

36 Nella pratica, la distinzione tra una consulenza soggetta a tassa ai sensi dell'art. 59 cpv. 1 lett. e LPD e l'accertamento informale o l'intervento a bassa soglia può dare adito a incertezze. Se l'IFPDT, ad esempio in un'indagine preliminare informale o nell'ambito di un intervento a bassa intensità, comunica al responsabile quali misure devono essere adottate affinché si possa escludere una violazione della protezione dei dati o si possa rinunciare all'apertura di un'indagine, tali indicazioni possono essere qualificate come attività di consulenza gratuita. Dal punto di vista politico-giuridico, tale procedura diventa discutibile al più tardi quando i responsabili, dopo che sono state rese note delle violazioni della protezione dei dati, vengono contattati dall'IFPDT e ricevono consigli su come correggere la situazione in modo conforme alla protezione dei dati e quando la situazione conforme alla protezione dei dati viene poi volontariamente attuata in tempo utile, cosicché l'IFPDT rinuncia all'apertura di un'indagine. Invece di una sanzione, ad esempio sotto forma di multa, i responsabili, dopo che è stata resa nota una violazione della protezione dei dati, hanno ricevuto una consulenza giuridica gratuita. D'altra parte, ciò corrisponde esattamente allo scopo di un intervento a bassa soglia, motivo per cui questa procedura deve essere limitata alle violazioni di minore importanza ai sensi dell'art. 49 cpv. 2 LPD.

D. Disposizioni speciali rispetto alla PA

37 Rispetto alla PA, la LPD contiene **disposizioni speciali** che, in quanto lex specialis, prevalgono sulla PA. Le disposizioni più importanti sono le seguenti:

- Limitazione delle parti (art. 52 cpv. 2 LPD)
- Informazione alla persona che ha presentato la denuncia (art. 49 cpv. 4 LPD)
- Obblighi di collaborazione (art. 49 cpv. 3 LPD)
- Assunzione delle prove (art. 50 cpv. 1 LPD)
- Assunzione coattiva delle prove (art. 50 cpv. 3 LPD)
- Informazione al pubblico (art. 57 cpv. 2 LPD)

Le disposizioni speciali della LPD tengono conto della **posizione particolare dell'IFPDT** in qualità di autorità di sorveglianza, motivo per cui gli obblighi di collaborazione e le possibilità di prova vanno oltre quelli previsti dalla PA. Da

questi vanno distinti i diritti di collaborazione, che sono disciplinati dalle disposizioni generali della PA.

III. PARTI DELLA PROCEDURA (CPV. 2)

A. Panoramica

Ai sensi dell'art. 52 cpv. 2 LPD, è parte solo l'organo federale o la persona privata contro cui è stata avviata un'indagine. La posizione delle parti è quindi disciplinata dall'art. 52 cpv. 2 LPD e non dall'art. 6 PA. Mentre secondo la normativa PA, oltre al destinatario della decisione, possono essere parti anche organizzazioni private, associazioni e autorità o terzi interessati dall'atto amministrativo, la **qualità di parte** nella procedura d'indagine dell'IFPDT è **limitata** all'organo federale o alla persona privata contro cui è stata avviata l'indagine. 38

Una procedura può essere condotta contro **più parti**, in particolare se i fatti oggetto dell'indagine riguardano più parti. Se più parti sono coinvolte in un trattamento, l'informazione di una parte nell'ambito della procedura può influire negativamente sui fatti dell'altra parte. Affinché in tali casi sia garantito il diritto di essere sentiti, è necessario un accorpamento dei procedimenti. Tali casi si verificano ad esempio quando il trattamento è effettuato da un incaricato per conto di un responsabile. 39

B. Privati come parti

È parte solo la persona privata contro la quale è stata avviata un'indagine. La qualità di parte è quindi limitata al destinatario materiale della disposizione. La **persona interessata**, anche se l'IFPDT ha avviato l'indagine su sua denuncia, non è parte della procedura. Sono considerate persone private sia le persone fisiche che le persone giuridiche di diritto privato. 40

Può essere parte di una procedura qualsiasi persona privata che presenti indizi sufficienti di una violazione delle norme sulla protezione dei dati. Non appena l'IFPDT avvia una procedura, può infatti ordinare misure amministrative in base all'articolo 51 LPD, che incidono sui diritti e sugli obblighi della parte e soddisfano i requisiti di cui all'articolo 49 LPD e all'articolo 6 PA. Per avviare una procedura contro una persona privata, non è **necessario alcun trattamento dei dati** da parte di quest'ultima. Ciò risulta 41

dalle misure amministrative esemplificative di cui all'art. 51 LPD, secondo cui possono essere disposte anche le misure di cui all'art. 7 LPD o una valutazione dell'impatto sulla protezione dei dati prima che abbia luogo un trattamento dei dati. Ciò è possibile, ad esempio, sulla base di denunce o nell'ambito di progetti legislativi, oppure se l'IFPDT viene a conoscenza di grandi progetti attraverso i media.

42 Oltre al responsabile ai sensi dell'articolo 5 lettera j LPD, possono quindi essere parti in una procedura anche **gli incaricati del trattamento** ai sensi dell'articolo 5 lettera k LPD, un **consulente in materia di protezione dei dati** ai sensi dell'articolo 10 LPD e la **rappresentanza** ai sensi dell'art. 14 LPD possono essere considerati parti di una procedura, nella misura in cui l'oggetto dell'indagine comporti una violazione delle norme sulla protezione dei dati da parte della persona privata oggetto dell'indagine.

43 La questione della **legittimazione passiva** di una parte si pone in particolare nel caso di **gruppi internazionali**, poiché come responsabile viene regolarmente indicata una persona giuridica con sede in Irlanda. Ad esempio, nelle direttive sulla protezione dei dati di Instagram, Facebook e Threads, Meta Platforms Ireland Ltd (MPIL) è indicata come responsabile. MPIL ha anche designato una rappresentanza in Svizzera e dispone inoltre di una succursale in Svizzera (Facebook Switzerland GmbH). In linea di principio, tutte e tre le entità menzionate possono essere considerate parti. Secondo il parere qui espresso, tutte e tre le entità menzionate possono essere parti di un procedimento, a condizione che l'oggetto dell'indagine rientri nell'ambito delle rispettive responsabilità.

44 Ad esempio, è possibile avviare un procedimento contro la filiale Meta in Svizzera. Anche se si sostiene che la filiale svizzera non ha nulla a che fare con il trattamento in questione, poiché opera solo come laboratorio di ricerca per l'intero gruppo, che i diritti di proprietà intellettuale sono di proprietà di un altro ente e che le richieste di cancellazione vengono evase da quest'ultimo, è comunque possibile avviare un procedimento contro la filiale in Svizzera. Secondo il parere qui espresso, una sede in Svizzera costituisce sempre un collegamento con il resto del gruppo internazionale ed è responsabile del rispetto delle norme svizzere, quindi anche della LPD. Anche se la sede svizzera non fosse legittimata dal punto di vista organizzativo ad adeguare il trattamento dei dati in questione, l'IFPDT può almeno constatare la violazione e obbligare la succursale, mediante decisione, a far adeguare il

trattamento in questione alle norme sulla protezione dei dati per le persone interessate in Svizzera tramite l'organo competente all'interno del gruppo. I gruppi internazionali non devono poter eludere gli obblighi svizzeri in materia di protezione dei dati attraverso la loro organizzazione interna.

C. Organi federali come parti

45 Anche un organo federale può essere parte in una procedura in materia di protezione dei dati. Ai sensi dell'articolo 5 lettera i LPD, un organo federale è un'autorità o un servizio della Confederazione o una persona incaricata di compiti pubblici. Il **concetto di organo federale** corrisponde alla definizione di cui all'articolo 3 lettera h aDSG. Sono considerati organi federali i dipartimenti e gli uffici federali, nonché i loro servizi e sezioni. Ne fanno parte anche gli istituti e le aziende federali e i comandi militari. Sono considerati organi federali anche tutte le persone fisiche e giuridiche che trattano dati per conto della Confederazione nell'adempimento di compiti di diritto pubblico. Gli organi dei Cantoni e dei Comuni non sono invece considerati organi federali, anche se svolgono compiti federali.

46 Nei procedimenti non disciplinati dall'articolo 49 LPD, le autorità o gli organi federali non hanno la qualità di parte ai sensi dell'articolo 6 PA nei procedimenti contro privati, in virtù del rapporto di sovranità nei confronti dei privati, ma hanno poteri analoghi e sono designati come «autorità precedente» nella procedura di ricorso. Se l'IFPDT avvia una procedura ai sensi dell'articolo 49 LPD contro un organo federale, quest'ultimo ha, in virtù della norma di rinvio costitutiva, lo stesso status e gli stessi poteri dei privati in quanto destinatario materiale della decisione. Di conseguenza, l'organo federale contro cui è stata avviata una procedura è parte nel **procedimento di ricorso** e l'IFPDT è l'autorità precedente.

IV. LEGITTIMAZIONE AD ADIRE L'IFPDT (CPV. 3)

47 Le decisioni dell'IFPDT sono soggette a ricorso ai sensi dell'art. 44 PA. L'autorità di ricorso è il Tribunale amministrativo federale (art. 47 cpv. 1 lett. b PA in combinato disposto con gli art. 31 e 33 lett. d LTF). In base all'art. 52 cpv. 3 LPD, l'IFPDT dispone di un diritto di ricorso contro le decisioni del Tribunale amministrativo federale. Esiste quindi una base legale speciale ai sensi dell'art. 89 cpv. 2 lett. d LTF. Per ulteriori informazioni si rimanda alle disposizioni pertinenti.

Il parere espresso riflette l'opinione personale dell'autore e non vincola l'IFPDT.

BIBLIOGRAFIA

Auer Christoph/Müller Markus/Schindler Benjamin (a cura di), VwVG Kommentar, 2a ed., Zurigo 2019 (cit.: VwVG-Kommentar, redattore/redattrice).

Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (a cura di), Datenschutzgesetz, Stämpflis Handkommentar, 2a ed., Berna 2022 (cit.: SHK-DSG, redattore/redattrice).

Bieri Adrian/Powell Julian (a cura di), Commentario Orell Füssli alla legge federale sulla protezione dei dati con ulteriori decreti, Zurigo 2023 (cit.: OFK-DSG, collaboratore/collaboratrice).

Blechta Gabor-Paul/Vasella David (a cura di), Datenschutzgesetz/Öffentlichkeitsgesetz, DSG/LTras (Legge sulla protezione dei dati/Legge sulla trasparenza), LPD/LTras. Commento di Basilea, 4a edizione, Basilea 2024 (cit. BSK-LPD, redattore/redattrice).

Da Molin Luca/Wesiak-Schmidt Kirsten (a cura di), Datenschutz im Unternehmen, Praxishandbuch mit Beispielen und Checklisten, Zurigo 2023 (cit.: Datenschutz im Unternehmen, redattore/redattrice).

Lobsiger Adrian, Alto rischio – nessun argomento decisivo contro i progetti di trasformazione digitale, SJZ, 2023, pagg. 311-319 (cit. Lobsiger, alto rischio – nessun argomento decisivo).

Métille Sylvain/Meier Philippe (a cura di), Commentaire Romand Loi sur la protection des données (LPD), Basilea 2023 (cit.: CR-LPD, autore).

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

Waldmann Bernhard/Krauskopf Patrick (a cura di), Praxiskommentar Verwaltungsverfahrensgesetz (VwVG), 3a ed., Friburgo e Zurigo 2022 (cit. PK VwVG, redattore/redattrice).

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 54 LPD

Un commentario di Florian Roth / Simon Mazidi

CITAZIONE SUGGERITA

Florian Roth/Simon Mazidi, Commentario all'art. 54 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Roth/Mazidi, art. 54 LPD N. XXX.

Sezione 3: Assistenza amministrativa

Art. 54 Assistenza amministrativa tra autorità svizzere

[1] Le autorità federali e cantonali comunicano all'IFPDT le informazioni e i dati personali necessari per l'adempimento dei suoi compiti legali.

[2] L'IFPDT comunica alle autorità seguenti le informazioni e i dati personali necessari per l'adempimento dei loro compiti legali:

a. autorità incaricate della protezione dei dati in Svizzera;

b. autorità di perseguimento penale competenti, in caso di denuncia di un reato conformemente all'articolo 65 capoverso 2;

c. autorità federali nonché organi di polizia cantonali e comunali, per l'esecuzione dei provvedimenti di cui agli articoli 50 capoverso 3 e 51.

STRUTTURA

In breve 673
I. Informazioni generali 673
A. Oggetto 673
B. Storia dell'origine 674
C. Scopo della norma 676
D. Forme di cooperazione e importanza 677
E. Delimitazioni 678
F. Limitazioni 680
1. Segreto d'ufficio 680
2. Requisiti di legge fondamentali 682
3. Principio della limitazione delle finalità 682
4. Principio di specialità 683
G. Esecuzione e protezione giuridica 683
II. Assistenza amministrativa a favore dell'IFPDT (cpv. 1) 686
III. Assistenza amministrativa a favore di altre autorità (cpv. 2) 690
A. Assistenza amministrativa alle autorità di protezione dei dati (lett. a) 691
B. Assistenza amministrativa alle autorità di contrasto (lett. b) 692
C. Assistenza amministrativa alle autorità federali e agli organi di polizia cantonali e comunali (lit. c) 693
Bibliografia 694
I materiali 698

IN BREVE

L'art. 54 LPD disciplina l'assistenza amministrativa tra l'IFPDT e altre autorità federali e cantonali. L'assistenza amministrativa è di notevole importanza per l'adempimento dei compiti legali dell'IFPDT. Essa consente la cooperazione tra l'IFPDT e altre autorità federali e cantonali, contribuendo così in modo significativo all'applicazione della legge sulla protezione dei dati. Il cpv. 1 disciplina l'assistenza amministrativa a favore dell'IFPDT necessaria per l'applicazione della LPD. Il cpv. 2 obbliga l'IFPDT a fornire assistenza amministrativa ad altre autorità. Le autorità alle quali l'IFPDT è obbligato a fornire assistenza amministrativa sono elencate in modo esaustivo nel cpv. 2.

I. INFORMAZIONI GENERALI

A. Oggetto

L'art. 54 LPD disciplina l'assistenza amministrativa tra l'IFPDT e altre autorità federali e cantonali. La disposizione fa parte delle competenze amministrative dell'IFPDT, che servono a far rispettare la protezione dei dati. Rappresenta inoltre una concretizzazione dell'art. 58 cpv. 1 lett. b LPD. Il cpv. 1 disciplina l'assistenza amministrativa a favore dell'IFPDT, necessaria per l'applicazione della LPD. Il cpv. 2 obbliga l'IFPDT a fornire assistenza amministrativa ad altre autorità, che dovrebbe consentire a queste ultime di adempiere ai rispettivi compiti legali nell'ambito della LPD. 1

L'art. 44 cpv. 2 frase 2 Cost. obbliga la Confederazione e i Cantoni a fornirsi reciprocamente assistenza amministrativa. L'obbligo di assistenza amministrativa è, da un lato, una manifestazione del requisito di cui all'art. 44 cpv. 1 Cost. secondo cui le autorità collaborano come partner nello Stato federale; la disposizione costituzionale obbliga la Confederazione e i Cantoni a sostenersi e collaborare reciprocamente nell'adempimento dei loro compiti. D'altra parte, si tratta di un'applicazione dell'obbligo di assistenza reciproca di cui all'art. 44 cpv. 2 frase 1 Cost. Già prima dell'entrata in vigore della Costituzione federale completamente rivista del 1999, la Commissione federale per la protezione dei dati descriveva il dovere fondamentale di tutte le autorità di cooperare in materia di informazioni come un principio 2

costituzionale non scritto del diritto svizzero. Questo principio costituzionale è ora sancito nel diritto positivo dall'art. 44 cpv. 2 Cost.

3 La disposizione costituzionale deve essere concretizzata a livello legislativo. L'art. 54 LPD rappresenta tale concretizzazione per quanto riguarda l'assistenza amministrativa tra l'IFPDT e le autorità cantonali. Va notato che l'art. 44 Cost. riguarda solo l'assistenza amministrativa tra autorità di comuni diversi e non tra autorità dello stesso comune. L'art. 54 LPD costituisce quindi una base giuridica separata per quanto riguarda l'assistenza amministrativa tra l'IFPDT e altre autorità federali.

4 Il termine "assistenza amministrativa" non è chiaramente definito dalla legge. Per assistenza amministrativa si intende generalmente il sostegno reciproco di unità amministrative (che non sono in rapporto di subordinazione l'una con l'altra) nell'adempimento dei loro compiti statutari, fornendo un'assistenza non disciplinata dal diritto processuale (diritto processuale civile, penale o amministrativo) (cfr. N. 15 e segg.). Possono essere o meno collegate ai procedimenti amministrativi in prima istanza. Anche l'assistenza al di fuori o prima di un procedimento amministrativo fa parte dell'assistenza amministrativa.

5 L'assistenza amministrativa comprende in generale tutta l'assistenza con cui un'autorità amministrativa federale o cantonale sostiene un'altra autorità amministrativa federale o cantonale nell'adempimento dei suoi compiti legali. Oltre alla fornitura di informazioni e dati (assistenza amministrativa informativa), è compresa anche la messa a disposizione di risorse fisiche o tecniche (veicoli, locali, attrezzature tecniche, ecc.). Il termine "autorità amministrativa" va inteso in senso funzionale e comprende tutte le persone fisiche e giuridiche che sono direttamente incaricate dell'adempimento di compiti di diritto pubblico della Confederazione, dei Cantoni o dei Comuni. Nel contesto dell'art. 54 LPD, l'attenzione è rivolta all'assistenza amministrativa informativa (cfr. n. 13).

B. Storia dell'origine

6 L'art. 54 LPD non ha suscitato alcuna discussione durante l'iter legislativo. L'assistenza amministrativa come presupposto necessario per l'adempimento dei compiti statutari dell'IFPDT era indiscutibile. Il progetto preliminare (art. 46 LPD) conteneva già una disposizione con lo stesso contenuto. Nella

vecchia LPD, l'articolo sull'assistenza amministrativa obbligava l'IFPDT a collaborare solo con le autorità di protezione dei dati nazionali ed estere (art. 31 cpv. 1 lett. c aDSG). L'estensione dell'assistenza amministrativa a tutte le autorità in seguito alla revisione della LPD è caratterizzata da un ampliamento delle competenze dell'IFPDT nell'ambito della LPD rivista.

Nella procedura di consultazione, alcuni Cantoni hanno criticato il fatto che il carico di lavoro aggiuntivo per le autorità cantonali e comunali non fosse chiaro e che le informazioni da fornire dovessero essere specificate in modo più preciso nell'ordinanza. Diversi partecipanti del mondo economico hanno sostenuto che i segreti aziendali o di produzione non dovrebbero essere divulgati nell'ambito di una procedura di assistenza amministrativa. 7

La disposizione sull'assistenza amministrativa nazionale (art. 48 LPD) ha subito solo alcune modifiche redazionali nella bozza di decreto rispetto alla bozza preliminare. Ad esempio, la formulazione del cpv. 1 è stata modificata nel senso che le autorità federali e cantonali comunicano ora all'IFPDT le informazioni e i dati personali necessari per l'adempimento dei suoi compiti legali. Nel progetto preliminare, la disposizione prevedeva ancora che le autorità comunicassero le informazioni e i dati personali necessari per l'applicazione della presente legge. Anche il cpv. 2 lett. a ha subito una piccola modifica redazionale: l'IFPDT comunica ora le informazioni e i dati personali alle autorità responsabili della protezione dei dati in Svizzera, nella misura in cui ciò è necessario per l'adempimento dei loro compiti legali. Il progetto preliminare limitava ancora la formulazione alle autorità cantonali responsabili della protezione dei dati. Nelle successive deliberazioni dell'Assemblea federale, l'assistenza amministrativa nazionale non ha più dato adito a discussioni; la disposizione è stata adottata nella versione del progetto di decreto senza modifiche materiali o redazionali. 8

Il fatto che l'assistenza amministrativa nazionale non sia stata oggetto di controversie significative può essere attribuito a diversi fattori. In primo luogo, l'utilità ufficiale dell'assistenza amministrativa nazionale per l'adempimento dei doveri statutari è indiscussa. Di conseguenza, Poltier dice semplicemente e giustamente: "[...] l'entraide relève de l'évidence [...]". La protezione dei dati può essere applicata più efficacemente attraverso le forme di cooperazione e collaborazione rese possibili dall'assistenza amministrativa. D'altra parte, la disposizione sull'assistenza amministrativa nazionale è una disposizione che si ritrova anche in molte altre leggi federali, dove mira anche 9

ad adempiere ai doveri di legge delle rispettive autorità. Il fatto che il Consiglio federale parli di una disposizione standard nel messaggio, che si trova anche in molte altre leggi federali, può al massimo significare che l'assistenza amministrativa è ampiamente riconosciuta come strumento nello Stato federale. In ogni caso, non esiste una formulazione standardizzata nelle singole leggi sostanziali (cfr. n. 14). Le singole disposizioni regolano l'ambito dell'assistenza amministrativa in modo troppo diverso.

C. Scopo della norma

10 La struttura federalista dello Stato e l'organizzazione dell'amministrazione basata sulla ripartizione dei compiti comportano un elevato grado di specializzazione tecnica delle singole autorità. A ciò si associa una restrizione di fatto e locale della giurisdizione, che minaccia costantemente di ostacolare l'adempimento dei compiti di legge. L'assistenza amministrativa serve a superare tali limitazioni giurisdizionali fornendo assistenza. L'IFPDT controlla quindi in modo completo l'applicazione delle norme federali sulla protezione dei dati. Tuttavia, le questioni relative alla protezione dei dati sorgono anche in relazione a settori specifici di competenza e di diritto per i quali, ad esempio, la vigilanza e l'applicazione sono affidate a un'altra autorità federale (FINMA, COMCO, ecc.). L'assistenza amministrativa è indispensabile anche a causa della divisione verticale delle competenze tra Confederazione e Cantoni: Ad esempio, per far rispettare le decisioni dell'IFPDT ai sensi dell'art. 50 e segg. LPD, sono generalmente coinvolte le autorità cantonali di esecuzione (cfr. art. 50 cpv. 3 LPD). L'assistenza amministrativa consente il necessario scambio di informazioni e la cooperazione tra le autorità, in modo da garantire l'adempimento dei mandati legali nonostante la differenziazione fattuale e locale delle attività ufficiali.

11 Lo scopo dell'assistenza amministrativa è quello di adempiere ai compiti pubblici nel modo più ottimale ed efficiente possibile e mira quindi a consentire e promuovere un'azione governativa efficace. In base all'art. 54 LPD, l'IFPDT può avvalersi della competenza e dell'esperienza di altre autorità nell'adempimento dei suoi compiti statutari. Poiché l'IFPDT può trovarsi ad affrontare un gran numero di questioni specifiche del settore, spesso dipende dalle informazioni e dal supporto di altre autorità per svolgere le indagini in modo corretto ed efficiente. L'art. 54 LPD garantisce questa

cooperazione a favore dell'IFPDT, contribuendo così all'applicazione della legge sulla protezione dei dati.

Un'altra funzione importante dell'assistenza amministrativa è la raccolta di prove. Le informazioni e i documenti che l'IFPDT ha ricevuto da altre autorità in seguito all'assistenza amministrativa per l'accertamento dei fatti rilevanti possono essere utilizzati come prove nei procedimenti amministrativi di primo grado dell'IFPDT. 12

D. Forme di cooperazione e importanza

Nella pratica, esistono diverse forme di cooperazione nell'ambito dell'assistenza amministrativa. Nel contesto della LPD, l'assistenza amministrativa informativa è al centro dell'attenzione. Questa comprende la divulgazione di dati fattuali e personali a sostegno dell'IFPDT e viceversa da parte dell'IFPDT ad altre autorità ed è esplicitamente trattata nell'art. 54 cpv. 1 e 2 LPD. In linea di principio, tutti gli atti procedurali che servono a chiarire i fatti (comprese le misure probatorie) o le misure esecutive possono essere considerati misure di assistenza amministrativa. Nell'ambito del chiarimento dei fatti, l'attenzione si concentra sull'assistenza amministrativa interna, come la fornitura di informazioni, l'ispezione di fascicoli ufficiali, la presentazione o il reperimento di documenti ufficiali o di altri documenti necessari, la cooperazione nel chiarimento di fatti rilevanti o l'accesso a una banca dati. Le interviste o le ispezioni possono essere effettuate anche come misure probatorie. L'assistenza amministrativa nel contesto delle misure di esecuzione si riferisce a misure che servono a far rispettare un ordine ufficiale. L'art. 50 cpv. 3 LPD fa espressamente riferimento alle misure di assistenza amministrativa dell'IFPDT in materia di prove e di esecuzione. 13

Insieme all'assistenza giudiziaria (cfr. n. 15 e segg.), l'assistenza amministrativa è un presupposto indispensabile per garantire uno spazio giuridico uniforme in Svizzera. L'assistenza amministrativa è di notevole importanza per l'adempimento dei compiti statutari dell'IFPDT. Tuttavia, l'affermazione di Bellanger secondo cui l'assistenza amministrativa nazionale appare "[...] comme un parent pauvre du droit [...]" non ha perso nulla della sua validità ancora oggi. Ciò è dovuto in particolare al fatto che l'assistenza amministrativa nazionale non è disciplinata in modo uniforme a livello federale. La PA tratta l'assistenza amministrativa all'art. 43. Tuttavia, questo riguarda solo l'assistenza nell'esecuzione di ordini emessi dalle autorità federali che non sono finalizzati 14

al pagamento di denaro o alla fornitura di garanzie. L'art. 43 PA non contempla invece l'assistenza amministrativa nell'ambito dell'accertamento dei fatti. Non esiste un regolamento generale che disciplini sia la procedura sia i diritti e gli obblighi delle parti coinvolte. Di conseguenza, l'assistenza amministrativa è regolata a livello di singole leggi specializzate. La portata dell'obbligo di assistenza amministrativa varia nei singoli casi, a seconda della legge specializzata applicabile. Nel caso in esame, la portata dell'obbligo di assistenza amministrativa è determinata principalmente dalla LPD, in particolare dall'art. 54 cpv. 1 e 2 e dall'art. 50 cpv. 3 in combinato disposto con l'art. 50 cpv. 1 LPD. cpv. 1 LPD. L'ambito di applicazione e le modalità dell'assistenza amministrativa devono ancora essere concretizzati nei dettagli.

E. Delimitazioni

15 L'assistenza amministrativa tra autorità svizzere (di seguito: assistenza amministrativa) deve essere distinta dall'assistenza legale da un lato e dall'assistenza amministrativa internazionale dall'altro. È difficile distinguere chiaramente l'assistenza amministrativa dall'assistenza legale. Tuttavia, la distinzione è importante per gli effetti giuridici che ne derivano. Dalla categorizzazione possono dipendere sia la scelta del diritto applicabile - e quindi la procedura - sia i limiti delle misure e la forma specifica di tutela legale. A livello di assistenza amministrativa e legale internazionale, le differenze e le loro conseguenze sono pronunciate: ad esempio, l'assistenza legale internazionale in materia penale può rientrare nell'ambito di applicazione dell'art. 6 CEDU in circostanze particolari. Il ricorso al Tribunale federale è ammissibile solo nel caso dell'assistenza giudiziaria internazionale in materia penale e dell'assistenza amministrativa in materia fiscale, che in genere ha finalità di perseguimento penale. Ad eccezione dell'assistenza amministrativa in materia fiscale, il ricorso al Tribunale federale non è ammesso contro le decisioni in materia di assistenza amministrativa internazionale.

16 Per distinguere l'assistenza amministrativa da quella legale, la dottrina e la giurisprudenza si basano su vari criteri, e talvolta per la qualificazione viene

utilizzata una combinazione di criteri. In particolare, si possono citare i seguenti criteri:

- Tipo o funzione delle autorità coinvolte: Se sono coinvolte autorità giudiziarie, si parla di assistenza legale. L'assistenza amministrativa, invece, si riferisce alle autorità amministrative.
- Natura del procedimento assistito (procedimento non contenzioso o contenzioso o procedimento per l'emissione di un'ordinanza o procedimento di appello): L'assistenza legale comprende forme di cooperazione che riguardano procedimenti esterni all'amministrazione. Questi ultimi si svolgono davanti a un'autorità esterna all'amministrazione e istituzionalmente indipendente da essa. L'assistenza legale si riferisce quindi principalmente all'assistenza procedurale (civile, penale o amministrativa) nel contesto dei procedimenti giudiziari. Un esempio classico è l'esecuzione delle sentenze. L'assistenza amministrativa, invece, comprende l'assistenza tra le autorità amministrative federali e cantonali che viene fornita al di fuori dei procedimenti stabiliti dal diritto processuale. Si svolge quindi nell'ambito di procedure amministrative interne o al di fuori di un procedimento amministrativo ed è effettuata su richiesta di un'autorità amministrativa o spontaneamente.

Seguendo questi criteri, si può parlare di assistenza amministrativa se l'assistenza viene fornita tra autorità amministrative nell'ambito di un procedimento amministrativo interno o al di fuori di un procedimento amministrativo. L'assistenza legale, invece, è fornita nell'ambito o a sostegno di un procedimento di diritto processuale - spesso un procedimento giudiziario. 17

Poiché il procedimento dinanzi all'IFPDT ai sensi degli artt. 49 e segg. LPD è un procedimento amministrativo di primo grado e non contenzioso - e non un procedimento (giudiziario) di diritto processuale - la cooperazione ufficiale assume la forma di assistenza amministrativa. Per questo motivo, l'assistenza legale non è contemplata nell'art. 54 LPD. L'assistenza amministrativa comprende anche l'esecuzione di misure (cautelari) che l'IFPDT può ordinare nell'ambito di un'indagine. 18

L'art. 54 LPD riguarda solo l'assistenza amministrativa tra autorità svizzere. L'assistenza transfrontaliera rientra nel regolamento sull'assistenza amministrativa internazionale (art. 55 LPD). 19

20 Inoltre, non tutta l'assistenza nell'ambito di una procedura amministrativa interna o al di fuori di una procedura amministrativa è coperta dall'assistenza amministrativa. L'assistenza fornita nell'ambito dell'assistenza amministrativa serve ad adempiere agli obblighi di legge dell'autorità richiedente. Le forme generali di cooperazione o alcuni accordi di cooperazione tra le autorità non costituiscono assistenza amministrativa. Tale cooperazione esiste quando autorità diverse sono responsabili della gestione di una questione specifica. Nell'ambito di applicazione della LPD, la cooperazione è disciplinata dall'art. 53 LPD.

21 Infine, l'assistenza amministrativa è sempre rivolta ad altre autorità. Non è personalizzata. Se l'IFPDT richiede l'assistenza di un funzionario con competenze specifiche nell'ambito di un'indagine, si applicano le disposizioni sulle perizie. In base all'art. 52 cpv. 1 LPD, all'art. 12 lett. e PA in combinato disposto con gli artt. 57 e segg. Art. 57 e segg. BZP.

F. Limitazioni

22 L'art. 54 LPD prevede l'obbligo giuridico per le autorità interessate di fornire assistenza amministrativa. Tuttavia, le informazioni e i dati personali possono essere scambiati solo nella misura in cui ciò sia consentito dal segreto d'ufficio e siano rispettati i requisiti di tutela dei diritti fondamentali, protezione dei dati e assistenza amministrativa, che in parte si sovrappongono.

1. Segreto d'ufficio

23 Il segreto d'ufficio è il primo ostacolo all'assistenza amministrativa. Il segreto d'ufficio è stato fortemente ridimensionato dal principio di pubblicità: Le informazioni devono essere esplicitamente etichettate come segrete ai sensi della legge federale sulla libertà d'informazione oppure devono esserci interessi rilevanti che si oppongono al principio della pubblicità. Le autorità possono ora trasmettere ad altre autorità tutte le informazioni che avrebbero dovuto mettere a disposizione dei privati in base al principio di pubblicità. Tuttavia, gli obblighi di riservatezza previsti dalla legge possono costituire un ostacolo alla divulgazione di informazioni a favore di altre autorità (art. 36 cpv. 6 lett. b LPD). Tali obblighi di riservatezza derivano, da un lato, dal segreto d'ufficio tutelato dal diritto penale (art. 320 CP), dal segreto professionale (art. 321 CP), dal segreto industriale e commerciale (art. 162 CP) o dal segreto fiscale (art. 110 CP). D'altra parte, secondo la legge sul personale, ai dipendenti

pubblici è vietato rivelare questioni professionali e aziendali che per loro natura o per disposizioni di legge o istruzioni devono essere tenute segrete (art. 22 LPers in combinato disposto con l'art. 94 OPers). Il segreto d'ufficio si applica anche ai funzionari di altri uffici che sono tenuti al segreto: È quindi una violazione del segreto d'ufficio se il funzionario rivela un segreto a un altro ufficio all'interno o all'esterno del suo dipartimento o a un superiore a cui non è direttamente subordinato. Non c'è violazione del segreto d'ufficio se c'è una giustificazione. Ciò avviene se la divulgazione delle informazioni è espressamente autorizzata da una legge sostanziale o se la divulgazione del segreto è consentita dal consenso scritto delle autorità superiori.

L'art. 54 LPD non affronta espressamente la questione se la disposizione 24
consenta di violare l'obbligo di riservatezza previsto dalla legge. A nostro avviso, la disposizione non può essere intesa come un'autorizzazione generale alla violazione degli obblighi di riservatezza previsti dalla legge a titolo di assistenza amministrativa, altrimenti l'obbligo di riservatezza potrebbe essere revocato solo su richiesta di un'altra autorità. In assenza di una disposizione giuridica concreta, l'art. 36 LPD può essere applicato per analogia - con riferimento a informazioni diverse dai dati personali. Ai sensi del cpv. 6 lett. b, gli organi federali possono rifiutare di divulgare informazioni, limitarle o subordinarle a condizioni se ciò è richiesto dagli obblighi di riservatezza previsti dalla legge. A nostro avviso, l'autorità interpellata deve quindi soppesare anche gli interessi legati alla concessione dell'assistenza amministrativa. Se, come abbiamo visto, l'art. 54 LPD non costituisce di per sé una base giuridica sufficiente per la divulgazione di informazioni e dati personali, la divulgazione è consentita ai sensi dell'art. 36 cpv. 2 solo se è indispensabile per l'adempimento dei compiti di legge (lett. a) o se sussistono altri motivi, come il consenso della persona interessata (lett. b). Occorre sempre trovare un equilibrio tra l'interesse all'assistenza amministrativa e gli interessi contrastanti alla riservatezza (cfr. anche art. 36 cpv. 6 lett. a LPD). In relazione a questa ponderazione degli interessi o per tutelare gli obblighi di riservatezza previsti dalla legge (art. 36 cpv. 6 lett. b LPD), può essere opportuno condizionare la divulgazione dei dati personali o renderli anonimi. La fornitura di assistenza amministrativa deve essere consentita anche in presenza di un'altra giustificazione ai sensi dell'art. 320 CP, come ad esempio l'autorizzazione dell'autorità superiore (art. 320 cpv. 2 CP).

2. Requisiti di legge fondamentali

25 Un altro ostacolo all'assistenza amministrativa è la tutela dei diritti fondamentali. L'art. 13 cpv. 2 Cost. protegge i dati personali e l'ambito materiale di protezione comprende anche la divulgazione di tali dati a terzi. La divulgazione di dati personali ad altre autorità costituisce quindi in genere una violazione dei diritti fondamentali delle persone interessate. L'assistenza che interferisce con i diritti fondamentali dei privati nel contesto dell'assistenza amministrativa deve soddisfare i requisiti dell'art. 36 Cost. In questi casi, il requisito di una base giuridica sufficiente per l'assistenza amministrativa deriva dall'art. 36 cpv. 1 Cost. Mentre le autorità federali - così come l'IFPDT - devono rispettare la LPD quando forniscono assistenza amministrativa, le autorità cantonali che forniscono assistenza amministrativa all'IFPDT sono soggette alle rispettive leggi cantonali sulla protezione dei dati. Anche le altre condizioni per l'ingerenza, ossia l'interesse pubblico preponderante e la proporzionalità, devono essere sempre rispettate quando si comunicano dati personali ad altre autorità. Infine, le autorità sono tenute a rispettare i principi dello Stato di diritto (art. 5 Cost.) anche quando forniscono assistenza amministrativa che non interferisce con i diritti fondamentali. Questi includono, ad esempio, il principio di legalità, il requisito dell'interesse pubblico e il principio di proporzionalità. Il legislatore federale ha incorporato i requisiti costituzionali per la divulgazione dei dati personali nella legge sulla protezione dei dati e li ha ulteriormente specificati.

3. Principio della limitazione delle finalità

26 Oltre al requisito di una base giuridica per la divulgazione dei dati personali, la LPD prevede una limitazione delle finalità (art. 6 cpv. 3 LPD). L'ulteriore utilizzo dei dati personali in seguito all'assistenza amministrativa può spesso non essere in linea con la limitazione delle finalità della raccolta e del trattamento dei dati originari ai sensi della legge sulla protezione dei dati. Tuttavia, ciò non esclude la possibilità di utilizzare i dati personali per altri scopi in un secondo momento, a condizione che vi sia una base legale o una giustificazione per questo. L'art. 54 LPD in combinato disposto con l'art. 36 LPD costituisce una base giuridica di questo tipo, che consente alle autorità di discostarsi dalla limitazione della finalità originaria quando vengono divulgati i dati personali.

4. Principio di specialità

Un'altra manifestazione del principio di limitazione delle finalità è emersa nel contesto dell'assistenza legale e amministrativa internazionale. Come la limitazione delle finalità nell'ambito della legge sulla protezione dei dati, serve a garantire un trattamento proporzionato delle informazioni e dei dati personali. Questo requisito, noto come principio di specialità, richiede che le informazioni e i dati personali possano essere utilizzati dall'autorità richiedente solo per gli scopi per cui sono stati trasmessi dall'autorità richiesta. A tal fine, l'autorità richiedente deve specificare lo scopo per cui le informazioni o i dati personali richiesti sono necessari. Anche se il principio di specialità viene spesso discusso solo in relazione all'assistenza amministrativa internazionale, è altrettanto rilevante per l'assistenza amministrativa nazionale. La limitazione delle finalità prevista dalla legge sull'assistenza amministrativa ha quindi un effetto restrittivo sulla divulgazione di informazioni e dati personali. 27

G. Esecuzione e protezione giuridica

La natura dell'assistenza amministrativa come partenariato tra autorità significa che le autorità sono organizzativamente su un piano di parità e quindi non vi è alcun rapporto di subordinazione tra loro. L'IFPDT non può far valere la sua richiesta di assistenza amministrativa nei confronti delle autorità federali o cantonali con un'istruzione o un ordine amministrativo interno. Non può nemmeno stabilire come, quando e in che misura deve essere fornita l'assistenza amministrativa; viceversa, lo stesso vale per l'assistenza amministrativa fornita dall'IFPDT a favore di altre autorità. Le modalità di assistenza amministrativa devono essere concordate tra le autorità coinvolte. La situazione è diversa se l'IFPDT ordina misure investigative nei confronti di organi federali ai sensi dell'art. 50 cpv. 3 LPD, per cui tali misure non rientrano nell'assistenza amministrativa. In questo caso, l'organo federale non fornisce assistenza all'IFPDT, ma è tenuto a collaborare in quanto destinatario dell'indagine. 28

L'assistenza amministrativa è fornita tra le autorità. Se l'autorità richiesta rifiuta di divulgare le informazioni o i dati personali dopo aver esaminato una richiesta, l'autorità richiedente non può contestare la decisione. La LPD non conferisce all'IFPDT o alle altre autorità di cui al cpv. 2 un diritto speciale di ricorso ai sensi dell'art. 48 cpv. 2 PA. Tuttavia, è ipotizzabile che, in caso di 29

rifiuto persistente da parte dell'autorità interpellata, quest'ultima possa rivolgersi al proprio organo superiore o a un'autorità di vigilanza superiore mediante un reclamo di vigilanza. Spetta poi all'autorità di vigilanza far rispettare l'obbligo di fornire assistenza amministrativa in caso di resistenza ingiustificata e, se necessario, impartire all'autorità interpellata le istruzioni necessarie. Le autorità che non appartengono allo stesso comune possono ricorrere al Tribunale federale in base all'art. 120 cpv. 1 lett. b LTF. In caso di controversia tra l'IFPDT e un'autorità cantonale di esecuzione in merito all'esistenza e alla portata dell'obbligo di fornire assistenza amministrativa ai sensi dell'art. 54 LPD, è possibile adire le vie legali.

30 Anche se l'assistenza amministrativa si svolge tra autorità e può quindi essere descritta come una "[...] azione all'interno dell'autorità [...]", essa può avere un effetto riflesso sui privati. Gli atti ufficiali compiuti nel contesto dell'assistenza amministrativa possono incidere su posizioni giuridiche o interessi meritevoli di tutela delle parti del procedimento o di terzi. Ciò include, ad esempio, il trasferimento di dati personali nel contesto dell'assistenza amministrativa informativa o l'uso di misure coercitive nel contesto dell'esecuzione. L'art. 54 LPD non stabilisce se le autorità siano obbligate a condurre un procedimento amministrativo quando forniscono assistenza amministrativa. Ai sensi dell'art. 52 cpv. 1 LPD, la procedura d'indagine è disciplinata dalla PA. Ne consegue che, se l'IFPDT richiede un'assistenza amministrativa nell'ambito della procedura d'indagine e questa ha un impatto sui diritti e sugli obblighi delle persone interessate, entrano in vigore i diritti procedurali garantiti dalla PA. La decisione dell'autorità interpellata di fornire assistenza amministrativa è da considerarsi una sentenza se vengono toccati gli interessi di privati meritevoli di tutela. In questo caso, i privati devono avere la possibilità di partecipare al procedimento. A tal fine, il privato ha lo status di parte e deve essere ascoltato ai sensi dell'art. 30 PA. La decisione di concedere l'assistenza amministrativa costituisce quindi un'ordinanza ai sensi dell'art. 5 PA, che deve essere motivata e contenere informazioni sul diritto di ricorso (art. 35 PA).

31 Per quanto riguarda i tempi di esercizio dei diritti procedurali, si possono fare varie differenziazioni in base alla dottrina e alla giurisprudenza:

- L'autorità richiedente non è tenuta a sentire le parti del procedimento o i terzi se chiede assistenza amministrativa ad altre autorità. La rinuncia al procedimento amministrativo può essere giustificata dalla tutela giuridica successivamente accordata nel procedimento principale. Ciò consente alle

parti del procedimento di far valere i propri diritti in un secondo momento davanti all'IFPDT in qualità di autorità richiedente. Se l'IFPDT basa la sua decisione nella procedura d'indagine sulle informazioni ottenute tramite l'assistenza amministrativa, deve informare la parte in causa e consentirle di accedere agli atti. Su questa base, la parte del procedimento può contestare l'esattezza delle informazioni o l'ammissibilità dell'ottenimento e della divulgazione delle informazioni.

- La decisione dell'autorità interpellata di fornire assistenza amministrativa viene generalmente presa sotto forma di sentenza se vengono toccati gli interessi di privati meritevoli di tutela. Tuttavia, l'autorità non è tenuta a emettere un'ordinanza se è obbligata a fornire assistenza amministrativa e non ha margine di giudizio. Tuttavia, il procedimento amministrativo è spesso appropriato. Ciò è particolarmente vero se la disposizione legale sull'assistenza amministrativa lascia un margine di giudizio, il che è concepibile in diverse costellazioni: tale margine di giudizio può sorgere se l'autorità interpellata deve decidere se la divulgazione delle informazioni e dei dati personali è effettivamente necessaria per l'adempimento del compito legale dell'autorità richiedente. Inoltre, quando si divulgano dati personali, la proporzionalità della divulgazione deve sempre essere esaminata a causa dell'interferenza con l'art. 13 cpv. 2 Cost. e, se necessario, devono essere imposte condizioni o altre restrizioni (ad es. riduzioni). Infine, poiché l'art. 54 LPD non si pronuncia sugli obblighi di riservatezza previsti dalla legge, in singoli casi può essere necessario soppesare gli interessi delle parti tra l'indispensabilità dell'assistenza fornita ai sensi dell'art. 36 cpv. 2 lett. a LPD e l'eventuale interesse contrastante alla riservatezza. Tuttavia, poiché in questi casi esiste anche una tutela giuridica successiva per le parti in causa, in dottrina si sostiene che il procedimento amministrativo è necessario solo se sussiste la minaccia di uno svantaggio irreparabile al di là dell'ambito del giudizio. Se entrambe le condizioni sono soddisfatte, prima che l'autorità interpellata decida se concedere o meno l'assistenza amministrativa, alla parte del procedimento deve essere garantito un contraddittorio e quindi una tutela giuridica.
- Infine, l'autorità interpellata deve tenere conto anche della posizione giuridica dei terzi. Nella misura in cui i dati personali vengono trasmessi nel contesto di un'assistenza amministrativa che incide sui diritti e sugli obblighi di persone non coinvolte nel procedimento principale, a queste

ultime deve essere riconosciuto lo status di parte. Poiché non esiste alcuna possibilità di tutela giuridica successiva per i terzi, i diritti procedurali devono essere rispettati al momento della divulgazione dei dati personali. Ciò è possibile solo se vengono ascoltati in anticipo e se viene emessa una decisione motivata e contestabile.

32 La procedura di ricorso è disciplinata dalla PA. Le decisioni sono soggette a ricorso presso il Tribunale amministrativo federale ai sensi dell'art. 44 PA. In ultima istanza, il ricorso in materia di diritto pubblico può essere presentato al Tribunale federale ai sensi degli artt. 82 e segg. LTF; le decisioni relative all'assistenza amministrativa nazionale possono essere impugnate senza limitazioni. Solo le decisioni in materia di assistenza amministrativa internazionale, ad eccezione dell'assistenza amministrativa in materia fiscale, sono escluse dal ricorso in materia di diritto pubblico. Inoltre, l'eccezione di cui all'Art. 83 lit. v LTF si applica solo alle decisioni del Tribunale Amministrativo Federale su divergenze di opinione tra autorità nell'ambito dell'assistenza amministrativa nazionale. I ricorsi dei privati non sono interessati.

33 Gli atti di esecuzione costituiscono di per sé atti reali, motivo per cui non sono generalmente impugnabili. In questo contesto, è possibile solo un ricorso di vigilanza. Questo può essere presentato o all'autorità di vigilanza cantonale competente o all'IFPDT. Quest'ultimo, in quanto autorità federale richiedente, rimane responsabile dell'esecuzione, per cui deve anche controllare la corretta esecuzione dell'assistenza all'esecuzione da parte dei Cantoni.

II. ASSISTENZA AMMINISTRATIVA A FAVORE DELL'IFPDT (CPV. 1)

34 Il cpv. 1 stabilisce il principio secondo cui le autorità federali e cantonali forniscono all'IFPDT le informazioni e i dati personali necessari per l'adempimento dei suoi compiti legali. Il cpv. 1 ha una duplice natura, in quanto autorizza l'IFPDT a ottenere assistenza amministrativa da altre autorità. Dall'altro lato, obbliga le autorità interpellate a fornire assistenza amministrativa.

35 Le autorità richieste sono le autorità federali e le autorità cantonali. Le autorità comunali non sono espressamente menzionate nell'art. 54 cpv. 1 LPD.

Baeriswyl ne deduce che le autorità comunali non sono obbligate a fornire assistenza amministrativa all'IFPDT. Questa opinione è supportata da un'interpretazione sistematica: Le autorità comunali sono esplicitamente menzionate nel cpv. 3, ma non nel cpv. 1. Inoltre, secondo un'opinione diffusa, i Comuni non sono destinatari dell'art. 44 Cost. che regola i principi dell'assistenza amministrativa nello Stato federale. Tuttavia, vi sono buone ragioni per un'opinione contraria: in primo luogo, non vi è alcuna indicazione nei materiali che l'assistenza amministrativa nazionale di cui all'art. 54 LPD debba essere intesa in modo tale da escludere le autorità comunali dal termine "autorità cantonali". In secondo luogo, sembra discutibile che l'esclusione delle autorità comunali sia opportuna per quanto riguarda la funzione dell'assistenza amministrativa - ossia consentire all'IFPDT di svolgere i suoi compiti nell'ambito di un'applicazione coerente della protezione dei dati - soprattutto perché l'ambito del trasferimento di compiti pubblici ai Comuni è lasciato ai Cantoni e quindi le autorità con ambiti di competenza molto ampi sarebbero escluse dall'obbligo di fornire assistenza amministrativa. Soprattutto in considerazione dello scopo, è ragionevole supporre che anche i Comuni debbano fornire assistenza amministrativa all'IFPDT.

Il contenuto e la portata delle informazioni da fornire non sono descritti in modo più dettagliato nel cpv. 1. La disposizione si riferisce alle informazioni e ai dati personali che devono essere forniti all'FDPIC. La disposizione si riferisce alle informazioni e ai dati personali necessari per l'adempimento dei compiti statutari dell'IFPDT. L'esplicita menzione dei dati personali nel cpv. 1 chiarisce almeno che tutte le informazioni relative a una persona fisica identificata o identificabile possono essere comunicate all'IFPDT nel contesto dell'assistenza amministrativa. Questa disposizione è completata dall'art. 39 lett. c GDPR, secondo cui l'IFPDT può trattare dati personali, compresi quelli particolarmente sensibili, nell'ambito della cooperazione con le autorità federali, cantonali ed estere. Il riferimento alle informazioni chiarisce che l'art. 54 LPD si riferisce all'assistenza amministrativa informativa. Oltre alla divulgazione di dati personali espressamente menzionata, si riferisce anche alla divulgazione di dati fattuali (cfr. n. 13). L'assistenza amministrativa nel contesto delle misure di esecuzione è menzionata nell'art. 50 cpv. 3 LPD. A causa dell'ampia formulazione del cpv. 1, il contenuto del tipo di informazioni e di dati personali è determinato principalmente da un'interpretazione basata sui compiti legali dell'IFPDT. 36

37 I compiti legali dell'IFPDT sono diversi e sono elencati nel capitolo 7 della LPD. In primo luogo, l'indagine sulle violazioni delle norme sulla protezione dei dati ai sensi degli artt. 49 e segg. LPD. Tra gli altri compiti dell'IFPDT figurano la tenuta di un registro delle attività di trattamento degli organi federali (art. 56 LPD) e la presentazione di un rapporto annuale all'Assemblea federale (art. 57 LPD). L'art. 58 LPD elenca poi altri compiti in modo non esaustivo. Non è chiaro fin dall'inizio per quali compiti e in che misura l'IFPDT richieda informazioni e dati personali ad altre autorità. Sarà quindi chiaro nella pratica in quali situazioni e per quali azioni l'IFPDT dipende da tali informazioni o dati personali per adempiere a un compito legale. Tuttavia, è logico che l'IFPDT richieda assistenza amministrativa alle autorità federali o cantonali quando indaga su violazioni delle norme sulla protezione dei dati. L'assistenza amministrativa è uno strumento fondamentale sia per il chiarimento dei fatti che per l'applicazione delle misure amministrative ai sensi dell'art. 51 LPD. L'IFPDT può, ad esempio, richiedere l'assistenza delle autorità di polizia cantonali per l'esecuzione di misure investigative.

38 La comunicazione di informazioni o dati personali di cui al cpv. 1 può avvenire spontaneamente o su richiesta. Tuttavia, la formulazione della disposizione è molto meno chiara rispetto, ad esempio, all'art. 112 cpv. 1 DBG, che si riferisce espressamente a entrambe le forme di assistenza amministrativa. L'assistenza amministrativa spontanea si verifica quando un'autorità è legalmente obbligata a informare d'ufficio un'altra autorità su fatti di cui è a conoscenza. Altre autorità possono, ad esempio, informare l'IFPDT di propria iniziativa che il trattamento dei dati da parte di un organo federale o di un privato potrebbe violare le norme sulla protezione dei dati. D'altra parte, l'assistenza amministrativa può essere fornita anche su richiesta dell'IFPDT. L'assistenza amministrativa su richiesta è il concetto classico di assistenza amministrativa.

39 Poiché le altre autorità sono obbligate a divulgare le informazioni o i dati personali, in questo caso l'assistenza è obbligatoria e non a discrezione dell'autorità richiesta. Dal punto di vista della formulazione ("divulgare"), la disposizione è paragonabile all'art. 32 cpv. 1 LPGA e all'art. 87 cpv. 1 LPP, che prescrivono anch'essi un'assistenza obbligatoria. Tuttavia, va notato che l'obbligo di fornire assistenza amministrativa sussiste solo se è necessario divulgare le informazioni e i dati personali. Ciò presuppone che l'autorità richiesta sia autorizzata a verificare la necessità della divulgazione.

L'assistenza amministrativa può essere fornita solo se e nella misura in cui l'IFPDT non sarebbe in grado di adempiere al proprio mandato legale senza le informazioni o i dati personali, o potrebbe farlo solo con notevoli spese aggiuntive. Di conseguenza, Kerboas/Lennman affermano anche che un semplice miglioramento o una maggiore efficienza nell'adempimento del compito legale non può servire da giustificazione per la divulgazione. Se la necessità non è data, non c'è nemmeno l'obbligo di divulgare le informazioni o i dati personali. Per la divulgazione di dati personali (art. 36 cpv. 3 Cost.) e di informazioni (art. 5 cpv. 2 Cost.), ciò deriva già dal principio di proporzionalità (cfr. n. 25). Inoltre, può essere giustificato il rifiuto di fornire assistenza amministrativa o, se necessario, la divulgazione subordinata a condizioni o restrizioni (ad esempio, riformulazioni) (cfr. n. 24).

A differenza delle disposizioni sull'assistenza amministrativa contenute in altre leggi sostanziali (art. 32 cpv. 1 LPGA, art. 45 cpv. 1 BüG o art. 87 cpv. 1 LPP), l'art. 54 LPD non prevede espressamente che l'autorità richiedente debba presentare una richiesta scritta e motivata all'autorità richiesta. Una richiesta scritta e motivata è necessaria, ad esempio, quando vi è una maggiore necessità di legittimare la divulgazione delle informazioni in questione. È il caso, ad esempio, del diritto delle assicurazioni sociali, in quanto la divulgazione dei dati costituisce una deviazione dal principio della riservatezza; nelle procedure di naturalizzazione, i dati richiesti per valutare l'acquisizione o la perdita della cittadinanza svizzera sono spesso dati personali particolarmente sensibili ai sensi dell'art. 5 lett. c LPD. Tale necessità di legittimazione non sussiste per tutte le informazioni ottenute dall'IFPDT. L'esenzione dall'obbligo di richiesta scritta di cui al cpv. 1 esprime il fatto che le possibilità di azione dell'IFPDT non devono essere eccessivamente limitate e che vi è un interesse all'applicazione più semplice ed efficiente possibile della protezione dei dati. Soprattutto quando l'IFPDT richiede semplici informazioni ad altri uffici, la richiesta scritta non è obbligatoria. Se l'IFPDT richiede la divulgazione di dati personali o se le informazioni devono essere utilizzate nell'ambito di un'indagine per violazione delle norme sulla protezione dei dati, l'opinione espressa in questa sede è che la richiesta debba essere formulata per iscritto, anche in considerazione dei diritti di protezione giuridica delle persone interessate (cfr. n. 30 s.). 40

41 L'art. 54 LPD non fornisce una base per la raccolta di informazioni di massa su un gran numero di persone. Ai sensi della vecchia LPD, l'IFPDT ha dichiarato: "La divulgazione di dati completi, ad esempio tramite elenchi (elettronici) e il trasferimento ad altre raccolte di dati, richiede una base giuridica esplicita in cui devono essere disciplinati anche i limiti necessari per il trattamento dei dati e la sicurezza". In assenza di un'autorizzazione esplicita nell'art. 54 LPD, si può presumere che l'IFPDT non possa ottenere o divulgare informazioni di massa in relazione ai dati personali. Si può anche supporre che le richieste senza un motivo preciso o una domanda specifica (le cosiddette "fishing expedition") non siano consentite nel caso dell'assistenza amministrativa su richiesta. Con riferimento all'art. 19 cpv. 1 lett. a LPD (che oggi corrisponde all'art. 36 cpv. 2 lett. a LPD), il Tribunale amministrativo federale ha affermato che "l'autorità richiedente [...] deve descrivere all'autorità interpellata i fatti rilevanti, identificare specificamente le informazioni e i documenti richiesti e indicare il motivo della richiesta [...]". A nostro avviso, ciò vale anche per l'art. 54 LPD.

42 A deve sempre essere indicato il motivo, anche se questo requisito non è esplicitamente indicato nel cpv. 1: Da un lato, l'autorità richiesta deve essere in grado di valutare la necessità di divulgare le informazioni e i dati personali. In secondo luogo, il principio di limitazione delle finalità previsto dalla legge sull'assistenza amministrativa (principio di specialità) richiede l'indicazione dello scopo per il quale le informazioni o i dati personali richiesti sono necessari (cfr. n. 27). Se l'assistenza amministrativa è fornita su richiesta dell'IFPDT, quest'ultimo deve quindi sempre giustificare la misura in cui ha bisogno delle informazioni o dei dati personali per adempiere ai suoi doveri di legge nel caso specifico.

III. ASSISTENZA AMMINISTRATIVA A FAVORE DI ALTRE AUTORITÀ (CPV. 2)

43 L'IFPDT comunica informazioni e dati personali a determinate autorità nella misura in cui ciò è necessario per l'adempimento dei loro compiti legali. Il cpv. 2 elenca in modo esaustivo le autorità per le quali l'IFPDT è tenuto a fornire assistenza amministrativa.

44 L'art. 54 LPD funge da base giuridica per la prestazione reciproca di assistenza amministrativa. Pertanto, per quanto riguarda il contenuto e la portata delle

informazioni ("informazioni e dati personali"), la necessità di divulgazione e le ulteriori modalità, si rimanda ai commenti sul cpv. 1. Come nel caso del cpv. 1, l'assistenza amministrativa può essere fornita sia spontaneamente che su richiesta delle autorità indicate nel cpv. 2. In caso di richiesta, l'IFPDT è tenuto a fornire assistenza. In altre parole, la divulgazione di informazioni e dati personali non è a discrezione dell'IFPDT. Tuttavia, il presupposto è che la divulgazione sia necessaria e che non sia impedita da altre restrizioni. Ad esempio, l'IFPDT è anche soggetto al segreto d'ufficio ai sensi dell'art. 22 LPers.

A. Assistenza amministrativa alle autorità di protezione dei dati (lett. a)

Il cpv. 2 lett. a stabilisce la reciprocità per il trasferimento di informazioni e dati personali nei confronti di altre autorità di protezione dei dati: così come l'IFPDT può richiedere informazioni e dati personali a queste autorità ai sensi del cpv. 1, le altre autorità di protezione dei dati possono richiedere informazioni all'IFPDT. Le autorità responsabili della protezione dei dati in Svizzera sono autorità il cui mandato legale consiste anche nel controllo e nell'applicazione della protezione dei dati. Ciò deriva dalle basi giuridiche pertinenti a livello federale, cantonale o comunale. 45

I requisiti dell'art. 15 della Convenzione 108+ possono essere utilizzati per concretizzare il concetto di autorità di protezione dei dati. L'art. 15 cpv. 5 della Convenzione 108+ stabilisce, tra l'altro, che l'autorità di controllo deve agire in completa indipendenza e imparzialità e non deve essere vincolata da istruzioni nello svolgimento dei suoi compiti e nell'esercizio dei suoi poteri. In questo contesto, le autorità cantonali e comunali indipendenti per la protezione dei dati e altre organizzazioni di diritto pubblico possono essere considerate autorità indipendenti per la protezione dei dati ai sensi dell'art. 15 cpv. 5 della Convenzione 108+. 46

I consulenti per la protezione dei dati degli organi federali (art. 10 cpv. 4 LPD) esercitano la loro funzione nei confronti dell'organo federale ai sensi dell'art. 26 cpv. 1 lett. b LPD in modo indipendente e su istruzioni. Tuttavia, non hanno lo status di autorità. 47

Oltre alla divulgazione di informazioni e dati personali su richiesta di un'altra autorità in singoli casi, lo scambio di informazioni avviene attraverso i 48

seguenti meccanismi e forum istituzionalizzati. Questi meccanismi garantiscono un flusso di informazioni reciproco tra l'IFPDT e le autorità cantonali e comunali per la protezione dei dati e consentono alle autorità di contribuire con le loro preoccupazioni e competenze.

- Nell'associazione privatim, le autorità indipendenti per la protezione dei dati degli enti pubblici svizzeri si riuniscono nella Conferenza dei Commissari svizzeri per la protezione dei dati. Questa promuove la cooperazione tra i Cantoni, i Comuni e la Confederazione nel settore della protezione dei dati attraverso un costante scambio di informazioni. L'associazione esprime le proprie opinioni su questioni relative alla protezione dei dati sotto forma di dichiarazioni, risposte a consultazioni, linee guida e schede informative. Ad esempio, privatim ha pubblicato un opuscolo sui rischi e le misure specifiche del cloud e ha commentato la decisione di diversi governi cantonali di utilizzare "Microsoft 365" nell'amministrazione. Insieme all'IFPDT, l'associazione ha anche aggiornato le linee guida sull'applicazione della legge sulla protezione dei dati al trattamento digitale dei dati personali in relazione alle elezioni e alle votazioni in Svizzera. Si tratta di una forma generale di cooperazione tra le autorità.
- In base all'art. 111g LIG, all'art. 102d LDT e all'art. 8b IPB, le autorità cantonali per la protezione dei dati e l'IFPDT collaborano, nell'ambito delle rispettive competenze, per un controllo coordinato del trattamento dei dati personali nel contesto della cooperazione Schengen/Dublino. A tal fine, l'IFPDT ha istituito un gruppo di coordinamento delle autorità svizzere di protezione dei dati nel quadro dell'attuazione degli accordi di associazione. Il gruppo di coordinamento si occupa dello scambio di informazioni necessarie per un controllo efficace del trattamento dei dati, discute le difficoltà di interpretazione e applicazione della legislazione, analizza i problemi che possono sorgere nell'esercizio del controllo o in relazione ai diritti delle persone interessate ed elabora proposte e pareri armonizzati al fine di trovare soluzioni comuni.

B. Assistenza amministrativa alle autorità di contrasto (lett. b)

49 In base all'art. 65 cpv. 2 LPD, l'IFPDT ha il diritto di segnalare sospetti di reati contro le disposizioni penali del capitolo 8 della LPD. Per contro, le segnalazioni di violazioni della sicurezza dei dati ai sensi dell'art. 24 LPD

possono essere utilizzate in un procedimento penale contro la persona soggetta all'obbligo di segnalazione solo con il suo consenso.

Nell'interesse di un'efficace applicazione della protezione dei dati, l'IFPDT può utilizzare questo diritto di notifica per lavorare a un'applicazione standardizzata della LPD. Può costituirsi come parte civile nell'ambito di un procedimento penale cantonale. Può inoltre impugnare le ordinanze di archiviazione e ricorrere contro le decisioni cantonali. 50

La denuncia del presunto reato all'autorità penale cantonale competente comporta generalmente la divulgazione di dati personali. Si tratta di dati personali particolarmente sensibili ai sensi dell'art. 5 lett. c cpv. 5 LPD. L'art. 54 cpv. 2 lett. b LPD costituisce la base giuridica necessaria per la divulgazione dei dati personali. 51

C. Assistenza amministrativa alle autorità federali e agli organi di polizia cantonali e comunali (lit. c)

Ai sensi dell'art. 50 cpv. 3 LPD, l'IFPDT può ricorrere ad altre autorità federali e a organi di polizia cantonali o comunali per attuare le misure di cui all'art. 50 cpv. 1 LPD. Le misure consistono nel fatto che l'IFPDT può ordinare l'accesso a tutte le informazioni, i documenti, gli elenchi delle attività di trattamento e i dati personali necessari per l'indagine (lett. a), l'accesso a locali e impianti (lett. b), l'interrogatorio di testimoni (lett. c) o le perizie (lett. d). Tuttavia, ciò è possibile solo se è stata avviata un'indagine e il privato o l'ente federale non adempie al suo dovere di collaborazione. L'assistenza amministrativa da parte delle autorità di polizia cantonali o comunali assume la forma di misure esecutive che servono a far rispettare l'ordine ufficiale dell'IFPDT. Questa assistenza amministrativa è fornita a favore dell'IFPDT e rientra pertanto nell'art. 54 cpv. 1 LPD. L'art. 54 cpv. 2 lett. c LPD fornisce la base giuridica necessaria all'IFPDT per trasmettere alle autorità summenzionate le informazioni e i dati personali necessari per l'effettiva esecuzione dei suoi ordini. 52

Per l'esecuzione delle misure di cui all'art. 51 LPD, l'IFPDT può inoltre trasmettere informazioni e dati personali alle autorità federali e agli organi di polizia cantonali e comunali che sono tenuti ad adempiere ai loro compiti legali. L'art. 51 prevede misure amministrative e conferisce all'IFPDT poteri di disposizione. Ai sensi del cpv. 1, in caso di violazione delle norme sulla 53

protezione dei dati, può ordinare l'adeguamento, l'interruzione o la cancellazione totale o parziale del trattamento e la cancellazione o la distruzione totale o parziale dei dati personali.

54 A differenza dell'esecuzione delle misure ordinate ai sensi dell'art. 50 LPD, l'esecuzione degli ordini dell'IFPDT ai sensi dell'art. 51 LPD non è espressamente disciplinata nella LPD. In questo caso si applica la PA. Almeno per quanto riguarda i privati, ciò è già evidente dal fatto che l'IFPDT ha la facoltà di emettere sentenze, il che significa che è soggetto alla PA ai sensi dell'art. 1 cpv. 2 lett. c PA. La PA è già applicabile ai procedimenti amministrativi dell'IFPDT a causa dell'assenza di disposizioni di esenzione applicabili ai sensi dell'art. 2 lett. f. La PA è applicabile ai procedimenti amministrativi dell'IFPDT. L'art. 52 cpv. 1 LPD conferma ancora una volta espressamente l'applicabilità della PA ai procedimenti amministrativi dell'IFPDT. Questa disposizione ha principalmente uno scopo chiarificatore.

55 L'art. 41 PA fornisce la base giuridica necessaria per l'esecuzione delle ordinanze. L'IFPDT può avvalersi dell'elenco di misure esecutive contenute nella disposizione, certamente non esaustivo. L'IFPDT deve attenersi alla procedura prevista dall'art. 41 PA, che comprende la minaccia di esecuzione con la fissazione di un termine (successivo), la determinazione e l'esecuzione delle misure coercitive. In caso di pericolo imminente, può rinunciare alla minaccia di misure coercitive e alla concessione di un termine per l'adempimento.

56 Se l'IFPDT ordina la cancellazione parziale o completa o addirittura la distruzione e la persona privata o l'organo federale si rifiuta, può provvedere personalmente alla cancellazione o alla distruzione ai sensi dell'art. 41 cpv. 1 lett. a e lett. b PA.

57 L'IFPDT può ricorrere alle autorità federali e agli organi di polizia cantonali e comunali per l'esecuzione. Ai sensi dell'art. 54 cpv. 2 lett. c LPD, l'IFPDT può trasmettere a tali autorità le informazioni e i dati personali necessari per l'esecuzione.

BIBLIOGRAFIA

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).

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 55 LPD

Un commentario di Florian Roth / Simon Mazidi

CITAZIONE SUGGERITA

Florian Roth/Simon Mazidi, Commentario all'art. 55 LPD, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (a cura di), Commentario online alla Legge federale sulla protezione dei dati

Breve citazione: OK-Roth/Mazidi, art. 55 LPD N. XXX.

Art. 55 Assistenza amministrativa alle autorità estere

[1] L'IFPDT può scambiare informazioni o dati personali con autorità estere incaricate della protezione dei dati ai fini dell'adempimento dei rispettivi compiti legali in materia di protezione dei dati se:

a. la reciprocità dell'assistenza amministrativa è garantita;

b. le informazioni e i dati personali sono utilizzati soltanto nell'ambito della procedura concernente la protezione dei dati su cui si fonda la domanda di assistenza amministrativa;

c. l'autorità destinataria s'impegna a salvaguardare i segreti professionali, d'affari e di fabbricazione;

d. le informazioni e i dati personali sono comunicati a terzi soltanto previo consenso dell'autorità mittente; e

e. l'autorità destinataria s'impegna a rispettare gli oneri e le limitazioni d'uso richiesti dall'autorità mittente.

2 Per motivare la propria domanda di assistenza amministrativa o per dare seguito alla domanda di un'autorità, l'IFPDT può trasmettere in particolare le seguenti informazioni:

a. l'identità del titolare del trattamento, del responsabile del trattamento o di qualsiasi altra persona che partecipa al trattamento;

b. le categorie di persone interessate;

c. l'identità delle persone interessate sempreché:

le persone interessate abbiano dato il loro consenso, o
la comunicazione dell'identità delle persone interessate sia indispensabile per l'adempimento dei compiti legali dell'IFPDT o dell'autorità estera;

d. i dati personali o le categorie di dati personali trattati;

e. lo scopo del trattamento;

f. i destinatari o le categorie di destinatari;

g. le misure tecniche e organizzative.

3 Prima di trasmettere a un'autorità estera informazioni che potrebbero contenere segreti professionali, d'affari o di fabbricazione, l'IFPDT informa le persone fisiche o giuridiche titolari di tali segreti e le invita a esprimere un parere, salvo che ciò sia impossibile o richieda un onere sproporzionato.

STRUTTURA

In breve 704
I. Considerazioni generali 704
A. Oggetto della normativa 704
1. Base 704
2. Contesto internazionale 705
B. Cronistoria 707
C. Finalità della norma 708
D. Delimitazioni 709
1. Assistenza amministrativa nazionale 709
2. Delimitazione rispetto all'assistenza giudiziaria 709
3. Semplice cooperazione amministrativa 711
E. Forme di cooperazione 711
1. Forme di cooperazione 712
2. Cooperazione multilaterale 713
3. Trattati internazionali 713
F. Schranken 714
G. Tutela giuridica 716
II. Presupposti (cpv. 1) 719
A. Considerazioni generali 719
1. Autorità competenti 719
2. Ambito e contenuto 720
3. Natura giuridica 720
B. Presupposti di ammissibilità 721
1. Reciprocità (lett. a) 721
2. Principio di specialità (lett. b) 721
3. Principio di riservatezza (lett. c) 723
4. Principio della lunga mano (lett. d) 724
5. Rispetto delle condizioni e delle restrizioni (lett. e) 725
III. Comunicazione di dati personali (capoverso 2) 726
IV. Obbligo di informazione e presa di posizione (cpv. 3) 727
Bibliografia 729
I materiali 734

IN BREVE

L'articolo 55 LPD disciplina l'assistenza amministrativa internazionale tra l'IFPDT e le autorità straniere competenti in materia di protezione dei dati. La disposizione consente la cooperazione transfrontaliera tra le autorità di protezione dei dati e contribuisce in modo significativo all'applicazione della legislazione in materia. Il cpv. 1 disciplina le condizioni alle quali l'IFPDT può scambiare informazioni o dati personali con autorità straniere. Il cpv. 2 stabilisce quali informazioni l'IFPDT può comunicare in relazione a tale scambio. Il cpv. 3 definisce i diritti di determinate persone che possono essere interessate da un atto di assistenza amministrativa.

I. CONSIDERAZIONI GENERALI

A. Oggetto della normativa

1. Base

1 L'assistenza amministrativa internazionale ha lo scopo di garantire il **reciproco sostegno transfrontaliero delle autorità competenti in materia di protezione dei dati** (di seguito: autorità di protezione dei dati) nell'adempimento dei loro compiti legali, fornendo assistenza al di fuori di una procedura disciplinata dal diritto processuale. L'articolo 55 LPD disciplina l'assistenza amministrativa internazionale tra l'IFPDT e le autorità di protezione dei dati straniere.

2 L'art. 55 è una **nuova disposizione** della LPD. La disposizione precedente (art. 31 cpv. 1 lett. c aDSG) obbligava l'IFPDT solo a collaborare con le autorità straniere di protezione dei dati. Ciò comprendeva uno scambio tecnico su singoli temi o una collaborazione regolare in seno a comitati, gruppi di lavoro o conferenze. Tuttavia, la disposizione non forniva una base giuridica sufficiente all'IFPDT per collaborare con le autorità estere e scambiare informazioni nell'ambito della sorveglianza e del controllo del diritto federale in materia di protezione dei dati. Ciononostante, già nell'ambito della aDSG l'IFPDT ha collaborato pienamente con le autorità straniere di protezione dei dati. All'epoca lo scambio transfrontaliero di dati era in gran parte regolato

dalle norme generali dell'assistenza amministrativa, basate principalmente sugli obblighi di diritto internazionale (art. 13 segg. della Convenzione 108).

L'articolo 55 LPD stabilisce ora **effettive norme procedurali**, disciplinando i presupposti per lo scambio di informazioni o dati personali con autorità estere (cpv. 1) e le informazioni che possono essere trasmesse (cpv. 2). Il cpv. 3 conferisce poi ai titolari di un segreto professionale, commerciale o di fabbricazione il diritto all'informazione e la possibilità di esprimere il proprio parere qualora l'IFPDT comunichi a un'autorità estera informazioni che potrebbero contenere tali segreti. 3

L'articolo 55 LPD è all'insegna dell'**armonizzazione con il diritto europeo**. L'articolo 50 della direttiva (UE) 2016/680 richiede che le autorità di controllo si prestino reciproca assistenza amministrativa. Allo stesso tempo, la disposizione soddisfa i requisiti dell'articolo 61 DSGVO e degli articoli 16-21 della Convenzione 108+. 4

2. Contesto internazionale

L'obiettivo della Convenzione 108+ è quello di creare un livello uniforme di protezione dei dati e di rafforzare i **meccanismi di applicazione**. Ciò include in particolare la cooperazione transfrontaliera tra le autorità di controllo. La Svizzera ha ratificato la Convenzione 108+ il 7 settembre 2023. Per entrare in vigore, la Convenzione 108+ richiede la ratifica da parte di 38 Stati contraenti. Nella primavera del 2025 questo numero non era ancora stato raggiunto. Nei riferimenti successivi alla Convenzione 108+ occorre quindi tenere conto del fatto che essa non è ancora entrata in vigore. Tuttavia, sembra probabile che ciò avverrà a breve. 5

La Convenzione 108+ obbliga le Parti contraenti a collaborare e a prestarsi reciproca assistenza nell'attuazione della Convenzione. Essa prevede, in forma non esaustiva, diverse forme di cooperazione. In primo luogo, le autorità di controllo si prestano assistenza amministrativa, in particolare scambiandosi tutte le **informazioni pertinenti e utili**. Si può trattare di due tipi di informazioni: 6

- Lo **scambio generale di informazioni e documenti** sul diritto e la prassi amministrativa in materia di protezione dei dati. Questo scambio non dovrebbe presentare problemi, poiché le informazioni possono essere scambiate liberamente e rese accessibili al pubblico.

- Lo **scambio di informazioni riservate**, compresi i dati personali. Per quanto riguarda i dati personali, la Convenzione 108+ prevede che questi possano essere oggetto di trattamento solo se sono di importanza cruciale per la cooperazione (cioè se senza la loro fornitura la cooperazione sarebbe inefficace) o se l'interessato ha dato il suo consenso esplicito, riferito al caso specifico, volontario e informato. In caso contrario, lo scambio di dati personali provenienti da un trattamento concreto è escluso.

7 Oltre allo scambio di informazioni pertinenti e utili, gli obiettivi della cooperazione possono essere raggiunti anche attraverso **indagini concertate**, come ad esempio indagini o operazioni coordinate, nonché attraverso l'attuazione di misure comuni.

8 Le autorità di controllo sono tenute a soddisfare le richieste che ricevono da altre autorità di controllo. L'art. 20 della Convenzione 108+ prevede il **rifiuto delle richieste** in modo definitivo solo se la richiesta non è compatibile con i poteri dell'autorità di controllo (lett. a), la richiesta non è conforme alle disposizioni della Convenzione 108+ (lett. b) o se l'adempimento della richiesta non è compatibile con la sovranità, la sicurezza nazionale o l'ordine pubblico (ad es. per garantire la riservatezza delle indagini di polizia) della Parte contraente o con i diritti e le libertà fondamentali delle persone soggette alla giurisdizione di tale Parte contraente (lett. c).

9 A livello di diritto dell'Unione esistono due atti giuridici rilevanti per la protezione dei dati. Il **DSGVO** è il decreto fondamentale in materia di protezione dei dati e disciplina la protezione dei dati trattati nell'ambito del mercato interno. All'articolo 61 disciplina in modo dettagliato l'assistenza amministrativa tra le autorità di controllo degli Stati membri dell'UE o del SEE, senza che siano necessari accordi specifici tra gli Stati membri nei singoli casi. L'assistenza amministrativa internazionale è disciplinata dall'articolo 50 lettera b DSGVO. La DSGVO non fa parte dell'acquis di Schengen, pertanto non è vincolante per la Svizzera.

10 La **direttiva (UE) 2016/680** serve a proteggere i dati personali trattati a fini di prevenzione, indagine, accertamento o perseguimento di reati o di esecuzione di sanzioni penali, compresa la protezione da e la difesa contro minacce alla sicurezza pubblica. Poiché il contenuto della direttiva (UE) 2016/680 si basa sulla DSGVO, le disposizioni dei due atti giuridici sono in gran parte

coincidenti. La direttiva fa parte dell'acquis di Schengen. In qualità di Stato associato a Schengen, la Svizzera è tenuta ad accettare, attuare e applicare gli sviluppi dell'acquis di Schengen, la cui attuazione in Svizzera è avvenuta nell'ambito della revisione totale della LPD per quanto riguarda l'autorità di controllo. L'obbligo delle autorità di controllo di prestarsi reciproca assistenza amministrativa è disciplinato dall'articolo 50 della direttiva (UE) 2016/680.

B. Cronistoria

Nel **progetto preliminare** della LPD, la disposizione relativa all'assistenza amministrativa internazionale (art. 47 LP-P) era ancora suddivisa in due capoversi, il primo dei quali disciplinava le richieste di assistenza amministrativa dell'IFPDT alle autorità estere e il secondo l'assistenza amministrativa dell'IFPDT a favore delle autorità estere. Il primo paragrafo stabiliva le informazioni che l'IFPDT poteva comunicare alle autorità straniere per ottenere assistenza amministrativa; il secondo paragrafo stabiliva le condizioni alle quali l'IFPDT poteva prestare assistenza amministrativa alle autorità straniere. 11

Nel corso della **consultazione**, alcuni partecipanti hanno fatto notare che la sistematica dell'articolo 47 era carente. Infatti, a seconda che l'IFPDT fosse l'autorità richiedente o l'autorità interpellata, non si applicavano le stesse condizioni per la comunicazione delle informazioni. Diversi partecipanti si sono infine espressi a favore del fatto che le informazioni che costituiscono segreti commerciali o di fabbricazione non possano essere comunicate nell'ambito di una procedura di assistenza amministrativa tra l'IFPDT e un'autorità straniera di protezione dei dati senza che sia garantita la protezione di tali segreti o senza che il detentore del segreto abbia dato il suo consenso. 12

La sistematica della disposizione ha subito una modifica fondamentale nel **progetto di** LPD e dopo la consultazione (art. 49 P-LPD). Anziché sottoporre le richieste di assistenza amministrativa dell'IFPDT alle autorità estere e l'assistenza amministrativa dell'IFPDT a favore delle autorità estere a normative diverse, sono state uniformate le condizioni per lo scambio di informazioni o dati personali con le autorità estere di cui al cpv. 1 e la comunicazione di dati personali di cui al cpv. 2. Il cpv. 2 disciplina in modo uniforme quali informazioni l'IFPDT può comunicare all'autorità estera per motivare la sua richiesta di assistenza amministrativa o per dare seguito alla 13

richiesta di un'autorità estera. Le modifiche hanno comportato anche un inasprimento: il progetto è stato integrato con il requisito della reciprocità (art. 49 cpv. 1 lett. a P-LPD) ed è stato inserito un nuovo cpv. 3 relativo ai segreti professionali, commerciali o di fabbricazione. Le riserve espresse in sede di consultazione in merito alla sistematica e alla comunicazione dei segreti commerciali e di fabbricazione sembrano quindi essere state ascoltate.

14 Nelle successive **deliberazioni** delle Camere federali, l'assistenza amministrativa internazionale non ha più dato adito a discussioni; la disposizione è stata approvata nella versione del progetto di legge con solo lievi modifiche redazionali.

C. Finalità della norma

15 In considerazione del **carattere sempre più transfrontaliero del trattamento dei dati**, la cooperazione internazionale tra le autorità di protezione dei dati assume un'importanza sempre maggiore. L'aumento quantitativo del trattamento transfrontaliero dei dati personali ha aumentato il rischio di violazioni della sfera privata e della protezione dei dati in generale. Per far fronte a questo rischio è indispensabile una cooperazione efficace e stretta sotto forma di assistenza amministrativa internazionale. Al centro di tale cooperazione vi è il sostegno reciproco delle autorità di protezione dei dati: nell'ambito della loro attività di vigilanza e consulenza, esse hanno il compito di garantire il rispetto delle norme pertinenti in materia di protezione dei dati anche in un contesto transfrontaliero, tutelando così efficacemente i diritti delle persone interessate.

16 L'articolo 55 LPD costituisce la **base giuridica** che consente all'IFPDT di collaborare con le autorità straniere di protezione dei dati nell'ambito della sua attività di vigilanza e di scambiare informazioni e dati personali. Ciò consente all'IFPDT di esercitare la sua attività di sorveglianza anche in caso di trattamenti transfrontalieri di dati da parte di organi federali e privati e di adempiere così ai suoi compiti legali. Nell'ambito della sua attività di sorveglianza e consulenza in materia di trattamenti transfrontalieri di dati da parte di organi federali e privati, l'IFPDT può quindi, se necessario, contattare l'autorità di protezione dei dati del rispettivo Stato destinatario. Ciò è opportuno, ad esempio, quando, in mancanza di conoscenze specialistiche in loco, deve ricorrere alle conoscenze e alle informazioni di un'autorità di

protezione dei dati straniera per valutare in che misura siano soddisfatti i requisiti di protezione dei dati relativi allo scambio di dati.

La cooperazione internazionale sotto forma di assistenza amministrativa serve sempre a **preservare la sovranità**. In base alla sovranità territoriale nel diritto internazionale, uno Stato ha fondamentalmente il potere sovrano esclusivo sul proprio territorio. Questo deve essere rispettato dagli altri Stati. Le autorità di uno Stato straniero non possono quindi compiere atti ufficiali sul territorio di un altro Stato senza il consenso di quest'ultimo. Non hanno quindi accesso diretto ai dati e alle informazioni che si trovano sul territorio straniero. L'assistenza amministrativa consente di superare questo ostacolo alla sovranità in una procedura ordinata, in quanto l'IFPDT, che dispone dei dati e delle informazioni necessari, può fornire assistenza amministrativa alle autorità straniere di protezione dei dati. Le autorità straniere di protezione dei dati possono così essere indirizzate alla via dell'assistenza amministrativa. In questo modo è possibile impedire alle autorità straniere di protezione dei dati di adottare autonomamente misure (investigative) extraterritoriali. Ciò vale naturalmente anche nel caso contrario, quando l'IFPDT necessita di informazioni e dati personali di cui dispongono le autorità straniere di protezione dei dati. 17

D. Delimitazioni

1. Assistenza amministrativa nazionale

A differenza dell'assistenza amministrativa nazionale, l'assistenza amministrativa internazionale comprende l'assistenza fornita alle autorità straniere o internazionali o che l'IFPDT riceve da autorità straniere o internazionali. L'oggetto è quindi l'**assistenza transfrontaliera** tra l'IFPDT e le autorità straniere di protezione dei dati. Si tratta sempre di un'assistenza a favore di un altro Stato. Non è compresa l'assistenza amministrativa nazionale che viene fornita tra l'IFPDT e altre autorità federali o cantonali per l'adempimento dei rispettivi compiti legali e che è disciplinata dall'articolo 54 LPD. 18

2. Delimitazione rispetto all'assistenza giudiziaria

La delimitazione tra assistenza amministrativa e assistenza giudiziaria in ambito internazionale è difficile. Mentre nel contesto nazionale esistono 19

almeno dei criteri di delimitazione – anche se in questo caso non è sempre possibile tracciare una linea di demarcazione netta –, la situazione giuridica nel contesto internazionale è ancora più confusa. Spesso i due istituti giuridici non vengono più distinti, ma vengono trattati **congiuntamente**. Una parte della dottrina chiede quindi di considerare l'assistenza amministrativa e l'assistenza giudiziaria in modo dogmatico congiunto. Alcune leggi raggruppano quindi i due tipi di assistenza nello stesso paragrafo.

20 A nostro avviso, tuttavia, la distinzione è essenziale a causa degli **effetti giuridici** che ne derivano. Sia la scelta del diritto applicabile (base giuridica) – e quindi le norme procedurali e di ricorso – sia i rispettivi presupposti e limiti delle misure possono essere diversi: In circostanze particolari, l'assistenza giudiziaria internazionale in materia penale può rientrare nel campo di applicazione dell'articolo 6 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU; RS 0.101). Un ricorso al Tribunale federale è ammissibile solo in caso di assistenza giudiziaria internazionale e di assistenza amministrativa in materia fiscale, che di norma ha finalità penali.

21 Per determinare l'assistenza amministrativa e giudiziaria si possono applicare in linea di principio i seguenti **criteri**, che talvolta possono anche essere combinati:

- **Tipo o funzione delle autorità coinvolte:** l'assistenza giudiziaria internazionale avviene tra autorità giudiziarie. L'assistenza amministrativa, invece, viene prestata tra autorità amministrative dello Stato richiedente e dello Stato richiesto.
- **Natura del procedimento assistito**: dal punto di vista procedurale, si ha assistenza giudiziaria internazionale quando viene fornita assistenza a un'autorità straniera o internazionale per un procedimento penale, amministrativo o civile. Di norma, essa viene prestata in relazione a un procedimento esterno all'amministrazione (cioè giudiziario). L'assistenza amministrativa internazionale, invece, consiste in un'assistenza tra le autorità dello Stato richiedente e dello Stato richiesto al di fuori di un procedimento (giudiziario) disciplinato dal diritto processuale, allo scopo di adempiere a compiti legali.

22 Poiché la cooperazione ai sensi dell'articolo 55 LPD consiste in un'assistenza transfrontaliera tra autorità amministrative (IFPDT e autorità straniere di

protezione dei dati) e poiché tale assistenza è fornita al di fuori di un procedimento disciplinato dal diritto processuale, la cooperazione tra autorità avviene sotto **forma di assistenza amministrativa**. L'articolo 55 LPD disciplina quindi solo l'assistenza amministrativa internazionale; la LPD non disciplina invece l'assistenza giudiziaria internazionale.

3. Semplice cooperazione amministrativa

Non tutte le forme di assistenza transfrontaliera tra l'IFPDT e le autorità di protezione dei dati straniere che avvengono al di fuori di una procedura disciplinata dal diritto processuale costituiscono assistenza amministrativa. L'assistenza amministrativa transfrontaliera si riferisce sempre a persone determinate o determinabili e avviene quindi nell'ambito di un caso concreto. Il cpv. 1 si riferisce chiaramente a **casi concreti** in cui un'autorità di protezione dei dati riceve informazioni e dati personali per poter adempiere al proprio mandato legale. 23

La cooperazione amministrativa finalizzata allo scambio generale di informazioni ed esperienze (ad esempio sulle *best practices*) è una semplice **cooperazione amministrativa**. A tal fine, l'IFPDT può collaborare con le autorità straniere di protezione dei dati indipendentemente da un caso specifico e dalla relativa attività di vigilanza concreta. Ciò consente uno scambio su questioni rilevanti che sorgono in relazione al trattamento transfrontaliero dei dati, nonché l'elaborazione di pareri o raccomandazioni. La semplice cooperazione amministrativa può essere basata sull'art. 58 cpv. 1 lett. b LPD. 24

E. Forme di cooperazione

In assenza di una legge generale sull'assistenza amministrativa internazionale, le singole disposizioni in materia di assistenza amministrativa sono sparse nelle diverse **leggi speciali** e nei trattati internazionali. Esse presentano una notevole eterogeneità, il che rende molto difficile una categorizzazione trasversale. L'approccio settoriale consente invece di tenere conto in modo mirato delle peculiarità del settore specifico e degli interessi e delle esigenze delle autorità coinvolte e delle persone interessate. Il contenuto e la portata della cooperazione formale con le autorità straniere di protezione dei dati nel campo della LPD si basano quindi in primo luogo sull'articolo 55 LPD. Le forme di cooperazione devono tuttavia essere concretizzate nei dettagli. 25

1. Forme di cooperazione

26 L'articolo 55 LPD lascia aperta la forma della cooperazione. La disposizione stabilisce semplicemente che l'IFPDT può scambiare informazioni o dati personali con autorità straniere per l'adempimento dei rispettivi compiti previsti dalla legge nel settore della protezione dei dati. Spetta quindi all'IFPDT decidere, a sua **discrezione**, l'intensità e la forma della cooperazione con le autorità straniere di protezione dei dati.

27 Il testo dell'articolo 55 LPD, secondo cui l'IFPDT può scambiare informazioni e dati personali con le autorità straniere, chiarisce che l'**assistenza amministrativa in materia di informazioni** è al centro dello scambio con le autorità straniere di protezione dei dati. Ciò comprende la comunicazione di dati oggettivi e personali allo scopo di fornire assistenza all'IFPDT e, viceversa, da parte dell'IFPDT ad altre autorità straniere di protezione dei dati per l'adempimento dei rispettivi compiti legali. Questa forma di cooperazione può essere collegata all'indagine di presunte violazioni delle disposizioni delle rispettive leggi sulla protezione dei dati.

28 L'articolo 55 LPD non si esprime espressamente sulla possibilità di **condurre indagini coordinate**. Tuttavia, in base all'articolo 55 LPD, l'IFPDT è autorizzato a intraprendere tali forme di cooperazione. Il testo dell'articolo 55 LPD può essere interpretato nel senso che lo svolgimento di indagini coordinate fa parte dello scambio di informazioni e dati personali. Infine, anche la cooperazione nell'ambito di indagini coordinate si basa in ultima analisi su uno scambio di informazioni. Nei materiali non vi sono inoltre indicazioni che limitino le forme di cooperazione allo scambio di informazioni. L'art. 55 LPD lascia piuttosto aperte le forme di cooperazione, il che depone a favore di una comprensione il più possibile ampia dell'assistenza amministrativa internazionale. Considerato lo scopo dell'assistenza amministrativa internazionale, ovvero garantire nel modo più efficace possibile il rispetto delle norme sulla protezione dei dati in un contesto transfrontaliero, è ovvio che tutte le forme di cooperazione rientrano nell'assistenza amministrativa internazionale, purché siano soddisfatte le condizioni di cui al cpv. 1. Di conseguenza, anche la fornitura di assistenza nelle indagini e lo svolgimento di indagini coordinate sono contemplati dall'articolo 55 LPD.

Attualmente non esiste una base giuridica specifica per il **riconoscimento e l'esecuzione** delle decisioni delle autorità straniere di protezione dei dati. Anche le misure di assistenza amministrativa concesse dall'IFPDT ai sensi dell'articolo 55 LPD non arrivano al punto di comprendere l'esecuzione in Svizzera delle decisioni delle autorità straniere di protezione dei dati, come ad esempio le sanzioni. L'esecuzione delle sanzioni delle autorità straniere di protezione dei dati fallirebbe spesso a causa del requisito della doppia incriminabilità, dato che le norme penali della LPD e del DSGVO non coincidono. Ciò è particolarmente rilevante poiché i responsabili del trattamento e gli incaricati del trattamento in Svizzera rientrano nel campo di applicazione territoriale del DSGVO e possono quindi essere soggetti al regime sanzionatorio. 29

2. Cooperazione multilaterale

Il carattere sempre più transfrontaliero del trattamento dei dati comporta un rafforzamento della vigilanza transfrontaliera, che si traduce in una rete di autorità di vigilanza alla quale partecipa anche l'IFPDT. Lo scambio transfrontaliero di informazioni, che tra l'altro mira a favorire lo sviluppo di norme transfrontaliere, avviene spesso in **organismi multilaterali** e reti internazionali. Questi presentano un grado più o meno elevato di istituzionalizzazione e costituiscono una forma di semplice cooperazione amministrativa (cfr. N. 23 f.). 30

3. Trattati internazionali

Al di là dell'articolo 55 LPD, il Consiglio federale è libero di regolamentare in modo specifico la cooperazione tra l'IFPDT e le autorità straniere di protezione dei dati nell'ambito di trattati internazionali. L'IFPDT avrebbe preferito che l'articolo 55 LPD fosse stato integrato in modo tale da consentirgli di regolamentare autonomamente le modalità di cooperazione con le autorità straniere nell'ambito di un accordo. L'art. 67 lett. a LPD prevede tuttavia che il **Consiglio federale** possa concludere autonomamente trattati internazionali relativi alla cooperazione internazionale tra autorità di protezione dei dati. 31

L'art. 55 LPD costituisce già una base sufficiente per consentire lo scambio di dati personali e, ad esempio, anche di segreti professionali, commerciali e di fabbricazione, alle condizioni di cui al cpv. 1. A tal fine non è necessario un 32

trattato internazionale. Tuttavia, un trattato di questo tipo è opportuno quando una **collaborazione a lungo termine** richiede un livello più elevato di cooperazione e questa deve essere formalizzata. Anche la delimitazione delle competenze delle diverse autorità di protezione dei dati può essere disciplinata nell'ambito di un trattato internazionale. Infine, un trattato internazionale è necessario se si intendono stabilire diritti e doveri delle autorità di protezione dei dati che vanno oltre l'art. 55 LPD. Al di fuori del campo di applicazione della Convenzione 108+ e della direttiva (UE) 2016/680, si può pensare a un obbligo di assistenza amministrativa o alla regolamentazione della comunicazione a terzi (cfr. N. 8 e N. 10).

F. Schranken

33 Nell'ambito dell'assistenza amministrativa internazionale occorre sempre tenere presente che sono coinvolti due rapporti giuridici, che talvolta possono essere in **contrasto** tra loro. Da un lato, esiste un rapporto di diritto internazionale tra lo Stato richiedente e lo Stato richiesto. Tale rapporto è disciplinato in primo luogo dai requisiti per la prestazione di assistenza amministrativa, come previsto nel presente cpv. 1. In primo piano vi è la questione di sapere in che misura sia possibile collaborare con lo Stato richiedente in materia di protezione dei dati sulla base del cpv. 1. Dall'altro lato, esiste anche un rapporto giuridico tra lo Stato richiesto e la persona interessata dalle informazioni o dai dati personali trasmessi nell'ambito dell'assistenza amministrativa. In questo rapporto, per quanto riguarda i dati personali, si contrappongono il diritto costituzionale alla protezione della sfera privata e il compito dello Stato di garantire il rispetto delle norme sulla protezione dei dati in un contesto transfrontaliero. Per entrambi i rapporti, la tutela dei diritti fondamentali e la legislazione sulla protezione dei dati stabiliscono determinati requisiti che devono essere rispettati in caso di comunicazione transfrontaliera di informazioni e dati personali.

34 L'articolo 13 cpv. 2 della Cost. federale della Confederazione Svizzera (Cost.; RS 101) tutela i dati personali e quelli relativi alla persona. L'**autodeterminazione informale** garantisce che una persona possa decidere autonomamente a chi e quando rivelare fatti della propria vita personale e se e per quale scopo le informazioni che la riguardano possono essere trattate. L'ambito di protezione oggettivo non è quindi interessato solo quando il trattamento dei dati personali avviene in modo abusivo. È

sufficiente un trattamento senza il consenso degli interessati. La comunicazione di dati personali a terzi è quindi anch'essa contemplata dall'articolo 13 capoverso 2 Cost. La comunicazione di dati personali a un'autorità straniera di protezione dei dati costituisce quindi di norma una violazione dei diritti fondamentali delle persone interessate.

Le violazioni dei diritti fondamentali sono ammesse a determinate condizioni 35
(cfr. art. 36 Cost.). L'art. 55 LPD costituisce una base legale sufficiente per la comunicazione dei dati personali alle autorità straniere di protezione dei dati. Il rispetto il più efficace possibile delle norme sulla protezione dei dati in un contesto transfrontaliero costituisce anche un importante interesse pubblico, che deriva in ultima analisi anche dai diritti di protezione sanciti dall'articolo 13 cpv. 2 Cost. La comunicazione di dati personali alle autorità straniere di protezione dei dati deve quindi essere proporzionata. Gli elementi di diritto individuale dei principi di assistenza amministrativa sanciti dall'art. 55 cpv. 1 LPD – principio di specialità e di riservatezza (cfr. N. 54 segg. e N. 60 segg.), il principio della lunga mano (cfr. N. 65 segg.) e la possibilità di subordinare la comunicazione di dati personali a determinate condizioni o di renderli anonimi (cfr. N. 68 segg.) – contribuiscono indirettamente alla proporzionalità della comunicazione. Tuttavia, in caso di comunicazione di dati personali ad autorità straniere di protezione dei dati, l'IFPDT deve verificare in che misura la comunicazione sia proporzionata nel caso concreto. Ciò induce Kerboas/Lennman a commentare che tale **verifica della proporzionalità** richiede molto tempo e risorse in ogni singolo caso, ma a volte porta solo a scarsi risultati.

Anche l'assistenza amministrativa internazionale tra l'IFPDT e le autorità 36
straniere di protezione dei dati rientra nel **campo di applicazione della LPD**. Ne consegue in primo luogo che l'IFPDT può comunicare dati personali solo se, ai sensi dell'articolo 16 LPD, nello Stato dell'autorità di protezione dei dati richiedente esiste un livello di protezione adeguato. Nei rapporti con le parti contraenti della Convenzione 108+, si può generalmente presumere, salvo circostanze particolari, che sussista un livello di protezione adeguato. Anche i motivi previsti dall'articolo 36 capoverso 6 LPD ostacolano la comunicazione di dati personali all'estero da parte di organi federali, e quindi dell'IFPDT. L'IFPDT rifiuta quindi la comunicazione nell'ambito dell'assistenza amministrativa transfrontaliera o la limita se ciò è richiesto da interessi pubblici rilevanti, da interessi manifestamente meritevoli di

protezione della persona interessata (lett. a) o da disposizioni particolari in materia di protezione dei dati (lett. b). Per quanto riguarda la possibilità di rifiutare o limitare la comunicazione sulla base di obblighi legali di segretezza, si rimanda alle seguenti considerazioni (cfr. N. 64 e N. 77).

- **Gli interessi pubblici** che ostacolano la divulgazione possono essere la sicurezza militare, la protezione dello Stato o le attività di polizia. Tali interessi sussistono anche quando la divulgazione può compromettere la posizione in negoziati, il processo di formazione dell'opinione e della volontà dell'organo pubblico, l'efficacia di misure investigative, di sicurezza o di vigilanza o le relazioni con l'estero. Tra gli interessi pubblici possono rientrare anche quelli di politica economica, monetaria o valutaria. Se tali interessi sono coinvolti e si può presumere con una certa probabilità che la divulgazione causerebbe un danno grave, la divulgazione deve essere rifiutata.
- Per quanto riguarda l'**interesse degno di protezione** della persona interessata, occorre innanzitutto valutare in che misura la divulgazione delle informazioni comprometta in modo inaccettabile la protezione della sfera privata.

G. Tutela giuridica

37 L'assistenza amministrativa internazionale avviene tra l'IFPDT e un'autorità straniera di protezione dei dati. La divulgazione di informazioni e dati personali può essere inizialmente definita semplicemente come «[...] atto interno dell'autorità [...]» o attribuita all'**effettivo atto amministrativo**. Il fatto che l'effettivo atto amministrativo incida sulla posizione giuridica dei singoli costituisce quindi un effetto indiretto dell'assistenza amministrativa internazionale che questa può avere sui privati. L'articolo 55 LPD non si pronuncia sul fatto che le autorità siano tenute a fornire assistenza amministrativa per l'esecuzione di un procedimento amministrativo.

38 Una tutela giuridica efficace presuppone naturalmente un oggetto di ricorso idoneo e quindi una decisione. Se l'assistenza amministrativa in materia di informazioni è un'azione amministrativa non soggetta a decisione nel senso di un **atto reale** dell'IFPDT, occorre quindi ottenere prima una decisione di accertamento basata sull'art. 25*a* della legge federale sulla procedura amministrativa (legge sulla procedura amministrativa, PA; RS 172.021). In

questi casi, tuttavia, la persona interessata spesso non è a conoscenza dell'atto di assistenza amministrativa, motivo per cui non può di fatto avvalersi dell'art. 25*a* PA. Ai fini di un'efficace tutela giuridica, è fondamentale stabilire in quali casi sussiste il diritto all'emanazione di una decisione. Solo la decisione apre la possibilità di avvalersi della tutela giuridica amministrativa.

39 La necessità di una decisione per la divulgazione di informazioni e dati personali da parte dell'IFPDT è regolata dalle norme generali della PA. La LPD non prevede deroghe speciali in materia. La decisione dell'IFPDT di prestare assistenza amministrativa deve essere considerata una decisione quando sono coinvolti **interessi meritevoli di tutela** di persone private. L'interesse meritevole di tutela non presuppone un interesse giuridicamente protetto. Sono sufficienti interessi puramente effettivi, economici o ideali, purché questi appaiano sempre meritevoli di tutela.

40 Il concetto di interesse degno di tutela si basa sulla qualità di parte ai sensi dell'art. 6 PA, che a sua volta è collegato all'art. 48 PA. Ai sensi della posizione di parte, ogni persona ha un interesse in una decisione che, in caso di emanazione di una decisione, sarebbe legittimata a presentare ricorso. Il presupposto è una **particolare rilevanza** per la persona. Questa deve avere un rapporto di particolare vicinanza con l'oggetto che deve essere regolato nella decisione e quindi essere interessata più della collettività. Tale coinvolgimento sussiste per Wyss, ad esempio, quando gli atti di assistenza amministrativa determinano in modo permanente e significativo diritti e doveri. Da ciò egli deduce che nei casi in cui la posizione giuridica viene modificata in modo irreversibile, è necessario emanare una decisione. Viceversa, va notato che la trasmissione di dati personali o di informazioni spesso costituisce «solo» una misura preparatoria in vista dell'emanazione *successiva* di una decisione. L'avvio di un procedimento amministrativo non costituisce di per sé una decisione. Nel campo dell'assistenza amministrativa internazionale, tuttavia, è importante sottolineare che la trasmissione dei dati all'estero può di per sé costituire una violazione degli interessi degni di protezione delle persone interessate, come confermato dall'art. 16 segg. LPD.

41 In generale si può affermare che la **comunicazione di dati personali** costituisce sempre una violazione dell'autodeterminazione informativa. Ciò significa che sussiste sempre un interesse sufficiente. Se l'IFPDT giunge alla conclusione che i requisiti per l'assistenza amministrativa di cui al cpv. 1 sono soddisfatti, deve avviare un procedimento in caso di comunicazione di dati

personali e decidere in merito alla comunicazione dei dati personali a un'autorità straniera di protezione dei dati in una decisione ai sensi dell'articolo 5 e dell'articolo 34 segg. PA. La qualità di parte nel procedimento consente alla persona interessata di esercitare i diritti delle parti concessi dalla PA: sussiste quindi, tra l'altro, il diritto di essere sentiti, il diritto di consultare gli atti, il diritto di essere rappresentati o anche il diritto di ricevere la notifica della decisione. Infine, la partecipazione al procedimento amministrativo è strettamente legata alla legittimazione a ricorrere.

42 Anche la **divulgazione di segreti professionali, commerciali o di fabbrica** costituisce senza dubbio un caso particolare. A questo proposito, cpv. 3 obbliga l'IFPDT a dare alle persone interessate la possibilità di esprimere il proprio parere prima di divulgare a un'autorità straniera di protezione dei dati informazioni che potrebbero contenere segreti professionali, commerciali o di fabbrica. Ciò deriva già dal diritto di essere sentiti ai sensi dell'articolo 29 PA. L'articolo 55 capoverso 3 LPD non crea quindi alcun valore aggiunto procedurale riconoscibile, ma serve a chiarire la situazione.

43 Il coinvolgimento delle persone interessate nella procedura amministrativa deve avvenire in modo tale che queste possano esercitare efficacemente i loro diritti di parte. In altre parole, la tutela giuridica deve essere garantita in tempo utile. Prima di comunicare le informazioni o i dati personali all'autorità di protezione dei dati richiedente, l'IFPDT deve informare le persone interessate della prevista comunicazione: una volta che le informazioni o i dati personali sono stati comunicati all'autorità di protezione dei dati richiedente, la tutela giuridica interna non può più essere efficace. L'ulteriore trattamento delle informazioni o dei dati personali è determinato al di fuori dell'ordinamento giuridico svizzero. Poiché l'utilizzo delle informazioni e dei dati personali all'estero non può essere impedito, la comunicazione all'autorità di protezione dei dati richiedente crea una situazione irreversibile. Ciò è stato riconosciuto dal Tribunale federale nel contesto dell'assistenza amministrativa internazionale in materia fiscale: «Una volta che i dati sono stati trasmessi all'estero, di norma non è più possibile impedire che vengano utilizzati».

44 Con l'IFPDT, un'autorità federale decide in merito alla collaborazione con le autorità straniere di protezione dei dati e alla comunicazione di informazioni e dati personali alle stesse. Se la decisione di comunicazione viene emanata

sotto forma di decisione ai sensi dell'art. 5 PA, anche il **ricorso** è disciplinato dalla PA. Ai sensi dell'art. 44 PA, le decisioni sono soggette a ricorso al Tribunale amministrativo federale. Le decisioni relative all'assistenza amministrativa internazionale sono in linea di principio escluse dal ricorso in materia di diritto pubblico al Tribunale federale. Ciò ha lo scopo di alleggerire il carico di lavoro del Tribunale federale e di consentire un procedimento rapido grazie alla riduzione del numero di istanze. Di conseguenza, il Tribunale amministrativo federale decide in ultima istanza in materia di assistenza amministrativa internazionale nel campo di applicazione della LPD. È tuttavia ipotizzabile che, per altre questioni di competenza del Tribunale federale, sia necessario decidere in via preliminare sulla ricevibilità dell'assistenza amministrativa internazionale.

II. PRESUPPOSTI (CPV. 1)

A. Considerazioni generali

L'articolo 55 capoverso 1 LPD disciplina i presupposti ai quali l'IFPDT può scambiare informazioni e dati personali con le autorità estere per l'adempimento dei rispettivi compiti legali nel settore della protezione dei dati. I presupposti costituiscono **elementi caratteristici** dell'assistenza amministrativa transfrontaliera. Essi si sono sviluppati nel contesto dell'assistenza giudiziaria e vengono utilizzati nel settore dell'assistenza amministrativa. 45

1. Autorità competenti

Ai sensi dell'art. 55 cpv. 1 LPD sono comprese le autorità straniere competenti in materia di protezione dei dati nel loro Stato. In altre parole, lo scambio di informazioni e dati personali avviene solo con **autorità straniere di protezione dei dati**. La LPD non contiene requisiti più dettagliati per la qualifica di autorità straniera di protezione dei dati. A nostro avviso, per la comprensione del termine si può fare riferimento all'autorità di controllo descritta nell'articolo 15 della Convenzione 108+. Tale disposizione obbliga le parti contraenti a istituire una o più autorità pubbliche di controllo e sorveglianza indipendenti e imparziali che contribuiscano alla protezione delle persone fisiche in relazione al trattamento dei loro dati personali. Tali autorità possono essere costituite da un unico responsabile della protezione 46

dei dati o da un collegio. Oltre all'indipendenza, è essenziale che l'autorità di controllo disponga di strumenti di sorveglianza e controllo efficaci. L'autorità deve quindi avere anche competenze investigative.

47 Inoltre, occorre distinguere tra gli organismi che trattano i dati dei rispettivi Stati – comprese le autorità di controllo in determinati settori economici o industriali – e le autorità di controllo specifiche nel settore della protezione dei dati. La cooperazione transfrontaliera nel contesto della protezione dei dati avviene principalmente a livello degli **organi che trattano i dati**. Questi ultimi devono valutare quotidianamente, nell'ambito dell'adempimento dei loro compiti legali, se lo scambio di informazioni e dati personali con un'autorità straniera è ammissibile. Per gli organi che trattano dati, la cooperazione è regolata dalla rispettiva legge specifica. A tal proposito occorre sempre tenere conto anche degli articoli 16 e 36 LPD. L'IFPDT è invece incaricato della sorveglianza di questi organi che trattano dati e a tal fine può ricorrere all'assistenza amministrativa internazionale disciplinata dall'articolo 55 LPD.

2. Ambito e contenuto

48 Lo scambio di informazioni e dati personali riguarda tutti i **compiti legali** dell'IFPDT o dell'autorità straniera di protezione dei dati. L'ambito dei compiti legali è determinato dalla legislazione nazionale e l'ammissibilità dello scambio è stabilita in base alla richiesta, che deve illustrare in che misura le informazioni o i dati personali sono necessari per l'adempimento dei compiti legali. I compiti legali dell'IFPDT sono elencati nel capitolo 7 della LPD. Per evadere le richieste di assistenza amministrativa straniere, l'IFPDT può intraprendere tutte le azioni che gli sono consentite dalle disposizioni della LPD applicabili alla sua attività.

49 Oltre alle **informazioni**, l'IFPDT può scambiare anche **dati personali** ai sensi dell'articolo 5 lettera a LPD. L'IFPDT può quindi comunicare tutte le informazioni che si riferiscono a una persona fisica identificata o identificabile.

3. Natura giuridica

50 L'articolo 55 LPD non contiene **alcun obbligo** di assistenza amministrativa transfrontaliera. Esso autorizza semplicemente l'IFPDT a prestare assistenza amministrativa o a richiederla alle condizioni di cui al cpv. 1. Nei rapporti con

le autorità straniere di protezione dei dati che appartengono agli Stati contraenti della Convenzione 108+, occorre tuttavia rispettare l'obbligo di prestare assistenza amministrativa previsto dalla Convenzione e i motivi di rifiuto (cfr. N. 8).

B. Presupposti di ammissibilità

Affinché l'IFPDT possa scambiare informazioni e dati personali con le autorità straniere di protezione dei dati, devono essere soddisfatti **cumulativamente** i cinque presupposti di cui all'art. 55 cpv. 1 LPD. Nella pratica è difficile valutare in modo definitivo in che misura i singoli presupposti siano soddisfatti. In pratica, pertanto, i requisiti dovrebbero essere fissati per iscritto nell'ambito della concessione dell'assistenza amministrativa e comunicati all'autorità straniera di protezione dei dati richiedente. 51

1. Reciprocità (lett. a)

L'articolo 55 cpv. 1 lettera a LPD prevede che tra la Svizzera e lo Stato estero sia garantita la **reciprocità dell'assistenza amministrativa**. La reciprocità è un elemento caratteristico dell'assistenza amministrativa. Di conseguenza, un'autorità di protezione dei dati richiedente può chiedere assistenza amministrativa sotto forma di informazioni e dati personali solo se è disposta a sua volta a concedere assistenza amministrativa. 52

Tale assistenza amministrativa è garantita nei rapporti con le parti contraenti della Convenzione 108+ e con gli Stati membri dell'UE sulla base della direttiva (UE) 2016/680. Nei rapporti con altre autorità di protezione dei dati straniere, la reciprocità è garantita in modo vincolante, a condizione che un **trattato internazionale** preveda l'assistenza amministrativa con reciprocità. Il Consiglio federale può concludere autonomamente tali trattati internazionali in base all'art. 67 lett. a LPD. In assenza di una base giuridica internazionale, l'IFPDT deve ottenere la garanzia della reciprocità nel singolo caso, potendo accogliere la richiesta di assistenza amministrativa solo sulla base di tale garanzia. 53

2. Principio di specialità (lett. b)

L'art. 55 cpv. 1 lett. b LPD è espressione del principio di specialità. Il principio di specialità o il principio di limitazione alla finalità costituisce un **principio** 54

tradizionale del diritto internazionale in materia di assistenza amministrativa e giudiziaria internazionale, che deriva dal diritto dell'estradizione. Esso è inoltre sancito dall'art. 19 della Convenzione 108+. Il Tribunale federale attribuisce a tale principio – almeno nel campo del diritto dell'estradizione – il carattere di diritto internazionale consuetudinario. Per l'assistenza amministrativa, tuttavia, il principio è anche normato in molte leggi federali.

55 Secondo questo principio, le informazioni e i dati personali scambiati possono essere utilizzati dall'autorità richiedente **solo per la procedura di protezione dei dati** su cui si basa la richiesta di assistenza amministrativa e per la quale sono state trasmesse le informazioni o i dati personali. Un ulteriore utilizzo è consentito solo se le leggi dei due Stati o un trattato internazionale prevedono tale possibilità e se l'autorità richiesta che ha fornito le informazioni o i dati personali autorizza l'ulteriore utilizzo nel caso specifico. Per un successivo utilizzo parallelo delle informazioni e dei dati personali in un eventuale procedimento penale devono essere rispettati i principi dell'assistenza giudiziaria internazionale in materia penale.

56 Il principio di specialità funge da **barriera** che tutela in primo luogo la sovranità dello Stato interpellato. Allo stesso tempo, però, la limitazione alla finalità serve anche a rafforzare i diritti della personalità delle persone interessate e a garantire un uso proporzionato delle informazioni e dei dati personali. La limitazione alla finalità vieta un ulteriore utilizzo illimitato da parte dello Stato richiedente.

57 Oltre alla sua funzione di barriera, il principio di specialità funge anche da **presupposto di ammissibilità** per la divulgazione di informazioni e dati personali: l'autorità di protezione dei dati richiedente deve fornire garanzie sufficienti che utilizzerà le informazioni o i dati personali solo per lo scopo per cui sono stati trasmessi dall'autorità richiesta. Sulla base del principio di diritto internazionale della buona fede contrattuale, il Tribunale federale ha finora sostenuto che il rispetto del principio di specialità da parte degli Stati può essere dato per scontato. Solo in presenza di indizi concreti di un uso improprio nello Stato richiedente è necessario verificare il rispetto del principio. Alla luce di questa giurisprudenza, l'IFPDT non è tenuto a richiedere alcuna garanzia se l'assistenza amministrativa si basa su un trattato internazionale che include il principio di specialità. In virtù del principio di buona fede sancito dall'articolo 26 della Convenzione di Vienna sul diritto dei

trattati (RS 0.111), entrambe le parti contraenti sono direttamente tenute al rispetto del principio di specialità. Se invece l'assistenza amministrativa si basa esclusivamente sull'art. 55 cpv. 1 lett. b LPD, l'IFPDT deve espressamente richiamare l'attenzione dell'autorità straniera di protezione dei dati richiedente sul principio di specialità e sui limiti entro i quali possono essere utilizzate le informazioni o i dati personali trasmessi.

Ai fini dell'ammissibilità, il principio di specialità presuppone che l'autorità di protezione dei dati richiedente indichi lo scopo per il quale sono necessarie le informazioni o i dati personali richiesti. Da tale principio deriva quindi un **obbligo di motivazione**. 58

La verificabilità e l'**applicabilità** del principio di specialità sono tuttavia limitate. Se un'autorità straniera di protezione dei dati viola il principio di specialità, l'IFPDT può rifiutare future richieste di assistenza amministrativa da parte di tale autorità, motivando che non sussiste una garanzia sufficiente del rispetto del principio di specialità. A parte ciò, si deve presumere che l'applicazione debba avvenire regolarmente da parte della persona interessata e tramite la tutela individuale dei diritti. Ciò vale nel caso in cui i dati personali dell'interessato vengano effettivamente utilizzati in un procedimento successivo a seguito di un riutilizzo non consentito, ossia in un procedimento che non si basa sulla richiesta di assistenza amministrativa originaria e per il quale i dati personali non sono stati trasmessi. In tal caso, l'interessato dovrebbe contestare la trasmissione non consentita nell'ambito del procedimento in questione. La possibilità di farlo dipende in particolare dal diritto processuale applicabile (eventualmente straniero). 59

3. Principio di riservatezza (lett. c)

L'articolo 55 cpv. 1 lettera c LPD è incentrato sulla tutela di particolari interessi di riservatezza. La disposizione richiede infatti che l'autorità richiedente si impegni a proteggere tali segreti. La **portata e il contenuto** dei segreti da tutelare risultano dalle disposizioni penali pertinenti e dalla giurisprudenza in materia. Per il segreto professionale si rimanda all'art. 321 CP, per il segreto di fabbrica e commerciale all'art. 162 CP e all'art. 273 CP. 60

Sono soggetti al **segreto professionale** in particolare i sacerdoti, gli avvocati, i medici, i dentisti, i farmacisti, le ostetriche e gli psicologi. 61

62 Il concetto di segreto è inteso in senso lato in relazione ai **segreti commerciali**; non esiste una definizione giuridica. Secondo la giurisprudenza del Tribunale federale, non sono considerati segreti i fatti noti o accessibili al pubblico (relativa sconosciutezza) di cui il detentore del segreto ha un interesse legittimo a mantenere la riservatezza (interesse oggettivo alla riservatezza) e che il detentore del segreto desidera mantenere segreti per motivi legittimi (interesse soggettivo alla riservatezza). I segreti commerciali sono informazioni che potrebbero compromettere il successo commerciale dell'impresa o falsare la concorrenza se fossero rese note alle imprese concorrenti. Sono quindi considerati segreti commerciali tutti i fatti tecnici, organizzativi, commerciali e finanziari della vita economica che possono influenzare il successo commerciale del titolare del segreto.

63 I **segreti di fabbricazione** devono essere trattati allo stesso modo dei segreti commerciali: essi riguardano in particolare l'aspetto tecnico della produzione, ovvero le conoscenze che contengono istruzioni per l'azione tecnica. Si tratta quindi di conoscenze utilizzate nella fabbricazione di prodotti che non sono riconoscibili nel prodotto venduto e che sono quindi suscettibili di essere tenute segrete. Ciò include, ad esempio, informazioni sui processi e sulle istruzioni di fabbricazione, produzione o costruzione, nonché i risultati della ricerca, i piani di produzione e di costruzione o le fonti di approvvigionamento.

64 Gli **obblighi di riservatezza** previsti dalla legge non ostacolano *di per sé* la divulgazione alle autorità straniere di protezione dei dati. L'articolo 55 cpv. 1 lettera c LPD chiarisce che tali informazioni possono essere comunicate a condizione che l'autorità di protezione dei dati richiedente rispetti il segreto professionale e i segreti commerciali e di fabbricazione (cfr. N. 77 segg.); l'articolo 55 LPD consente quindi una deroga all'obbligo legale di segretezza. L'art. 55 cpv. 3 LPD obbliga tuttavia l'IFPDT a richiedere il parere dei titolari del segreto interessati prima di comunicare informazioni che potrebbero contenere segreti professionali, commerciali o di fabbricazione (cfr. N. 78). Ciò dimostra che occorre sempre valutare l'interesse alla comunicazione delle informazioni rispetto all'interesse alla riservatezza.

4. Principio della lunga mano (lett. d)

65 Ai sensi dell'art. 55 cpv. 1 lett. d LPD, le informazioni e i dati personali possono essere comunicati **a terzi**, comprese altre autorità, solo se l'autorità

di protezione dei dati interpellata ha preventivamente autorizzato tale trasmissione. Per terzi si intendono in primo luogo le autorità terze dello Stato richiedente che non partecipano allo scambio tra l'IFPDT e l'autorità di protezione dei dati straniera.

Il **requisito dell'autorizzazione** protegge le persone interessate da un'ulteriore divulgazione delle informazioni o dei dati personali che le riguardano. Esso garantisce inoltre che l'IFPDT mantenga il controllo sulle informazioni e sui dati personali. In caso di particolare interesse, prima di autorizzare la trasmissione è necessario sentire la persona interessata; inoltre, devono essere rispettati gli altri diritti delle parti. Ciò vale in particolare per la comunicazione di dati personali. Per il resto si rimanda alle considerazioni relative alla tutela giuridica (cfr. N. 37 segg.). 66

L'IFPDT deve ottenere una **garanzia** in tal senso dall'autorità straniera di protezione dei dati. Egli può rinunciare a tale garanzia se il divieto di comunicazione a terzi è già efficacemente garantito da un'altra base giuridica, come un trattato internazionale. 67

5. Rispetto delle condizioni e delle restrizioni (lett. e)

Ai sensi dell'art. 55 cpv. 1 lett. e LPD, l'autorità richiedente deve rispettare le condizioni e le restrizioni imposte dall'autorità che le ha trasmesso le informazioni e i dati personali. Questa disposizione consente la comunicazione di informazioni e dati personali nei casi in cui, senza la possibilità di imporre condizioni o restrizioni come l'**anonimizzazione**, una richiesta di assistenza amministrativa dovrebbe essere respinta. 68

Poiché nell'ambito dell'assistenza amministrativa l'IFPDT è vincolato dall'art. 36 cpv. 6 LPD e tale disposizione subordina già la comunicazione di dati personali alla possibilità di imporre condizioni e restrizioni, la lett. e costituisce essenzialmente una ripetizione. La disposizione chiarisce tuttavia che anche nell'ambito dell'assistenza amministrativa internazionale l'IFPDT deve basare la comunicazione di dati personali su una **valutazione caso per caso** tra l'interesse all'assistenza amministrativa e gli interessi contrapposti ai sensi dell'articolo 36 cpv. 6 LPD. 69

III. COMUNICAZIONE DI DATI PERSONALI (CAPOVERSO 2)

70 L'articolo 55 capoverso 2 LPD stabilisce quali informazioni l'IFPDT può comunicare all'autorità straniera di protezione dei dati per motivare la sua richiesta di assistenza amministrativa o per soddisfare la richiesta di un'autorità straniera di protezione dei dati. L'elenco non è **esaustivo**, come si evince dalla formulazione «in particolare» nella frase introduttiva. In altre parole, l'IFPDT può fornire anche altre informazioni per motivare la sua richiesta di assistenza amministrativa o per soddisfare una richiesta di assistenza amministrativa di un'autorità estera.

71 Secondo la disposizione, l'IFPDT può fornire informazioni sull'**identità** del responsabile del trattamento, del subincaricato o di altri terzi coinvolti (lett. a) nonché sulle **categorie** di persone interessate (lett. b). La menzione delle categorie serve a classificare le persone in gruppi tipizzati che presentano determinate caratteristiche comuni. Nel messaggio vengono citati come esempi di tali categorie, tra l'altro, «consumatori», «militari» o «lavoratori».

72 L'IFPDT può comunicare l'**identità delle persone interessate** solo se queste hanno dato il loro consenso (lett. c n. 1). Si ha divulgazione dell'identità già quando una persona è identificabile. Ciò può risultare dai dati stessi. L'identità è tuttavia identificabile già quando risulta senza uno sforzo proporzionato dal contesto dei dati o dalla combinazione con altri dati.

73 Per la divulgazione dell'identità è necessario il **consenso** di ogni singola persona interessata. In caso contrario, la divulgazione non è ammessa. Per un consenso legalmente valido si applicano i requisiti di cui all'art. 6 cpv. 6 e cpv. 7 LPD. Il consenso è quindi valido solo se è stato dato volontariamente, dopo un'adeguata informazione, in relazione alla divulgazione concreta. Un'adeguata informazione comprende i dati relativi al responsabile, lo scopo o la finalità, le modalità e la portata del trattamento dei dati, le categorie di dati trattati e le informazioni relative alla trasmissione dei dati. Il consenso non è vincolato ad alcuna forma e quindi non è necessario che sia espresso per iscritto. Tuttavia, in caso di comunicazione di dati personali particolarmente sensibili ad autorità straniere di protezione dei dati, il consenso deve essere espresso in modo esplicito. Secondo il messaggio relativo alla LPD, una dichiarazione di volontà è esplicita «[...] se è espressa per iscritto o oralmente o mediante un segno e se la volontà espressa risulta immediatamente dalle parole o dal segno utilizzati».

Il consenso è fondamentale nel trattamento dei dati da parte di privati, perché serve a giustificare una violazione della personalità. Indipendentemente dal consenso, l'IFPDT rimane comunque il destinatario dei diritti fondamentali. La comunicazione dell'identità alle autorità straniere di protezione dei dati deve quindi continuare a servire un interesse pubblico ed essere proporzionata, al fine di poter essere giustificata, in quanto costituisce una violazione dell'articolo 13 capoverso 2 Cost. (cfr. N. 34 seg.). Il requisito del consenso non funge quindi da giustificazione per il trattamento dei dati da parte di organi federali come l'IFPDT, ma da **ulteriore ostacolo** alla divulgazione. 74

In via eccezionale, l'IFPDT può comunicare l'identità delle persone interessate se tale comunicazione è **indispensabile** per l'adempimento del compito legale dell'IFPDT o dell'autorità straniera di protezione dei dati (lett. c n. 2). La disposizione eccezionale è formulata in modo analogo all'art. 36 cpv. 2 lett. a e b LPD, che stabilisce tali requisiti per l'assistenza amministrativa nazionale, purché non esista una base legale speciale. Indispensabilità significa che il compito non può essere adempiuto senza la comunicazione dei dati. 75

Inoltre, l'IFPDT può fornire informazioni sui dati personali trattati o sulle categorie di dati personali trattati (lett. d), sullo scopo del trattamento (lett. e), sui destinatari e sulle categorie di destinatari (lett. f) e sulle misure tecniche e organizzative (lett. g). 76

IV. OBBLIGO DI INFORMAZIONE E PRESA DI POSIZIONE (CPV. 3)

L'articolo 55 capoverso 3 LPD obbliga l'IFPDT, nell'ambito di una procedura di assistenza amministrativa, a comunicare a un'autorità straniera di protezione dei dati informazioni che possono contenere **segreti professionali, commerciali o di fabbricazione** solo dopo aver dato alle persone interessate la possibilità di prendere posizione. Possono essere interessate sia persone fisiche che giuridiche. Contrariamente a quanto richiesto nella consultazione, il legislatore non ha subordinato la comunicazione dei segreti commerciali e di fabbricazione al consenso della persona interessata. 77

78 Lo scopo della disposizione è quello di tutelare i diritti delle persone interessate che sono detentrici di segreti professionali, commerciali o di fabbricazione. A tal fine, il capoverso 3 prevede un **obbligo di informazione e un diritto di essere sentite**. Prima di comunicare a un'autorità straniera di protezione dei dati informazioni che potrebbero contenere segreti professionali, commerciali o di fabbricazione, l'IFPDT deve informare le persone interessate che detengono tali segreti della possibile divulgazione. L'IFPDT è quindi tenuto a richiedere il parere delle persone interessate. Ciò consente alle persone interessate di esporre il proprio punto di vista all'IFPDT in una presa di posizione e di motivare perché le informazioni che riguardano segreti professionali, commerciali o di fabbricazione non devono essere comunicate all'autorità straniera di protezione dei dati.

79 Informando preventivamente le persone interessate e dando loro la possibilità di esprimere il proprio parere, l'IFPDT contribuisce a garantire che i loro interessi siano presi in considerazione e che i loro segreti siano protetti. Il parere deve essere preso in considerazione nel processo decisionale dell'IFPDT, ma non ha **alcun effetto vincolante**: il cpv. 3 non obbliga l'IFPDT a seguire il contenuto dei pareri delle persone interessate. Ha tuttavia il dovere di prendere atto delle osservazioni e di attribuirvi grande importanza nel processo decisionale. Quanto più sono interessati i segreti professionali, commerciali o di fabbricazione del detentore del segreto, tanto maggiore deve essere il peso attribuito alle osservazioni delle persone interessate.

80 Secondo Gerschwiler, le persone interessate devono essere informate già quando si può presumere con una **certa probabilità** che potrebbero essere divulgati segreti professionali, commerciali o di fabbricazione. Ciò è condivisibile. La protezione dei segreti professionali, commerciali e di fabbricazione può essere garantita in modo efficace solo se l'IFPDT non informa solo quando è certo che sono coinvolti segreti protetti dal diritto penale. Per poter tenere conto in modo efficace degli interessi dei detentori dei segreti e coinvolgerli tempestivamente nel processo decisionale attraverso la possibilità di presentare osservazioni, è necessario applicare un criterio generoso. Ciò può anche contribuire a evitare ricorsi successivi.

81 In via eccezionale, l'IFPDT non è tenuto a richiedere un parere alle persone interessate. Ciò avviene quando non è possibile ottenere un parere o quando ciò comporterebbe uno sforzo sproporzionato. Questa eccezione è stata evidentemente introdotta per motivi pratici e mira a evitare che la

comunicazione delle informazioni alle autorità straniere di protezione dei dati venga compromessa qualora la richiesta di un parere sia impossibile o comporti uno sforzo sproporzionato. Poiché con la comunicazione l'IFPDT interferisce con i segreti professionali, commerciali o di fabbricazione delle persone interessate, tutelati dal diritto penale, non si deve presumere affrettatamente che ciò sia **impossibile o irragionevole**. Tuttavia, la procedura ammissibile dovrà essere determinata in ultima istanza dalla giurisprudenza.

BIBLIOGRAFIA

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.

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 57 LPD

Un commentario di Myriam Christ

CITAZIONE SUGGERITA

Myriam Christ, Kommentierung zu Art. 57 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Christ, N. XXX zu Art. 57 DSG.

Art. 57 Informazione

[1] L'IFPDT presenta annualmente all'Assemblea federale un rapporto d'attività. Lo trasmette contemporaneamente al Consiglio federale. Il rapporto è pubblicato.

[2] Nei casi d'interesse generale, l'IFPDT informa il pubblico sui suoi accertamenti e sulle sue raccomandazioni.

STRUTTURA

In breve 739
I. Aspetti generali 739
A. Scopo della disposizione e contesto 739
B. Storia delle origini 740
C. Diritto comparato 742
II. Cpv. 1: Pubblicazione annuale del rapporto di attività 743
A. Pubblicazione annuale 743
B. Rapporto di attività 743
III. Cpv. 2: Pubblicazione di risultati e decisioni di interesse generale 746
A. Determinazione 746
B. Decreto 747
C. Interesse generale 747
D. Pubblicazione 748
Bibliografia 750
I Materiali 752

IN BREVE

La disposizione sulle relazioni pubbliche dell'IFPDT è una delle più importanti ma meno conosciute della legge sulla protezione dei dati. Già negli anni Ottanta, l'esperienza internazionale ha dimostrato che il successo dell'attuazione della legislazione sulla protezione dei dati richiede un dialogo tra l'autorità di controllo e le altre autorità federali o la popolazione civile (ad esempio, quando si tratta di evidenziare la necessità di un intervento legislativo o di esercitare pressioni su determinati responsabili del trattamento dei dati che non rispettano i requisiti di legge).

L'art. 57 cpv. 1 LPD obbliga l'IFPD a informare una volta all'anno l'Assemblea federale - organo elettivo dell'IFPD ai sensi dell'art. 43 cpv. 1 LPD - sulle sue attività. Il Consiglio federale viene informato per iscritto delle attività della DFP. Il secondo paragrafo mira a consentire al DFP di svolgere il suo mandato di informazione in modo indipendente dalle autorità federali controllate. La disposizione è formulata in modo molto aperto. L'IFPDT ha quindi numerose possibilità di esercitare il suo mandato legale di informazione.

I. ASPETTI GENERALI

A. Scopo della disposizione e contesto

L'art. 57 LPD non è una delle disposizioni più conosciute della LPD. Tuttavia, questa disposizione giuridica relativa alle relazioni pubbliche dell'IFPDT contribuisce in modo decisivo all'attuazione pratica dei requisiti della legge sulla protezione dei dati. In effetti, la sensibilizzazione alla legge sulla protezione dei dati sia nel settore privato che in quello pubblico avviene principalmente grazie all'attività di pubbliche relazioni dell'IFPDT (e dei commissari cantonali e comunali per la protezione dei dati). Per riuscire a sensibilizzare l'opinione pubblica sulla protezione dei dati è necessario un dialogo tra l'autorità di controllo e il pubblico. Le considerazioni o le misure in materia di protezione dei dati non dovrebbero quindi rimanere puramente interne alle agenzie di trattamento dei dati, sia nel settore privato che in quello pubblico, ma dovrebbero essere portate all'attenzione del pubblico in modo consapevole e proattivo. 1

2 La campagna di sensibilizzazione condotta dall'IFPDT persegue diversi obiettivi specifici. Da un lato, contribuisce a rafforzare l'efficacia delle attività di vigilanza della LPD (artt. 49-53 LPD): nell'ambito delle sue attività di vigilanza, la LPD può sanzionare il trattamento illecito dei dati. In base all'art. 57 LDP, può pubblicare le sue conclusioni e quindi esercitare pressione sul responsabile del trattamento dei dati che ha commesso l'errore, nonché incoraggiare altri responsabili del trattamento dei dati non direttamente interessati dall'indagine ad adeguare le loro pratiche. D'altro canto, l'attività di pubbliche relazioni dell'IFPD può sollevare in modo decisivo l'IFPD dal suo ruolo consultivo (art. 58 LPD). La pubblicazione di ausili facilmente comprensibili, come linee guida, lettere esemplificative o FAQ, contribuisce in modo decisivo a ridurre lo sforzo necessario per la consultazione personale e a prevenire potenziali violazioni della protezione dei dati.

3 Inoltre, sulla base della sua attività di pubbliche relazioni, l'IFPDT può rendere conto delle sue attività all'organo elettorale (Assemblea federale ai sensi dell'art. 43 cpv. 1 LPD) e quindi fornire all'Assemblea federale una panoramica sull'adempimento dei suoi compiti.

4 L'attività di pubbliche relazioni ai sensi dell'art. 57 LPD offre poi alla DFP la possibilità di pubblicare informazioni sugli sviluppi problematici e di segnalare ciò che ritiene necessario per un intervento legislativo.

5 In questo caso, va notato che l'applicazione individuale dei diritti attraverso i tribunali civili prevista dal legislatore (art. 32 cpv. 2 LPD) ha un ruolo subordinato o (quasi) nullo nella pratica. A fronte di procedimenti lunghi e costosi dall'esito incerto, le persone interessate avviano solo molto raramente un procedimento presso il tribunale competente. Ciò è tanto più vero in quanto sempre più trattamenti di dati vengono effettuati da privati all'estero. Ciò rende (quasi) impossibile intentare una causa promettente davanti a un tribunale civile svizzero. Di conseguenza, le questioni fondamentali della protezione dei dati sono raramente affrontate nella giurisprudenza e le poche decisioni dei tribunali hanno un significato limitato al di là del singolo caso. Grazie al suo lavoro di pubbliche relazioni, l'IFPDT svolge quindi un ruolo importante nell'applicazione della legge.

B. Storia delle origini

Cpv. 1:

Una disposizione molto simile all'attuale cpv. 1 era già contenuta nell'art. 30 aDSG. Sulla base dell'esperienza internazionale, che già negli anni '80 aveva dimostrato che la consapevolezza della legge sulla protezione dei dati è rafforzata, tra l'altro, dal lavoro di pubbliche relazioni delle autorità di protezione dei dati, questa disposizione è stata incorporata nella legge svizzera nel 1988 ed è entrata in vigore nel 1992. 6

L'art. 30a LPD non ha dato luogo a dibattiti in Parlamento - l'articolo corrispondeva al progetto del Consiglio federale del 1988. Ciò vale anche per l'art. 57 LPD. Nell'ambito della revisione, la disposizione è stata chiarita solo nella misura in cui la DFP deve ora presentare un rapporto annuale (e non più periodico). Questa precisazione corrisponde alla prassi della vecchia legge. 7

L'IFPDT riferisce all'Assemblea federale, fornendo così all'organo elettorale una panoramica sull'esercizio delle sue funzioni. Come nella vecchia legge, il Consiglio federale riceve solo il rapporto di attività scritto. 8

Inoltre, l'espressione "nonché quando necessario" è stata eliminata. D'ora in poi, l'IFPDT riferirà una volta all'anno. Né la valutazione della consultazione né il messaggio tengono conto di questa soppressione. In pratica, la possibilità di informare il pubblico anche quando necessario (cioè in qualsiasi momento e non solo una volta all'anno) non ha avuto un ruolo importante. Inoltre, va sottolineato in questo contesto che l'IFPD può informare il pubblico sulle sue attività sulla base dell'art. 57 cpv. 2 LPD, se necessario. 9

Cpv. 2:

L'art. 57 cpv. 2 LPD è stato abbreviato nella revisione rispetto al cpv. 2 della vecchia LPD. Nello spirito della maggiore indipendenza dell'IFPDT, auspicata già nel dicembre 2011, l'IFPDT può ora decidere autonomamente su cosa informare il pubblico. La pubblicazione di dati personali soggetti a segreto d'ufficio non dipende più dal consenso dell'autorità interessata e non è più prevista una distinzione esplicita tra dati personali e dati fattuali nell'ambito del mandato informativo della DFP. 10

Il secondo paragrafo stabilisce inoltre che l'IFPDT "informa" e non semplicemente "può informare" su risultati di interesse generale. Questo chiarimento linguistico è apprezzabile, ma cambia poco nella pratica. La disposizione "può" prevista dalla vecchia legge stabiliva già un mandato di informazione vincolante. 11

C. Diritto comparato

Ad cpv. 1:

12 La preparazione periodica di un rapporto di attività era già prevista dall'art. 28, paragrafo 5, della direttiva 95/46/CE ed è disciplinata dall'art. 59 del DSGVO dal 25 maggio 2018. In termini di contenuto, questa disposizione si differenzia dall'art. 57 cpv. 1 DPA in quanto la corrispondente norma di diritto europeo specifica un possibile contenuto del rapporto di attività (elenco dei tipi di violazione segnalati e dei tipi di misure adottate ai sensi dell'art. 58 cpv. 2 DPA).

13 L'art. 15 cpv. 7 dell'ETS 108 stabilisce che ogni autorità di vigilanza europea elabora e pubblica regolarmente un rapporto di attività. Secondo la relazione esplicativa, il rapporto di attività deve essere pubblicato una volta all'anno. Tale relazione deve contenere, in particolare, informazioni sulle misure adottate per applicare la legislazione nazionale in materia di protezione dei dati. Ad eccezione del fatto che la LPD rivista non contiene requisiti in termini di contenuto, il legislatore svizzero ha adottato sia i requisiti del Consiglio d'Europa che quelli dell'UE. Va da sé, tuttavia, che le misure adottate per far rispettare le disposizioni in materia di protezione dei dati sono menzionate nel rapporto di attività dell'IFPDT anche in assenza di un corrispondente requisito legale.

Cpv. 2:

14 L'art. 15 cpv. 2 lett. e ETS 108 definisce il quadro dei compiti di sensibilizzazione delle autorità di vigilanza. Secondo la relazione esplicativa, le autorità di vigilanza devono rendere visibili in modo proattivo le misure che adottano, i loro compiti e le loro competenze. A tal fine, possono pubblicare relazioni periodiche sulle attività (cfr. art. 15 cpv. 7 ETS 108), dichiarazioni o raccomandazioni generali. Possono anche sensibilizzare il pubblico attraverso altri canali di comunicazione liberamente selezionabili. Secondo la relazione esplicativa, l'attività di pubbliche relazioni comprende anche l'informazione delle persone e dei responsabili del trattamento dei dati sui rispettivi diritti e obblighi in un linguaggio appropriato e facilmente comprensibile (soprattutto se il trattamento dei dati riguarda bambini o altre persone particolarmente vulnerabili).

II. CPV. 1: PUBBLICAZIONE ANNUALE DEL RAPPORTO DI ATTIVITÀ

A. Pubblicazione annuale

Nel contesto della revisione, l'art. 30 aDSG è stato leggermente chiarito: la pubblicazione deve avvenire "annualmente". Questa precisazione è stata richiesta nella consultazione, ma cambia poco nella pratica. La legge non contiene ancora alcuna indicazione sul momento della pubblicazione. Secondo la vecchia legge, era consuetudine che il rapporto coprisse il periodo tra il 1° aprile e il 31 marzo dell'anno successivo e venisse pubblicato alla fine di giugno. In occasione di ogni pubblicazione si tiene una conferenza stampa. L'FDPIC presenta il rapporto di persona, spesso accompagnato da un altro membro della direzione, e risponde alle domande dei media. Non ci sono indicazioni che questa pratica non continuerà con la nuova legge. 15

Il rapporto non viene sottoposto al Consiglio federale o all'Assemblea federale per eventuali adeguamenti, né prima né dopo la pubblicazione. In altre parole, il rapporto viene pubblicato nello stesso modo in cui viene presentato all'Assemblea federale e al Consiglio federale (cfr. le specifiche dell'art. 37 LDP a questo proposito). Tra l'altro, l'IFPDT esercita anche la vigilanza sul trattamento dei dati effettuato dagli organi federali. È quindi ipotizzabile che, a seconda dei risultati dell'indagine, gli organi federali controllati in base al diritto di vigilanza possano richiedere determinati adeguamenti del rapporto di attività. In questo contesto, la pubblicazione del rapporto di attività invariato è da accogliere con favore e contribuisce a rafforzare l'indipendenza dell'IFPDT. 16

Non è prevista la presentazione del rapporto di attività davanti alla commissione incaricata di preparare l'elezione dell'IFPDT o nei consigli, anche se ciò è occasionalmente richiesto dalla dottrina. 17

B. Rapporto di attività

Il rapporto di attività è il fulcro del lavoro di pubbliche relazioni dell'IFPD (cfr. art. 57 cpv. 2 e art. 58 LPD per ulteriori modalità di sensibilizzazione dell'opinione pubblica). 18

19 A differenza del diritto europeo - ossia l'art. 59 DSGVO e l'art. 15 cpv. 7 STEP 108 - in Svizzera né la LPD né la LDP impongono requisiti di contenuto. L'IFPDT è quindi in linea di principio libero di decidere il contenuto del rapporto di attività. Ai sensi dell'art. 58 cpv. 1 lett. f LPD, l'Incaricato della protezione dei dati svolge anche i compiti assegnatigli dalla Legge sull'informazione del pubblico del 17 dicembre 2004 (LTras, RS 152.3). Ai sensi dell'art. 19 LTras, l'Incaricato della protezione dei dati deve presentare regolarmente un rapporto al Consiglio federale e pubblicarlo. Dall'entrata in vigore della LTras, il 1° luglio 2006, l'IFPDT pubblica un rapporto di attività che ripercorre sia le sue attività di incaricato della protezione dei dati sia i suoi compiti di incaricato della pubblica informazione.

20 Il rapporto di attività segue una struttura simile di anno in anno, anche se la ponderazione delle singole aree tematiche può variare: Sfide attuali, Protezione dei dati (Digitalizzazione e diritti fondamentali; Giustizia, polizia, sicurezza; Fisco e finanze; Commercio ed economia; Salute; Lavoro; Assicurazioni; Trasporti; Internazionale), Principio pubblico (Generale; Richieste di accesso; Procedure di conciliazione; Procedure legislative), l'IFPDT (Compiti e risorse; Comunicazione; Statistiche; Organizzazione dell'IFPDT). L'FDPIC stabilisce anche diverse priorità tematiche per ogni rapporto di attività. Ad esempio, nel rapporto di attività 2020/2021 ha dedicato la prima attenzione alla revisione della LPD e la seconda al Privacy Shield e alle sfide ad esso associate.

21 Come tutte le autorità federali, l'IFPDT deve rispettare le disposizioni di legge applicabili nell'adempimento dei suoi compiti statutari, in particolare quelli relativi alla protezione dei segreti industriali e commerciali. Inoltre, è soggetto al segreto d'ufficio ai sensi dell'art. 22 della Legge sul personale federale (LFPr, RS 172.220.1). Di conseguenza, deve garantire il trattamento riservato dei dati personali a cui ha accesso nell'esercizio delle sue funzioni di vigilanza, in particolare quando pubblica il suo rapporto di attività.

22 Data la natura molto breve degli articoli del rapporto di attività (secondo la vecchia legge, circa una colonna per ogni indagine di vigilanza), è difficile immaginare - a differenza della pubblicazione delle sentenze - che nel rapporto di attività vengano rivelati segreti di fabbricazione o commerciali.

23 In pratica, l'IFPDT rende anonimi i nomi dei privati contro i quali è stato avviato un procedimento di vigilanza, ma non ancora concluso. Non appena il

procedimento è concluso, la persona giuridica interessata viene nominata nel successivo rapporto di attività. L'indicazione delle aziende colpevoli può non essere sempre piacevole per le persone interessate, ma non rientra nei segreti di fabbricazione o commerciali. Inoltre, l'indicazione del colpevole rientra nello scopo dell'art. 57 cpv. 1 LPD, poiché uno degli scopi dell'attività di pubbliche relazioni dell'IFPD è quello di esercitare pressione sul colpevole e di incoraggiare gli altri responsabili della protezione dei dati non direttamente interessati dall'indagine ad adeguare le loro pratiche.

La situazione è diversa nel caso dei segreti ufficiali, che possono essere divulgati anche su una sola riga. In questi casi, tuttavia, è probabile che prevalga l'interesse pubblico a informare l'opinione pubblica sul trattamento illecito dei dati da parte delle autorità federali, anche in considerazione della responsabilità storica dell'IFPDT dopo lo scandalo della Fiche (cfr. le osservazioni seguenti sull'art. 57 cpv. 2 LPD). 24

La legge non prevede inoltre alcuna disposizione in merito alla forma del rapporto di attività. La concezione e la diffusione sono quindi stabilite autonomamente dalla DFP. Il rapporto di attività non viene espressamente pubblicato nella veste grafica interna all'Amministrazione federale. L'indipendenza dell'IFPDT è quindi espressa anche formalmente. 25

A causa dell'obiettivo del rapporto, il rapporto di attività deve essere un documento accessibile al pubblico. L'IFPDT pubblica il rapporto come e-paper gratuito sul suo sito web; il rapporto stampato può essere ordinato per CHF 17.00 presso l'Ufficio federale delle costruzioni e della logistica. 26

Dal 2017/2018, il rapporto è stato pubblicato anche in italiano e in inglese. Tra il 1993 e il 2017, il rapporto è stato pubblicato solo in tedesco e francese. La mancanza di una traduzione in italiano era una chiara violazione dell'art. 10 della Legge federale sulle lingue nazionali e la comunicazione tra le comunità linguistiche (RS 441.1). Anche se questa legge federale non richiede la pubblicazione in inglese, è positivo che da alcuni anni il rapporto di attività venga pubblicato anche in inglese. Questa nuova traduzione semplifica la consultazione personale dell'IFPDT, dato che le persone di lingua inglese chiedono sempre più spesso all'IFPDT la sua consulenza legale. Il riferimento alla versione in inglese del rapporto di attività contribuisce a rendere più efficienti queste consultazioni in lingua straniera. 27

28 I destinatari del rapporto di attività sono l'Assemblea federale in quanto organo elettivo dell'IFPDT, i Consiglieri federali in quanto responsabili dei singoli dipartimenti, che svolgono innumerevoli operazioni di trattamento dei dati, e il pubblico in generale (professionisti dei media, consulenti legali, tecnici e popolazione civile in generale). In altre parole, l'art. 57 cpv. 1 LPD si applica a tutte le attività dell'IFPDT. Questa eterogeneità di destinatari rappresenta una sfida da non sottovalutare nella stesura del rapporto di attività.

29 In questo contesto, per completezza, va notato che le sfide in materia di protezione dei dati che si presentano nel settore privato e in quello pubblico sono spesso di natura simile. Per questo motivo, può essere istruttivo leggere i rapporti di attività dei commissari cantonali per la protezione dei dati, che sono obbligati dalla legge cantonale a pubblicare i rapporti di attività.

III. CPV. 2: PUBBLICAZIONE DI RISULTATI E DECISIONI DI INTERESSE GENERALE

A. Determinazione

30 "Determinazione" non è un termine giuridico chiaramente definito, ma descrive in modo esaustivo il mandato informativo giuridicamente vincolante dell'IFPDT.

31 Fatti di interesse generale rilevanti per la legge sulla protezione dei dati possono essere portati all'attenzione dell'IFPDT attraverso i media, la hotline o il modulo di contatto, o negli scambi con altre autorità federali o cantonali. La misura in cui l'IFPDT desidera reagire a un'informazione identificata è a sua discrezione, in particolare in termini di tempistica e canale di informazione.

32 Il termine "determinazione", giuridicamente confuso, offre il vantaggio di poter reagire a una (possibile) violazione della LPD in modo più flessibile e rapido rispetto all'emissione di un ordine. Inoltre, questo termine confuso offre la possibilità di informare il pubblico su una questione rilevante per la legge sulla protezione dei dati anche se non sono soddisfatte le condizioni per avviare un'indagine ai sensi dell'art. 49 LPD.

Resta da vedere se e con quale frequenza verranno pubblicati i risultati in futuro. Come per tutti i termini giuridicamente confusi, l'interpretazione di questo termine dipende dal rispettivo IFPDT. 33

B. Decreto

L'IFPDT può ora emanare ordinanze (cfr. artt. 49-51 LPD). Durante il processo di consultazione, alcuni partecipanti della comunità imprenditoriale hanno chiesto che l'IFPDT non pubblichi le sue sentenze, ma solo i fatti per i quali è stata aperta un'indagine. Questi partecipanti ritenevano che questo fosse l'unico modo per garantire i diritti personali delle persone interessate. Singoli partecipanti, invece, ritenevano che tutte le sentenze dell'IFPDT dovessero essere pubblicate. La regola stabilita dalla legge rappresenta quindi un compromesso e consente all'IFPDT di soppesare eventuali segreti d'ufficio o d'affari nei singoli casi con l'interesse generale a chiarire fatti illeciti. In linea di principio, l'interesse generale deve essere interpretato in senso ampio, in considerazione degli obiettivi dell'attività di pubbliche relazioni dell'IFPDT. 34

C. Interesse generale

Il concetto di "interesse generale" non è definito né nella LPD riveduta, né nella LPD riveduta, né nel messaggio del 2017. Nemmeno il precedente messaggio sulla vecchia LPD definiva il termine. All'epoca il Consiglio federale forniva solo un esempio: la pubblicazione di una raccomandazione su un sistema d'informazione di importanza nazionale era di interesse generale. La dottrina cita altri esempi più attuali: il trattamento dei dati in questione rappresenta una situazione di rischio particolare per i diritti fondamentali e i diritti personali delle persone interessate, riguarda l'attuazione generale della LPD, ha carattere di precedente o è ampiamente discusso in pubblico. Inoltre, secondo Rosenthal/Jöhri, la pubblicazione di reclami accertati (senza ulteriori specificazioni) può essere di interesse pubblico. A causa dell'attuale mercato digitale, anche la pubblicazione di una violazione della LPD da parte di un leader di mercato può essere di interesse pubblico. In ogni caso, il termine deve essere interpretato in modo ampio anche in base alla legge rivista. In caso contrario, l'IFPDT potrebbe svolgere la sua attività di pubbliche relazioni solo in modo inadeguato. 35

36 Di norma, le informazioni di interesse generale hanno una certa urgenza e si discostano dalla normale attività di informazione. Se non c'è urgenza, queste informazioni possono essere pubblicate nel prossimo rapporto di attività.

37 Le informazioni di interesse generale che devono essere pubblicate dipendono, tra l'altro, dalla priorità delle attività in corso in base alle risorse umane disponibili. Anche se è vero che l'Assemblea federale ha creato ulteriori posti con l'entrata in vigore della nuova LPD, l'IFPDT rimane cronicamente sotto organico. Pertanto, è possibile che i risultati che sarebbero di interesse generale continuino a essere pubblicati in ritardo o non vengano pubblicati affatto.

D. Pubblicazione

38 Come nella vecchia legge, il momento della pubblicazione può essere scelto liberamente. La questione del momento della pubblicazione non è sempre ugualmente importante. Tuttavia, se la pubblicazione di un accertamento viene utilizzata come mezzo di pressione, la pubblicazione strategica in termini di tempo è decisiva.

39 La LPD non prevede requisiti formali per l'attività di pubbliche relazioni dell'FDPIC. Il canale di comunicazione è quindi liberamente selezionabile anche in base alla nuova legge. In passato, l'IFPDT ha pubblicato sul proprio sito web lettere esemplificative, contratti esemplificativi, linee guida, schede informative e FAQ. Inoltre, redige pareri amministrativi interni. Inoltre, l'IFPDT tiene discorsi su argomenti di attualità, pubblica articoli scritti su riviste specializzate e rilascia interviste ai media. Il dipartimento di comunicazione gestisce un account Twitter (@derBeauftragte) e redige regolarmente comunicati stampa. Diversi membri del personale hanno collaborato alla produzione di un supporto didattico per i giovani. Sono possibili anche campagne più ampie. Indipendentemente dal canale di comunicazione scelto, l'FDPIC deve sempre seguire i principi di una politica di comunicazione professionale per sensibilizzare efficacemente l'opinione pubblica.

40 I risultati pubblicati non hanno la portata giuridica di decreti o leggi. Non sono giuridicamente vincolanti. In caso di controversia, il tribunale adito decide autonomamente, anche se l'interessato ha contattato preventivamente l'IFPDT in qualità di consulente o si è basato su un risultato pubblicato. Il

fatto che il privato abbia seguito il consiglio dell'IFPDT può tuttavia svolgere un ruolo importante nell'esame della colpa nelle azioni di riparazione.

Tuttavia, la pubblicazione delle conclusioni conosce anche dei limiti, stabiliti dall'art. 36 cpv. 6 LPD (interessi pubblici essenziali, interessi della persona interessata manifestamente degni di protezione, obblighi di riservatezza previsti dalla legge o disposizioni speciali in materia di protezione dei dati). Come tutte le autorità federali, l'IFPDT deve rispettare le disposizioni legali applicabili, in particolare quelle relative alla protezione dei segreti industriali e commerciali e quelle che tutelano la sfera confidenziale e privata (diffamazione [art. 173 CP], calunnia [art. 174 CP], ingiuria [art. 177 CP]) nonché il divieto di coercizione (art. 181 CP). Inoltre, è soggetto al segreto d'ufficio ai sensi dell'art. 22 CPC. Di conseguenza, l'IFPDT deve garantire il trattamento riservato dei dati personali a cui ha accesso nell'esercizio delle sue funzioni di controllo. Nulla fa pensare che l'IFPDT modificherà la sua prassi di contattare le persone responsabili interessate prima di una pubblicazione prevista e chiedere se i segreti aziendali o ufficiali debbano essere oscurati prima della pubblicazione. Tuttavia, questo contatto non deve essere confuso con l'ottenimento del consenso. 41

Inoltre, si applica il principio dell'anonimizzazione dei dati personali. Per questo motivo, i dati personali che devono essere pubblicati vengono sempre resi anonimi prima della pubblicazione prevista. I nomi del personale amministrativo di alto livello che agisce nell'esercizio del proprio mandato amministrativo o i nomi di persone private incaricate non godono di alcuna protezione speciale in questo contesto. 42

Esiste un'importante eccezione al principio dell'anonimizzazione. Se l'IFPDT ritiene che la pubblicazione della constatazione o della decisione non oscurata sia nell'interesse pubblico, può ora rinunciare all'anonimizzazione (secondo la vecchia legge, l'IFPDT poteva pubblicare dati personali soggetti al segreto d'ufficio solo con il consenso dell'autorità interessata). Questo sviluppo va accolto con favore, poiché rafforza chiaramente l'indipendenza dell'IFPDT. Con la crescente consapevolezza dell'opinione pubblica sui temi della protezione dei dati, questa revisione della legge non è una sorpresa. In sintesi, si può quindi presumere che il principio dell'anonimizzazione sarà interpretato in modo piuttosto restrittivo e che non tutte le pubblicazioni saranno anonimizzate per principio. 43

44 Per quanto riguarda l'anonimizzazione, va notato che l'anonimizzazione effettiva dei dati personali sta diventando sempre più difficile a causa dei progressi tecnologici. Inoltre, l'anonimizzazione può non essere efficace, soprattutto se la pubblicazione dei risultati viene utilizzata come mezzo di pressione.

45 Sono ovviamente riservate le disposizioni di diritto penale, come la diffamazione, la calunnia, l'ingiuria, la coercizione o l'abuso di autorità. L'FDPIC non gode di alcuna immunità penale e deve rispettare queste disposizioni penali nell'ambito della sua attività di pubbliche relazioni.

46 In questo contesto, va infine ricordato che la LPD si applica solo alla divulgazione o alla pubblicazione di dati personali (cfr. art. 1 LPD o art. 36 LPD). È tuttavia ipotizzabile che l'IFPDT, nell'ambito della sua attività di vigilanza, possa imbattersi in dati di fatto ai sensi dell'art. 5 lett. a). La divulgazione di dati fattuali non è soggetta alla LPD, ma questi dati possono essere protetti dal segreto d'ufficio e la loro divulgazione può quindi essere soggetta alle disposizioni della LPD (ad esempio strategie, piani o misure nel settore della sicurezza informatica). In questi casi, le spiegazioni relative alla divulgazione dei dati personali (art. 36 e segg. LPD) si applicano probabilmente per analogia. La LPD non contiene una disposizione relativa alla liberazione dal segreto d'ufficio dei dati di fatto. Si deve quindi presumere che anche l'IFPDT possa svincolarsi dal segreto d'ufficio in tali costellazioni. È discutibile se ciò corrisponda effettivamente alla volontà legislativa, soprattutto alla luce della situazione politicamente tesa in Europa.

BIBLIOGRAFIA

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).

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 58 LPD

Un commentario di Myriam Christ

CITAZIONE SUGGERITA

Myriam Christ, Kommentierung zu Art. 58 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Christ, N. XXX zu Art. 58 DSG.

Art. 58 Altri compiti

[1] L'IFPDT ha in particolare gli altri compiti seguenti:

a. informare, formare e consigliare gli organi federali e i privati in questioni concernenti la protezione dei dati;

b. assistere gli organi cantonali e collaborare con le autorità svizzere ed estere competenti in materia di protezione dei dati;

c. sensibilizzare il pubblico, soprattutto le persone vulnerabili, alla protezione dei dati;

d. informare, su richiesta, le persone interessate in merito all'esercizio dei loro diritti;

e. pronunciarsi sui progetti di atti normativi e sui provvedimenti della Confederazione implicanti il trattamento di dati;

f. assumere i compiti conferitigli dalla legge del 17 dicembre 2004[21] sulla trasparenza o da altre leggi federali;

g. elaborare strumenti di lavoro sotto forma di raccomandazioni di buona prassi per i titolari del trattamento, i responsabili del trattamento e le persone interessate; a tal fine tiene conto delle specificità di ciascun settore e della tutela delle persone vulnerabili.

[2] L'IFPDT può fornire consulenza anche agli organi federali che secondo gli articoli 2 e 4 non sono sottoposti alla sua vigilanza. Gli organi federali possono concedergli accesso ai loro atti.

[3] L'IFPDT è autorizzato a dichiarare alle autorità estere incaricate della protezione dei dati che, in materia di protezione dei dati, in Svizzera è ammessa la notificazione diretta, sempreché alla Svizzera sia concessa la reciprocità.

STRUTTURA

In breve ... 756
I. Generalità ... 756
A. Scopo della norma e contesto ... 756
B. Storia delle origini ... 757
C. Diritto comparato ... 757
II. Cpv. 1: Compiti speciali dell'FDPIC ... 758
A. Lit. a: Mandato di informazione ... 758
B. Lit. b: Supporto alle autorità cantonali e internazionali ... 760
C. Lit. c: Mandato di sensibilizzazione ... 761
D. Lit. d: mandato di consulenza ... 763
E. Lit. e: consultazione della DFP nel processo legislativo federale ... 764
F. Lit. f: Compiti di LTras ... 765
G. Lit. g: Raccomandazioni di buone prassi ... 765
III. Cpv. 2: mandato esteso di consulenza ... 766
IV. Cpv. 3: Assistenza internazionale reciproca ... 767
Bibliografia ... 767
I Materiali ... 768

IN BREVE

L'elenco dei compiti di cui all'art. 58 LPD completa i compiti dell'IFPD già previsti dall'art. 57 LPD. Ad esempio, questa disposizione prevede che l'IFPDT sensibilizzi l'opinione pubblica sulla protezione dei dati, commenti i progetti di decreti federali o pubblichi raccomandazioni di buone prassi. Tuttavia, l'elenco dei compiti di cui all'art. 58 LPD non è esaustivo. L'IFPD può quindi assumere altri compiti, non specificamente definiti, a condizione che siano coerenti con gli obiettivi fondamentali della LPD.

I. GENERALITÀ

A. Scopo della norma e contesto

1 Secondo la formulazione dell'ingresso ("Inoltre, la DFP svolge in particolare i seguenti compiti"), l'art. 58 LPD deve essere inteso come una disposizione complementare o generale all'art. 57 LPD. L'art. 58 LPD specifica l'ambito delle attività di consulenza e informazione della DFP ai sensi dell'art. 57 LPD, che la DFP stessa determina in larga misura sulla base della propria indipendenza sancita dalla legge.

2 Anche l'elenco dei compiti della DFP non è esaustivo ai sensi della legge riveduta ("in particolare"). La nuova legge lascia quindi un certo margine di manovra per ulteriori compiti, a condizione che non siano in contrasto con lo scopo della LPD. In questo contesto, va notato che ulteriori compiti dell'IFPD sono stabiliti in altre parti della LPD, ad esempio nell'art. 11 LPD (pareri sui codici di condotta), nell'art. 12 cpv. 4 LPD (notifica degli elenchi delle attività di trattamento), nell'art. 16 cpv. 2 LPD (divulgazione dei dati all'estero), nell'art. 23 LPD (consultazione dell'IFPD nel contesto delle valutazioni d'impatto sulla protezione dei dati) o nell'art. 24 LPD (notifica delle violazioni della sicurezza dei dati). Altri compiti dell'IFPDT sono stabiliti in varie leggi speciali, come l'art. 84b LAMal (garanzia della protezione dei dati da parte degli assicuratori) o l'art. 63 cpv. 3 in combinato disposto con l'art. 64 NDG (esame da parte degli assicuratori). Art. 64 NDG (verifica da parte dell'IFPDT della liceità del trattamento dei dati personali della persona che ne fa richiesta).

Per ulteriori informazioni sullo scopo della norma e sul suo contesto, si rimanda alle informazioni generali sull'art. 57 LPD. 3

B. Storia delle origini

Nell'ambito della revisione, l'art. 31 aDSG è stato adattato al diritto dell'UE e ai requisiti del Consiglio d'Europa. Per questo motivo, l'elenco dei compiti dell'IFPDT è stato leggermente adattato o integrato. 4

L'art. 31 cpv. 1 lett. d LPD (protezione adeguata della legislazione sulla protezione dei dati all'estero), l'art. 31 cpv. 1 lett. e LPD (esame delle garanzie per il trasferimento di dati verso Stati non equivalenti) e l'art. 31 cpv. 1 lett. f LPD (procedura di certificazione) non sono stati inclusi nell'art. 58 LPD rivisto. Ora non è più l'IFPDT ma il Consiglio federale o l'UFG a stabilire se la legislazione dello Stato in questione garantisce una protezione adeguata (art. 16 cpv. 1 LPD). L'elenco degli Stati, dei territori, dei settori specifici di uno Stato e delle organizzazioni internazionali che, secondo il Consiglio federale, garantiscono un'adeguata protezione dei dati è ora riportato nell'Appendice 1 della LPD. L'esame delle garanzie per il trasferimento dei dati a uno Stato non equivalente è ora disciplinato in dettaglio all'art. 16 cpv. 2 LPD ed è adottato in linea di principio anche dall'IFPDT ai sensi della nuova legge. La certificazione è ora disciplinata dall'art. 13 LPD. In base al diritto vigente, l'IFPDT non può più esaminare direttamente le procedure di certificazione (art. 31 cpv. 1 lett. f aDSG). In questo contesto è riservata una procedura di vigilanza ai sensi degli artt. 49 e segg. LPD è riservata in questo contesto. 5

Per ulteriori informazioni sulla storia dello sviluppo delle attività di consulenza e informazione delle autorità di controllo della protezione dei dati, si rimanda ai commenti sull'art. 57 LPD. 6

C. Diritto comparato

Nel diritto europeo, i compiti delle rispettive autorità di protezione dei dati sono stabiliti dall'art. 57 DSGVO, fatti salvi gli altri compiti stabiliti nei singoli passaggi della DSGVO. 7

L'art. 58 DSGVO stabilisce i poteri specifici con cui le autorità di controllo possono raggiungere gli obiettivi di cui all'art. 57 DSGVO. 8

9 Gli artt. 57 e 58 DPA vanno chiaramente oltre i "regolamenti fratelli" degli artt. 57 e 58 DPA in termini di livello di dettaglio. Questa attenzione ai dettagli nella legislazione europea sulla protezione dei dati mira a migliorare la certezza del diritto e la protezione dei diritti fondamentali, dopo che la disposizione precedente (art. 28 della direttiva 95/46/CE) forniva solo un quadro di massima, che nella vecchia legge era stato completato in modo molto diverso dalle disposizioni nazionali. A parte le differenze formali (livello di dettaglio e struttura), non si notano differenze fondamentali nel contenuto tra le disposizioni europee e quelle svizzere. Questa constatazione non sorprende: il vecchio elenco di compiti dell'art. 31 aDSG è stato integrato con l'obiettivo esplicito di attuare i requisiti del diritto europeo ai sensi dell'art. 46 cpv. 1 lett. d ed e della Direttiva (UE) 2016/680 e i requisiti dell'art. 12bis n. 2 lett. e E-SEV.

II. CPV. 1: COMPITI SPECIALI DELL'FDPIC

A. Lit. a: Mandato di informazione

10 Nell'ambito della revisione è stato aggiunto alla LPD l'art. 58 cpv. 1 lett. a. Questa nuova disposizione mira a specificare il mandato d'informazione della DFP di cui all'art. 57 LPD.

11 Questa nuova disposizione stabilisce esplicitamente che la DFP svolge il suo mandato di consulenza e informazione non solo nei confronti degli enti pubblici, ma anche dei privati. Questa precisazione linguistica, che corrisponde alla prassi dell'IFPDT sotto la vecchia legge, va accolta con favore.

12 Alla luce della formulazione della legge e del messaggio, l'IFPDT dispone di un ampio margine di discrezionalità per quanto riguarda l'attuazione pratica del mandato d'informazione. In linea di principio, è libero di scegliere quali decisori dell'amministrazione, della politica, della scienza e dell'economia informare, formare o consigliare. Tuttavia, la discrezionalità dell'IFPDT non è priva di limiti: L'indipendenza dell'IFPD deve essere sempre preservata, anche nell'attuazione del mandato di informazione di cui all'art. 58 cpv. 1 lett. a LPD. In pratica, si possono creare costellazioni problematiche se l'IFPDT stesso o i membri della sua direzione mantengono contatti personali troppo stretti con determinati responsabili delle decisioni e questo contatto o scambio crea

l'apparenza di parzialità da parte dell'IFPDT nei confronti di terzi o influenza l'IFPDT in un'eventuale procedura di vigilanza a valle.

Nell'ambito del suo mandato di informazione, l'IFPDT partecipa, ad esempio, 13
alla conferenza annuale sulla legge in materia di protezione dei dati presso l'Università di Friburgo, pubblica linee guida, esempi di lettere e domande frequenti sul trattamento dei dati da parte di organi federali o di privati, fornisce consulenza telefonica e scritta a privati o scambia regolarmente informazioni con l'Associazione per la protezione dei dati aziendali (VUD). Può anche organizzare eventi informativi o di formazione per i responsabili del settore pubblico. Sotto la voce "formazione" sarebbe ipotizzabile anche una collaborazione con le varie facoltà di giurisprudenza. Attualmente, il diritto della protezione dei dati non è un corso obbligatorio in nessuna università svizzera. Allo stato attuale, i futuri avvocati non sono affatto, o non sono sufficientemente, preparati ad affrontare le sfide della pratica legale per quanto riguarda il tema trasversale della "protezione dei dati".

L'IFPD può ora riscuotere onorari per la consulenza a privati in materia di 14
protezione dei dati ai sensi dell'art. 58 cpv. 1 LPD sulla base dell'art. 59 cpv. 1 lett. e LPD in combinato disposto con l'art. 44 LPD. Art. 44 LADP. Gli onorari sono calcolati in base al tempo impiegato, con una tariffa oraria compresa tra 150,00 e 250,00 franchi.

Ai fini di un'attuazione efficiente in tutta la Svizzera di questo mandato 15
d'informazione giuridicamente standardizzato, la nuova legge prevede anche che l'IFPDT e il suo sostituto non provengano dalla stessa regione linguistica. In linea di principio, l'IFPDT e il suo sostituto dovrebbero quindi continuare a essere responsabili dell'attuazione del mandato d'informazione nelle rispettive regioni d'origine (ad esempio, la gestione delle richieste di colloquio).

Quanto più spesso l'IFPDT adempie al suo mandato di informazione 16
attraverso vari canali, tanto più è probabile che un ampio pubblico venga informato sulle attuali sfide in materia di protezione dei dati. Tuttavia, l'effettiva attuazione del mandato informativo dipende dalle risorse umane disponibili, che rimangono modeste.

B. Lit. b: Supporto alle autorità cantonali e internazionali

17 L'art. 58 cpv. 1 LADP lett. b deriva dall'art. 31 cpv. 1 lett. a e lett. c LPD. Secondo la formulazione esplicita della legge, il sostegno alle autorità cantonali e internazionali non è un caso speciale delle attività di consulenza dell'IFPDT. L'IFPDT può "solo" sostenere le autorità cantonali e non "consigliarle". A causa della ripartizione delle competenze tra la Confederazione e i Cantoni, l'IFPDT non è autorizzato a fornire consulenza agli organi cantonali nella misura in cui le autorità cantonali per la protezione dei dati sono competenti a farlo. In base alla vecchia legge, la formulazione del testo ("organi cantonali") escludeva che l'IFPDT potesse fornire assistenza anche ai Comuni. Ora, grazie alla formulazione leggermente modificata della legge ("autorità svizzere"), è ipotizzabile che l'IFPDT possa sostenere anche gli enti comunali. Tuttavia, a causa della suddivisione delle competenze in materia di protezione dei dati, nella pratica gli enti comunali devono rivolgersi all'autorità cantonale competente per la protezione dei dati in caso di domande o incertezze.

18 Nella vecchia legge, inoltre, non era chiaro se la disposizione in questione si applicasse solo agli enti pubblici o coprisse anche gli enti di protezione dei dati delle aziende private. Alla luce dell'attuale formulazione dell'art. 58 cpv. 1 lett. b LPD, è chiaro che il campo di applicazione di questa disposizione è limitato agli enti pubblici.

19 Ne consegue che le consultazioni della LPD devono essere limitate agli ambiti per i quali i Cantoni non sono competenti (consultazioni di persone private e di organi federali, cfr. art. 58 cpv. 1 lett. a LPD) e ai chiarimenti relativi alle delimitazioni di competenza tra Confederazione e Cantoni. La cooperazione effettiva in singoli casi specifici non ha luogo a causa della divisione delle competenze tra Confederazione e Cantoni. In questo senso, la formulazione scelta ("collabora con le autorità svizzere") è fuorviante.

20 L'assistenza fornita dall'IFPD ai sensi dell'art. 58 cpv. 1 lett. b LPD non è ancora vincolata ad alcuna forma e rimane gratuita con la nuova legge.

21 Alla luce dei problemi sempre più transnazionali, il supporto delle autorità straniere diventa sempre più importante. Ai sensi dell'art. 58 cpv. 1 lett. b LADP, la LPD non solo scambia informazioni con i rappresentanti delle autorità cantonali, ma ha anche un seggio in diverse organizzazioni internazionali e in questo contesto sostiene le autorità straniere o

internazionali nell'attuazione di una protezione dei dati efficace a livello globale.

In virtù della sua indipendenza statutaria, l'IFPDT deve sempre essere in grado di decidere autonomamente se e in quale misura desidera sostenere un'altra autorità. Un mandato vincolante di assistenza non sarebbe compatibile con l'indipendenza dell'IFPDT. 22

Per quanto riguarda i limiti di questo sostegno offerto dall'IFPD, occorre anche notare che l'art. 58 cpv. 1 lett. b LPD non costituisce né una base per la competenza federale in materia di protezione dei dati, né una base per lo scambio di informazioni con altre autorità (a livello nazionale o internazionale). Questa disposizione dovrebbe solo consentire uno scambio professionale tra le autorità e quindi permettere agli altri enti pubblici di beneficiare delle conoscenze giuridiche e tecniche dell'IFPDT. 23

Sin dalla sua fondazione, lo scambio con le autorità cantonali è stato organizzato da rappresentanti di "privatim" o da alcuni gruppi di lavoro. Nella pratica, è stato più volte dimostrato che gli scambi tra rappresentanti federali e cantonali sono arricchenti nelle aree in cui le rispettive competenze si sovrappongono, in particolare durante la pandemia di Covid 19, che ha sollevato diverse questioni di protezione dei dati nel settore sanitario non solo a livello cantonale ma anche a livello nazionale (e internazionale). Recentemente, l'IFPDT e "privatim" hanno rivisto insieme la guida "Elezioni e votazioni" in vista delle elezioni federali del 2023: Le elezioni e le votazioni si svolgono a tutti i livelli federali e sono soggette a sfide simili a tutti i livelli federali. 24

C. Lit. c: Mandato di sensibilizzazione

L'art. 58 cpv. 1 lett. c LPD specifica il dovere di sensibilizzazione della DFP, come previsto dall'art. 57 LPD. 25

La sensibilizzazione delle persone bisognose di protezione è stata recentemente inclusa nella FADP in conformità con il diritto europeo (art. 57 cpv. 1 lett. b FADP). Tuttavia, il termine "persone vulnerabili" non è definito né nell'art. 58 LPD né nell'art. 5 LPD (termini). Il messaggio elenca i minori e gli anziani come persone bisognose di protezione. A causa della scelta dei termini ("in particolare"), questo elenco non è esaustivo. Anche i malati e i rifugiati, ad esempio, possono essere considerati persone bisognose di 26

particolare protezione ai sensi dell'art. 58 cpv. 1 lett. c LPD, soprattutto se si considera che in queste costellazioni vengono spesso trattati dati personali che richiedono una protezione particolare ai sensi dell'art. 5 lett. c nn. 1, 2 e 5 LPD. Ad esempio, l'IFPDT interviene anno dopo anno sul trattamento dei dati personali nel settore sanitario.

27 L'IFPDT si è già adoperato per sensibilizzare i giovani alla protezione dei dati secondo la vecchia legge. Ad esempio, ha ideato sette lezioni per gli alunni del livello secondario I e II, ognuna delle quali è dedicata a un argomento specifico che interessa i giovani nella loro vita quotidiana. Ha anche pubblicato sul suo sito web consigli per i neo-genitori. Anche il servizio interattivo sostenuto dall'FDPIC per sensibilizzare alla protezione dei dati e alla trasparenza nelle organizzazioni, "Think Data", è esplicitamente rivolto, tra gli altri, agli studenti. Tuttavia, il compito di sensibilizzare i bambini e i giovani ha anche dei limiti. In base all'art. 62 cpv. 1 della Cost. l'istruzione è di competenza dei Cantoni. Spetta quindi in primo luogo ai direttori didattici cantonali occuparsi della sensibilizzazione alla protezione dei dati durante la scuola dell'obbligo.

28 Per quanto riguarda il mandato di sensibilizzazione per le persone anziane, al momento non è nota una collaborazione specifica con un'organizzazione attiva in questo settore o un progetto rivolto specificamente a questo gruppo sociale. La collaborazione con "pro senectute" o altre associazioni o gruppi di interesse sarebbe ipotizzabile o auspicabile sulla base dell'art. 58 cpv. 1 lett. c LPD.

29 L'assegnazione di premi e riconoscimenti sul modello, ad esempio, del Premio Rodotà del Consiglio d'Europa o del Premio Grande Fratello del Chaos Computer Club Switzerland sarebbe un modo per sensibilizzare la popolazione civile in maniera un po' diversa.

30 Nell'attuazione del mandato di sensibilizzazione dell'IFPDT, tuttavia, occorre sempre tenere presente che - come, ad esempio, nel contesto della lotta al cambiamento climatico - si tratta di sensibilizzare la popolazione a un pericolo le cui conseguenze diventeranno evidenti o tangibili solo in un momento successivo. Questo rende molto più difficile il lavoro di sensibilizzazione.

D. Lit. d: mandato di consulenza

Il mandato consultivo della LPD è stato espressamente inserito nella revisione. Ciò riflette anche un cambiamento nella legge che è stato osservato nella pratica: a differenza di quanto previsto dal legislatore del 1988, le attività della DFP non si concentrano sulla supervisione, ma sulla consulenza ai privati: 31

L'applicazione individuale dei diritti attraverso i tribunali civili (art. 32 cpv. 2 LPD) prevista dal legislatore ha un ruolo subordinato o (quasi) nullo nella pratica. A fronte di procedimenti lunghi e costosi dall'esito incerto, gli interessati avviano solo molto raramente un procedimento davanti al tribunale competente. Ciò è tanto più vero in quanto sempre più trattamenti di dati vengono effettuati da privati con sede all'estero e comportano una violazione della privacy in Svizzera. Ciò rende (quasi) impossibile o difficile intentare una causa promettente davanti a un tribunale civile svizzero. Di conseguenza, le questioni fondamentali della protezione dei dati non sono quasi mai oggetto di discussione nella giurisprudenza e le poche decisioni dei tribunali hanno un significato limitato al di là del singolo caso. Con il suo mandato consultivo, l'IFPDT ha quindi un ruolo importante da svolgere nell'applicazione della legge. 32

L'FDPIC è libero in termini di forma. Svolge il suo mandato consultivo sia oralmente (hotline) che per iscritto (modulo di contatto, lettere o reclami campione, guide, FAQ, comunicati stampa, Twitter). 33

A differenza delle consultazioni con "persone private su questioni relative alla protezione dei dati" ai sensi dell'art. 58 cpv. 1 lett. a LPD, le "informazioni su come una persona privata può esercitare i propri diritti" ai sensi dell'art. 58 cpv. 1 lett. d LPD in combinato disposto con l'art. 59 cpv. 1 lett. d LPD non sono coperte dalla LPD. Art. 59 cpv. 1 lett. e al contrario LPD a titolo gratuito. Va da sé che la demarcazione tra il campo di applicazione della lett. a e quello della lett. d LPD è probabilmente difficile nella pratica. Nell'interesse dell'uguaglianza giuridica, è auspicabile che la LPD faccia un uso generoso dell'eccezione prevista dall'art. 59 cpv. 3 LPD (rinuncia all'addebito di tasse) in questo contesto. 34

Nel corso delle sue consultazioni, l'IFPDT apprende in prima persona in quali settori o in quali aziende possono sorgere problemi con la legge sulla protezione dei dati. L'attuazione più ampia possibile del mandato di 35

consulenza contribuisce quindi, tra l'altro, alla capacità dell'IFPDT di svolgere in modo efficiente il suo mandato di vigilanza ai sensi degli articoli 49 e seguenti. La LPD può essere attuata in modo efficiente.

E. Lit. e: consultazione della DFP nel processo legislativo federale

36 La consultazione dell'IFPDT nella procedura legislativa federale è un caso particolare del mandato consultivo dell'IFPDT.

37 Secondo la nuova formulazione della legge, l'Incaricato deve essere consultato su tutti i progetti di legge relativi a decreti e misure federali che riguardano l'elaborazione dei dati (e non solo sui progetti di legge che riguardano la protezione dei dati in misura considerevole). Questa precisazione linguistica rispecchia la prassi della vecchia legge e va accolta con favore nell'ottica della certezza del diritto.

38 Nell'art. 38 cpv. 2 LDP, questo obbligo di tutti gli organi federali è stato ulteriormente specificato: Gli organi federali sottopongono all'IFPDT tutti i progetti di legge riguardanti il trattamento dei dati personali, la protezione dei dati e l'accesso ai documenti ufficiali.

39 Il termine interno (non ufficiale) per le osservazioni nell'ambito delle consultazioni d'ufficio è di tre settimane. In pratica, però, non tutti gli uffici federali si attengono a questa disposizione ufficiosa. In alcuni casi, la scadenza molto breve per i commenti può portare a una riduzione della qualità del parere dell'IFPDT. È auspicabile che, dopo la fine della pandemia di Corona, questo termine venga nuovamente rispettato in misura maggiore. Un ritorno al "courant normal" consentirebbe all'IFPDT di preparare con cura i suoi pareri e, laddove lo ritenga necessario, di cercare un dialogo con l'ufficio federale competente e trovare una soluzione praticabile per tutte le agenzie coinvolte.

40 Se l'IFPD è stato ignorato nella procedura legislativa e ritiene che vi sia un interesse pubblico in questa informazione, può rivolgersi direttamente al pubblico sulla base dell'art. 57 cpv. 2 LPD (in combinato disposto con l'art. 39 lett. i LPD).

41 Il termine "misure" è un concetto confuso. Questa vaghezza linguistica consente all'IFPDT di far parte di diversi organi o gruppi di lavoro. L'IFPD può quindi essere coinvolto nella prima fase di un nuovo progetto di

protezione dei dati sulla base dell'art. 58 cpv. 1 lett. e LPD. Ad esempio, l'IFPDT è stato consultato in una fase iniziale nell'ambito della strategia cloud dell'Amministrazione federale. Oppure, ad esempio, la SECO si è avvalsa della consulenza dell'IFPDT in occasione della revisione delle linee guida dell'art. 26 dell'ORSAE 3, pubblicate nel febbraio 2023. In questo contesto va tuttavia sottolineato che la consultazione della DFP all'inizio di un nuovo progetto non esclude la possibilità che la DFP riveda successivamente il progetto in questione nell'ambito della sua attività di vigilanza ai sensi degli artt. 49 e segg. della LDP. LPD, la DFP può riesaminare successivamente il progetto in questione. In altre parole, la consultazione della DFP non deve essere confusa con una sorta di "procedura di certificazione".

F. Lit. f: Compiti di LTras

La menzione dei compiti dell'IFPDT ai sensi di LTras è puramente dichiarativa. I compiti dell'IFPDT in relazione al principio dell'accesso del pubblico derivano direttamente dall'art. 18 LTras (gestione della procedura di conciliazione, accesso del pubblico, consultazione nella procedura legislativa) e dall'art. 19 LTras (valutazione). 42

Il coordinamento tra la LPD e l'UFC è disciplinato rispettivamente dall'art. 7 cpv. 2 e dall'art. 9 dell'UFC e dall'art. 36 cpv. 3 della LPD. 43

È discutibile se la protezione dei dati o il principio dell'accesso del pubblico siano serviti se la stessa autorità deve sostenere un'efficace protezione dei dati da un lato e garantire il massimo accesso possibile ai documenti ufficiali dall'altro. La soluzione svizzera si applica anche in altri Paesi, come la Germania (a livello federale) o il Regno Unito. La Francia, invece, ha affidato questi due compiti a due autorità diverse. A livello europeo, il compromesso in materia è disciplinato dall'art. 86 del DSGVO. 44

G. Lit. g: Raccomandazioni di buone prassi

L'art. 58 cpv. 1 lett. g LPD è stato introdotto di recente nella LPD nell'ambito della revisione. Tuttavia, l'IFPDT svolgeva già intensamente questo compito nell'ambito delle sue attività di consulenza sotto la vecchia legge, pubblicando numerose guide, lettere di esempio e FAQ sul suo sito web. 45

La pubblicazione delle raccomandazioni di buona prassi è, come la consultazione della LPD nel quadro della procedura legislativa a livello 46

federale (art. 58 cpv. 1 lett. e LPD), un caso particolare dell'attività consultiva della LPD. Anche per quanto riguarda le raccomandazioni di buona prassi, va sottolineato che l'attuazione delle raccomandazioni non preclude alcuna procedura di vigilanza. In altre parole, le raccomandazioni non sono giuridicamente vincolanti. La LPD non può intraprendere un'azione legislativa sulla base dell'art. 58 cpv. 1 lett. g LPD. Il tribunale chiamato a decidere se si è verificata o meno una violazione della LADP in un caso individuale è indipendente da qualsiasi raccomandazione formulata dalla LPD. Tuttavia, il fatto che un privato abbia seguito le raccomandazioni della DFP può svolgere un ruolo importante nell'esame della colpa nel contesto delle azioni riparatorie.

47 Per quanto riguarda il concetto di persona vulnerabile, si rimanda alle osservazioni precedenti sull'art. 58 cpv. 1 lett. c LPD.

III. CPV. 2: MANDATO ESTESO DI CONSULENZA

48 Dal punto di vista del contenuto, l'art. 58 cpv. 2 LADP corrisponde all'art. 31 cpv. 2 aDSG.

49 Alcune operazioni di trattamento dei dati sono escluse dal campo di applicazione della LPD ai sensi dell'art. 2 cpv. 2, 3 e 4 LPD e dell'art. 4 cpv. 2 LPD. L'art. 58 cpv. 2 LPD consente all'IFPD, se lo desidera, di esprimersi su questioni escluse dal campo di applicazione della LPD in base al testo della legge. La precisazione linguistica della seconda frase chiarisce che gli organi federali eventualmente interessati possono concedere alla DFP l'accesso ai dossier. In altre parole, in questi casi viene meno il segreto d'ufficio.

50 L'art. 58 cpv. 2 LPD è una cosiddetta "disposizione facoltativa". A differenza dei compiti di cui al cpv. 1, per i compiti di consulenza di cui al cpv. 2 non è previsto alcun diritto.

51 L'elenco di cui all'art. 58 cpv. 1 LPD non è esaustivo. È quindi possibile che l'IFPDT fornisca consulenza su trattamenti di dati che non rientrano nel campo di applicazione della LPD (cfr. art. 2 cpv. 2 lett. a LPD). Questa possibilità è espressione del fatto che l'art. 13 Cost. ha una validità globale e non si applica solo agli ambiti in cui la LPD è applicabile.

52 A causa della continua scarsità di risorse della DFP, l'art. 58 cpv. 2 LPD, come la disposizione precedente, sarà probabilmente applicato raramente.

Per completezza, in questo contesto va anche sottolineato che nei settori in cui la LPD non è applicabile, è esclusa qualsiasi attività di vigilanza da parte dell'IFPD, ad esempio nei procedimenti civili in corso. 53

IV. CPV. 3: ASSISTENZA INTERNAZIONALE RECIPROCA

L'art. 58 cpv. 3 LPD è stato inserito di recente nella LDP nell'ambito della revisione. Lo scopo di questa disposizione è quello di semplificare la trasmissione di documenti ufficiali agli incaricati privati della protezione dei dati domiciliati all'estero, che devono designare una rappresentanza in Svizzera ai sensi dell'art. 14 LADP. 54

BIBLIOGRAFIA

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).

I MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 60 LPD

Un commentario di Jonas D. Gassmann

CITAZIONE SUGGERITA

Jonas D. Gassmann, Kommentierung zu Art. 60 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Gassmann, N. XXX zu Art. 60 DSG.

Capitolo 8: Disposizioni penali

Art. 60 Violazione degli obblighi di informare, di concedere l'accesso e di collaborare

[1] Sono puniti, a querela di parte, con la multa fino a 250 000 franchi i privati che:

a. violano gli obblighi di cui agli articoli 19, 21 e 25–27, fornendo intenzionalmente informazioni inesatte o incomplete;

b. omettono intenzionalmente:

di informare la persona interessata conformemente agli articoli 19 capoverso 1 e 21 capoverso 1, o
di fornire alla persona interessata le informazioni di cui all'articolo 19 capoverso 2.

[2] Sono puniti con la multa fino a 250 000 franchi i privati che in violazione dell'articolo 49 capoverso 3 forniscono intenzionalmente all'IFPDT, nel quadro di un'inchiesta, informazioni false o rifiutano intenzionalmente di collaborare.

STRUTTURA

In breve 774
I. Aspetti generali 774
II. Elementi oggettivi del reato 775
A. Cerchia di autori del reato 775
B. Condotta sanzionabile 776
1. fornire informazioni false o incomplete (Art. 60 cpv. 1 lett. a) 776
2. Mancata informazione (Art. 60 cpv. 1 lett. b) 777
3. Fornire informazioni false o rifiutare di collaborare a un'indagine dell'IFPDT (Art. 60 cpv. 2) 778
III. Elementi soggettivi del reato 779
IV. Illegalità e colpevolezza 780
Bibliografia 780
I Materiali 781

IN BREVE

L'art. 60 punisce (i) la violazione intenzionale dell'obbligo di informazione, (ii) la violazione intenzionale dell'obbligo di informazione e (iii) la mancata collaborazione intenzionale con l'IFPDT nell'ambito di un'indagine. Se viene commesso uno di questi reati, può essere comminata una multa fino a 250.000 franchi svizzeri.

I. ASPETTI GENERALI

1 L'art. 60 riprende il contenuto normativo già presente nell'art. 34 aDSG. L'art. 34 cpv. 2 lett. aDSG non viene ripreso, poiché i relativi obblighi di comunicazione non sono più contenuti nella LPD rivista. Inoltre, la disposizione penale si estende anche all'obbligo di informazione in caso di decisione individuale automatizzata ai sensi dell'art. 21. A differenza dell'art. 34 aDSG in combinato disposto con l'art. 14 aDSG, l'obbligo di informazione si applica anche in caso di decisione individuale automatizzata. Ai sensi dell'art. 14 aDSG, l'obbligo di informazione non si applica più solo ai dati personali e ai profili della personalità che richiedono una protezione speciale, ma ora, ai sensi dell'art. 60 in combinato disposto con l'art. 19, a tutti i dati personali. Art. 19 per tutti i dati personali. Questo amplia ulteriormente la disposizione. Nella bozza preliminare, era stato creato un articolo molto completo a questo scopo. È stata prevista una sanzione per la violazione intenzionale degli obblighi di informazione, comunicazione e collaborazione, oltre a un elemento di negligenza. Nel processo di consultazione, la punibilità delle violazioni per negligenza è stata in parte criticata. Di conseguenza, il reato di negligenza è stato eliminato dall'art. 54 della bozza di LPD.

2 La disposizione penale dell'art. 60 cpv. 1 è un reato di applicazione, mentre quella dell'art. 60 cpv. 2 è un reato d'ufficio.

3 La disposizione dell'art. 60 mira, da un lato, a proteggere le persone che possono essere colpite da minacce alla loro personalità e, dall'altro, a tutelare la funzione di vigilanza dell'IFPDT (e quindi la sua capacità di funzionare) nella sfera privata. Si tratta di un reato di pericolo astratto; il reato si perfeziona con la fornitura di informazioni false o incomplete o con l'omissione di informazioni/dettagli in violazione del dovere o con il rifiuto di

collaborare con l'IFPDT. Non è necessario che vi sia una violazione della personalità o che la procedura d'indagine dell'IFPDT sia stata compromessa.

L'art. 60 cpv. 2 si distingue dalla disposizione dell'art. 63 in quanto, a differenza di quest'ultimo, l'art. 60 cpv. 2 non richiede l'esistenza di un ordine in senso formale. 4

La disposizione sanzionatoria continua a essere strutturata come reato, ma il limite massimo dell'ammenda prevista è stato notevolmente innalzato. L'art. 50 LPD prevedeva ancora una multa fino a 500.000 franchi. Il Consiglio federale ha giustificato questo importo con "la mancanza di controllo delle persone interessate sui loro dati, la mancanza di trasparenza nel trattamento dei dati e gli attori economici sempre più potenti". È stato inoltre fatto un confronto con altre disposizioni penali del diritto penale accessorio (come l'art. 49 della legge sulle banche) e l'importanza di multe elevate per decidere se la legislazione svizzera offre ancora un "livello di protezione sufficiente" rispetto all'UE. Il limite massimo delle ammende previsto nel progetto preliminare è stato oggetto di critiche durante il processo di consultazione. In alcuni casi le multe sono state considerate troppo basse, in altri troppo alte. È stato anche criticato il fatto che le sanzioni fossero rivolte solo ai privati. In risposta a ciò, il limite massimo dell'ammenda previsto dall'art. 54 E-DSA è stato fissato a 250.000 franchi, che corrisponde a 25 volte l'ammenda precedente. L'ammenda effettiva viene determinata tenendo conto delle condizioni economiche dell'autore del reato (art. 106 cpv. 3 CP in combinato disposto con l'art. 47 CP). L'art. 54 LPD è stato ripreso come art. 60 con alcune modifiche redazionali. 5

II. ELEMENTI OGGETTIVI DEL REATO

A. Cerchia di autori del reato

L'art. 60 è un reato speciale, in quanto possono essere considerati autori solo coloro che sono obbligati a fornire informazioni (art. 60 cpv. 1) o che sono invitati dall'IFPDT a fornire informazioni o a collaborare in altro modo nell'ambito di un'indagine (art. 60 cpv. 2). Chi non può essere un autore di reato ai sensi dell'art. 60 e quindi non risponde a una richiesta di informazioni o fornisce informazioni false rimane impunito. Se le condizioni sono soddisfatte, è possibile essere puniti come istigatori. 6

7 L'orientamento della disposizione penale è in contrasto con il DSGVO, in cui è responsabile la rispettiva azienda. In Svizzera, invece, sono ritenute responsabili le persone fisiche che agiscono effettivamente per conto dell'azienda e che realizzano colpevolmente il reato. Ciò è giustificato dal rifiuto dell'attribuzione di responsabilità a terzi nella responsabilità penale delle imprese, previsto dall'art. 102 StGB. Inoltre, non esistono ancora sufficienti garanzie procedurali nel diritto processuale amministrativo, il che porterebbe all'incertezza giuridica. Per ovviare alla mancanza di responsabilità penale delle società, il Consiglio federale ha previsto un inasprimento della responsabilità penale degli organi di governo applicando l'art. 6 del Codice di procedura amministrativa oltre all'art. 29 del Codice penale.

8 L'azione penale può essere intentata contro i dirigenti, ma anche contro altre persone responsabili di operazioni rilevanti. Allo stesso tempo, però, i soggetti obbligati non sono responsabili solo per le informazioni false che essi stessi forniscono, ma anche, ad esempio, per il caso in cui un dipendente fornisca informazioni false in base alle sue istruzioni.

B. Condotta sanzionabile

9 L'art. 60 prevede tre diversi reati. Le sanzioni sono previste per la violazione dell'obbligo di informazione (art. 60 cpv. 1 lett. a; infra, n. 10 e segg.), per la violazione dell'obbligo di informazione (art. 60 cpv. 1 lett. b; infra, n. 17 e segg.) e per la mancata collaborazione con l'IFPDT nel corso di un'indagine (art. 60 cpv. 2; infra, n. 19 e segg.).

1. fornire informazioni false o incomplete (Art. 60 cpv. 1 lett. a)

10 L'art. 60 cpv. 1 lett. a incrimina la fornitura di informazioni false o incomplete e si riferisce quindi alla violazione degli artt. 19, 21 e 25-27.

11 Gli elementi oggettivi del reato comprendono l'esistenza di un obbligo di informazione e l'inesistenza di un motivo che elimini o limiti tale obbligo (artt. 19, 21 e 25-27). È possibile distinguere tra il dovere di informare di cui agli artt. 19 e 21 e il dovere di fornire informazioni di cui agli artt. 25-27.

12 Nell'ambito dell'obbligo di informazione (art. 25), solo chi fornisce informazioni false o incomplete è perseguibile, ma non chi, ad esempio, adduce un falso motivo di rifiuto ai sensi dell'art. 26. Un'informazione è falsa

se non corrisponde alla realtà (ad esempio, se alla persona che richiede informazioni vengono forniti dati diversi da quelli effettivamente trattati o se si afferma in modo non veritiero che non viene trattato alcun dato della persona stessa). Inoltre, un'informazione è falsa anche se è fuorviante, ossia se crea una falsa impressione dei fatti reali. Le informazioni sono incomplete se non vengono fornite tutte le informazioni elencate nell'articolo 25 (ad esempio, se non viene comunicato il periodo di conservazione dei dati personali, anche se sarebbe possibile). Le informazioni possono anche essere cumulativamente false e incomplete.

Tuttavia, non è un reato se qualcuno rivela che le informazioni sono incomplete oscurandole o in altro modo, poiché ciò non crea un'apparenza di completezza. Il motivo è che, in caso di rifiuto di divulgazione, è possibile agire senza problemi ai sensi dell'art. 32, in base al quale il tribunale civile può ordinare la fornitura di informazioni sotto pena dell'art. 292 CP. Inoltre, l'art. 60 cpv. 1 lett. a non si applica ai casi in cui le informazioni vengono fornite ma viene richiesto un compenso in violazione del divieto. Tuttavia, l'art. 146 CP (frode) è talvolta applicabile in questo caso se si crea la falsa impressione che il compenso sia quello normalmente dovuto. 13

Non rientra nel campo di applicazione dell'art. 60 cpv. 1 lett. a nemmeno il caso in cui (ad esempio perché viene negata l'esistenza di una situazione che richiede un'informazione) l'informazione non venga fornita affatto o solo con ritardo. Tuttavia, in caso di rifiuto di fornire informazioni, è possibile una responsabilità penale ai sensi dell'Art. 60 cpv. 1 lett. b. 14

Nell'ambito dell'obbligo di informazione (artt. 19 e 21), anche la fornitura di informazioni false o incomplete è punibile. 15

Nell'art. 21, l'obbligo di informazione non si riferisce più solo all'acquisizione di dati personali particolarmente sensibili e di profili della personalità, come nell'art. 14 aDSG, ma ora all'acquisizione di tutti i dati personali. L'obbligo di informazione è quindi diventato più completo in termini di contenuto e il rischio di responsabilità penale è stato ampliato. 16

2. Mancata informazione (Art. 60 cpv. 1 lett. b)

L'art. 60 cpv. 1 lett. b contempla i casi in cui un privato omette (i) di informare la persona interessata che sono stati ottenuti dati personali che la riguardano (art. 19 cpv. 1) o che è stata presa una decisione individuale automatizzata (art. 17

21 cpv. 1) o (ii) di fornire alla persona interessata le informazioni necessarie per far valere i suoi diritti ai sensi della LPD (art. 19 cpv. 2). Il reato oggettivo di cui all'art. 61 lett. b sarebbe soddisfatto, ad esempio, se un'azienda non fornisce informazioni su quali dati personali tratta in una dichiarazione sulla protezione dei dati giuridicamente adeguata.

18 Il reato è punibile anche se un'azienda fornisce un motivo per non fornire le informazioni. A questo proposito, la responsabilità penale è più ampia rispetto all'art. 60 cpv. 1 lett. a.

3. Fornire informazioni false o rifiutare di collaborare a un'indagine dell'IFPDT (Art. 60 cpv. 2)

19 La disposizione penale dell'art. 60 cpv. 2 riprende il contenuto normativo dell'art. 34 cpv. 2 lett. b aDSG, che dichiarava punibile la fornitura di informazioni false o il rifiuto di collaborare nell'ambito di un'indagine dell'IFPDT. La norma fa riferimento all'obbligo di collaborazione di cui all'art. 49 cpv. 3, secondo il quale i privati sono tenuti a fornire all'IFPDT tutte le informazioni e i documenti necessari all'indagine. La variante di reato "fornitura di informazioni false" è strutturata come un reato di attività e la variante di reato "rifiuto di cooperare" come un vero e proprio reato di omissione.

20 Il reato oggettivo presuppone un'indagine formale da parte dell'IFPDT ai sensi dell'art. 49, avviata a causa di una possibile violazione delle disposizioni sulla protezione dei dati. L'art. 60 cpv. 2 non contempla le false informazioni o il rifiuto di collaborare nell'ambito di indagini condotte dall'IFPDT al di fuori di un'indagine formale. Un altro prerequisito è che (i) l'IFPDT abbia richiesto in modo inequivocabile all'autore del reato di fornire informazioni o di collaborare in altro modo nell'ambito dell'indagine avviata, (ii) l'IFPDT avesse il diritto di fare questa richiesta, (iii) l'autore del reato abbia fornito informazioni false o si sia rifiutato di collaborare come richiesto, e (iv) l'autore del reato non avesse il diritto di fornire informazioni false o di rifiutarsi di collaborare (ad esempio, sulla base del diritto di rifiutare informazioni di cui all'art. 49 cpv. 3). La falsa informazione non è punibile se l'IFPDT non ha richiesto alcuna informazione.

Il tribunale penale non può limitarsi a esaminare l'azione o l'omissione dell'imputato, ma deve anche verificare se la richiesta di informazioni o di collaborazione da parte dell'IFPDT fosse legittima. 21

La richiesta dell'IFPDT non deve necessariamente essere formulata con riferimento alla responsabilità penale (a differenza dell'art. 63 e dell'art. 292 CP), ma deve essere chiaro alla persona richiesta che la sua collaborazione non è volontaria. Nei casi in cui l'IFPDT chieda a una persona potenzialmente punibile di collaborare, deve essere richiesto che egli informi esplicitamente tale persona del diritto di rifiutare di fornire informazioni. 22

III. ELEMENTI SOGGETTIVI DEL REATO

Dal punto di vista soggettivo, è richiesto il dolo. È sufficiente il dolo eventuale, ossia il considerare possibile la realizzazione del reato e accettarlo. Al momento della commissione del reato, l'autore deve essere stato a conoscenza delle circostanze del caso in base alle quali i fatti oggettivi del reato devono essere considerati accertati, e deve aver compreso le successive valutazioni giuridiche almeno in termini profani (la cosiddetta valutazione parallela in termini profani). 23

Nella pratica, probabilmente non è raro che la persona che agisce sia consapevole della possibilità che le informazioni siano incomplete e che le accetti perché preferisce fornire tali informazioni piuttosto che non fornirne affatto. Se la persona interessata riceve una dichiarazione di completezza, di solito si presume che le informazioni non siano complete. La persona obbligata a fornire informazioni agisce per negligenza e non è quindi perseguibile se ha fatto affidamento sul fatto che i dati forniti, che non erano stati controllati, erano completi. La distinzione dall'esistenza del dolo eventuale deve essere fatta sulla base di prove indiziarie in ogni singolo caso. 24

Se l'autore del reato si sbaglia sui fatti rilevanti per il reato, ciò costituisce un errore di fatto ai sensi dell'articolo 13 CP. In questo caso, il tribunale giudica il reato in base alla percezione dei fatti da parte dell'autore del reato. Ciò è particolarmente rilevante se la persona obbligata a fornire informazioni fornisce informazioni incomplete perché ritiene che siano state fornite in modo completo. Un errore di fatto può sussistere anche per quanto riguarda gli elementi normativi del reato, come ad esempio la questione dell'esistenza 25

di un corrispondente obbligo di informazione o di denuncia. Il fattore decisivo in questo caso è l'opinione di un terzo medio.

IV. ILLEGALITÀ E COLPEVOLEZZA

26 Per quanto riguarda l'illiceità, si applicano le regole generali del CP ai sensi dell'art. 333 cpv. 1 CP. Un comportamento conforme all'illecito può essere eccezionalmente consentito sulla base di motivi di giustificazione legali o sovralegali.

27 Anche per quanto riguarda la colpevolezza valgono le regole generali dell'art. 333 cpv. 1 CP. Il reato può essere ostacolato da un errore di proibizione ai sensi dell'art. 21 CP. Tuttavia, ciò avviene solo se la persona considerata come autore del reato non poteva sapere di agire illegalmente. In questo caso, la persona crede di non aver fatto nulla di male. Se l'errore di diritto poteva essere evitato, la sanzione viene solo ridotta.

BIBLIOGRAFIA

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.

I MATERIALI

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

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 61 LPD

Un commentario di Jonas D. Gassmann

CITAZIONE SUGGERITA

Jonas D. Gassmann, Kommentierung zu Art. 61 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Gassmann, N. XXX zu Art. 61 DSG.

Art. 61 Violazione degli obblighi di diligenza

A querela di parte sono puniti con la multa fino a 250 000 franchi i privati che intenzionalmente:

a. comunicano dati personali all'estero in violazione dell'articolo 16 capoversi 1 e 2 e senza che sussistano le condizioni di cui all'articolo 17;

b. affidano il trattamento di dati personali a un responsabile senza che sussistano le condizioni di cui all'articolo 9 capoversi 1 e 2;

c. non rispettano i requisiti minimi in materia di sicurezza dei dati emanati dal Consiglio federale in virtù dell'articolo 8 capoverso 3.

STRUTTURA

In breve 785
I. Aspetti generali 785
II. Fatti oggettivi 786
A. Violazione dei requisiti per l'esportazione dei dati (Art. 61 lett. a) 786
1. Generale 786
2. Nessuna responsabilità penale dell'importatore 787
B. Violazione dei requisiti quando si trasferisce il trattamento dei dati a un incaricato del trattamento (art. 61 lett. b) 788
1. Generale 788
2. Nessuna responsabilità penale per l'incaricato del trattamento (o per le persone che agiscono per suo conto). 789
C. Violazione dei requisiti minimi di sicurezza dei dati (art. 61 lett. c) 789
1. Generale 789
2. Violazione dei principi dell'art. 1 LPD 789
3. Violazione degli obiettivi dell'art. 2 DPA 790
4. Violazione della disposizione sulle misure tecniche e organizzative (art. 3 DPA) 790
5. Omissione della registrazione ai sensi dell'art. 4 DPA 791
6. Mancata elaborazione di un regolamento sul trattamento dei dati ai sensi dell'art. 5 f. LPD. LPD 791
7. Considerazione dei costi nella determinazione di un'adeguata sicurezza dei dati e di misure appropriate 792
III. Reato soggettivo 793
IV. Illegalità e colpevolezza 793
Bibliografia 794
I Materiali 794

IN BREVE

La disposizione dell'art. 61 punisce (i) la violazione intenzionale dei requisiti durante l'esportazione dei dati, (ii) la violazione intenzionale dei requisiti durante il trasferimento del trattamento dei dati a un incaricato del trattamento e (iii) la mancata osservanza intenzionale dei requisiti minimi di sicurezza dei dati. Se viene commesso uno di questi reati, può essere comminata una multa fino a 250.000 franchi svizzeri. Nel caso del reato di inosservanza intenzionale dei requisiti minimi di sicurezza dei dati (art. 61 lett. c), sussistono fondati dubbi sulla sua giustiziabilità.

I. ASPETTI GENERALI

La disposizione dell'art. 61 è nuova. Il Consiglio federale ha giustificato l'introduzione di questa disposizione nel messaggio affermando che la legge sulla protezione dei dati, completamente rivista, prevedeva "nuovi obblighi elementari" che "non erano coperti dalle disposizioni penali esistenti". Si tratta di un reato di messa in pericolo astratto; il reato si perfeziona nel momento in cui viene commesso, pertanto la responsabilità penale non richiede che terzi non autorizzati siano a conoscenza dei dati personali in questione. 1

La disposizione penale dell'art. 61 è un reato di applicazione. 2

Lo scopo dell'art. 61 è quello di far rispettare gli obblighi dei responsabili del trattamento e degli incaricati del trattamento stabiliti dalla legge (art. 16 cpv. 1 e 2, in combinato disposto con l'art. 17; art. 9 cpv. 1 e 2; art. 8 cpv. 3) rendendone punibile la violazione. Secondo il messaggio, la punizione ha lo scopo ultimo di contribuire all'effettiva protezione della personalità delle persone interessate. L'art. 61 lett. a va letto anche nel contesto dell'obiettivo della revisione della LPD, come indicato dal Consiglio federale nel suo rapporto sulla valutazione della LPD del 9 dicembre 2011: la revisione dovrebbe affrontare l'aumento del trattamento dei dati, la dimensione sempre più internazionale del trattamento dei dati e la crescente difficoltà di continuare a poter controllare i dati una volta divulgati. 3

Il reato di cui all'art. 61 è un reato speciale: solo coloro che hanno la responsabilità di garantire l'osservanza degli obblighi di cui all'art. 61 possono essere considerati autori del reato, mentre nel caso delle persone giuridiche si 4

tratta della loro direzione ai sensi dell'art. 29 CP. Per sua natura, la disposizione dell'art. 61 si rivolge quindi in primo luogo alle persone autorizzate a dare istruzioni, in quanto responsabili dell'osservanza dei doveri in questione. Chi non impedisce le violazioni da parte dei dipendenti subordinati o non ne annulla gli effetti può essere considerato un autore di reato (art. 6 cpv. 2 e 3 del Codice Penale in combinato disposto con l'art. 64 cpv. 1 della LPD).

5 Per quanto riguarda il reato di cui all'art. 61 lett. c, nel corso del processo legislativo è stato ripetutamente criticato in quanto troppo vago. Tuttavia, la richiesta di cancellazione non è stata accolta. Meyle/Morand/Vasella mettono giustamente in discussione la giustiziabilità dei "requisiti minimi di sicurezza dei dati" disciplinati nella LPD (cfr. infra, n. 17 e segg.).

II. FATTI OGGETTIVI

6 L'art. 61 LPD elenca tre reati, il cui compimento è considerato una violazione della diligenza. La conseguenza di una violazione da parte di privati è una multa fino a 250.000 franchi svizzeri. In particolare, la violazione dei seguenti tre reati è perseguibile penalmente su richiesta: Violazione dei requisiti per l'esportazione dei dati (Art. 61 lett. a, di seguito n. 7 e segg.), violazione dei requisiti per il trasferimento del trattamento dei dati a un incaricato del trattamento (Art. 61 lett. b, di seguito n. 12 e segg.) e mancato rispetto dei requisiti minimi di sicurezza dei dati (Art. 61 lett. c, di seguito n. 15 e segg.).

A. Violazione dei requisiti per l'esportazione dei dati (Art. 61 lett. a)

1. Generale

7 In base al diritto previgente, chi non rispettava i requisiti di legge nell'ambito della divulgazione di dati a Stati che non disponevano di un'adeguata protezione giuridica dei dati rimaneva impunito. Ai sensi dell'art. 34 cpv. 2 lett. aDSG, era perseguibile solo chi si occupava della protezione sotto forma di contratto, ma ometteva deliberatamente di segnalarlo all'IFPDT ai sensi dell'art. 6 cpv. 3 aDSG o forniva deliberatamente informazioni false.

8 Ai sensi dell'art. 61 lett. a, è perseguibile chiunque esporti intenzionalmente dati in uno Stato che non dispone di un'adeguata protezione dei dati e non

può né dimostrare un'adeguata garanzia di protezione dei dati né avvalersi di un'esenzione ai sensi dell'art. 17. Se il Consiglio federale non ha emesso una "decisione di adeguatezza" ai sensi dell'art. 16 cpv. 1, i dati personali possono essere comunicati allo Stato in questione solo alle condizioni di cui all'art. 16 cpv. 2, la cui maggiore rilevanza pratica è la stipula di clausole contrattuali standard ("clausole standard di protezione dei dati", lett. d).

Nell'ambito del DSGVO, con la Decisione di esecuzione (UE) 2021/914 del 4 giugno 2021, la Commissione europea ha abrogato le precedenti clausole contrattuali standard con effetto dal 27 settembre 2021 e le ha sostituite con nuove clausole contrattuali standard. L'IFPDT ha riconosciuto queste nuove clausole contrattuali standard il 27 agosto 2021, con la riserva di adattarle e/o integrarle se necessario in casi specifici di applicazione. Tuttavia, chi comunica dati a uno Stato che non dispone di un'adeguata protezione giuridica dei dati non può accontentarsi di stipulare clausole contrattuali standard riconosciute. La formulazione dell'art. 16 cpv. 2 lett. d richiede piuttosto che queste clausole contrattuali standard garantiscano effettivamente una protezione dei dati "adeguata". Le nuove clausole contrattuali standard richiedono che le parti (i) garantiscano inoltre di poter rispettare le clausole contrattuali standard indipendentemente dal diritto nazionale dell'importatore e (ii) documentino la loro valutazione al riguardo. Deve quindi essere effettuata una cosiddetta valutazione d'impatto del trasferimento (TIA) e i dati possono essere trasferiti solo se la TIA è soddisfacente. 9

L'art. 10 cpv. 1 DPA specifica o relativizza che l'esportatore di dati deve adottare "misure ragionevoli" nel caso di divulgazione di dati mediante clausole contrattuali standard per garantire che l'importatore di dati si conformi alle clausole in questione. Ne consegue che (nel senso dell'approccio basato sul rischio) può essere accettato il rischio residuo che la legislazione locale dell'importatore comprometta il rispetto delle clausole contrattuali standard da parte dell'importatore, purché siano state adottate misure per ridurre adeguatamente tale rischio. Si veda il commento agli articoli 16 e 17. 10

2. Nessuna responsabilità penale dell'importatore

Chiunque (in qualità di esportatore) divulghi dati personali all'estero pur sapendo che il destinatario (importatore) dei dati non garantisce un'adeguata 11

protezione dei dati nonostante il contratto, si espone al rischio di responsabilità penale ai sensi dell'art. 61 lett. a. Il rischio di responsabilità penale non si applica all'importatore. Al contrario, l'importatore che accetta i dati personali o li utilizza in violazione del contratto o della protezione dei dati non è soggetto al rischio di responsabilità penale - l'unico reato previsto dall'art. 61 lett. a è la divulgazione dei dati personali.

B. Violazione dei requisiti quando si trasferisce il trattamento dei dati a un incaricato del trattamento (art. 61 lett. b)

1. Generale

12 Ai sensi dell'art. 61 lett. b, chiunque ceda intenzionalmente il trattamento dei dati a un incaricato del trattamento senza che siano soddisfatti i requisiti di cui all'art. 9 cpv. 1 e 2 è perseguibile penalmente. Ai sensi dell'art. 9 cpv. 1, il trattamento dei dati personali può essere trasferito a un incaricato del trattamento per contratto o per legge se (a) i dati sono trattati nello stesso modo in cui il responsabile del trattamento sarebbe autorizzato a farlo lui stesso e (b) nessun obbligo legale o contrattuale di segretezza vieta il trasferimento. Ai sensi dell'art. 9, cpv. 2, il responsabile del trattamento deve in particolare assicurarsi "che l'incaricato del trattamento sia in grado di garantire la sicurezza dei dati". I fatti oggettivi di cui all'art. 61 lett. b sarebbero soddisfatti, ad esempio, se un'azienda, in qualità di responsabile del trattamento dei dati, utilizzasse un incaricato del trattamento dei dati (ad esempio un fornitore di servizi cloud) senza aver stipulato con quest'ultimo un contratto di trattamento dei dati giuridicamente sufficiente.

13 L'art. 7 DPA specifica questi requisiti per i trattamenti commissionati: il responsabile del trattamento deve approvare preventivamente l'incarico a elaboratori subappaltati in modo generale o specifico (art. 7 cpv. 1 DPA). Nel caso di un'autorizzazione generale, il responsabile del trattamento deve essere informato di qualsiasi cambiamento previsto per quanto riguarda il coinvolgimento o la sostituzione di altri terzi e il responsabile del trattamento può opporsi (art. 7 cpv. 2 DPA). Si veda il commento all'art. 9 per tutto ciò.

2. Nessuna responsabilità penale per l'incaricato del trattamento (o per le persone che agiscono per suo conto).

La violazione dell'art. 9 cpv. 3, ossia l'obbligo dell'incaricato di ottenere l'autorizzazione preventiva del responsabile del trattamento per i nuovi subincaricati, non è punibile. Anche in caso di violazione dell'art. 9 cpv. 1 o 2, secondo la formulazione dell'art. 61 lett. b, l'incaricato del trattamento (o le persone che agiscono per suo conto) non è perseguibile: solo il responsabile (o le persone che agiscono per suo conto) può essere punito. Lo stesso deve valere anche nel caso in cui l'incaricato del trattamento deleghi a sua volta il trattamento dei dati a un subincaricato: le norme che giustificano la punibilità devono essere interpretate in modo restrittivo. 14

C. Violazione dei requisiti minimi di sicurezza dei dati (art. 61 lett. c)

1. Generale

Ai sensi dell'art. 61 lett. c, è perseguibile chiunque non rispetti intenzionalmente le prescrizioni minime di sicurezza dei dati emanate dal Consiglio federale ai sensi dell'art. 8 cpv. 3. Si fa riferimento alla prima sezione ("Sicurezza dei dati", art. 1 e segg.) del primo capitolo della LPD. 15

La disposizione dell'art. 61 lett. c è un reato di messa in pericolo astratto concepito come norma generale (cfr. già sopra, n. 1); non è necessario che si sia verificata una "violazione dei dati". E viceversa, non tutte le "violazioni dei dati" comportano una responsabilità penale: se c'è una "violazione dei dati" ma i "requisiti minimi di sicurezza dei dati" sono stati rispettati, non c'è responsabilità penale. 16

2. Violazione dei principi dell'art. 1 LPD

La disposizione dell'art. 1 LPD contiene i principi che il responsabile del trattamento e l'incaricato del trattamento devono osservare nel determinare il livello di protezione adeguato e le misure idonee. Si tratta di linee guida generali e non di requisiti concreti (minimi) di sicurezza dei dati. Secondo la corretta opinione di Meyle/Morand/Vasella, questa disposizione molto generale riguardante la procedura del responsabile del trattamento nel determinare le misure di sicurezza non è giustiziabile - non è evidente quali 17

"requisiti minimi" per la sicurezza dei dati ai sensi dell'art. 8(3) dovrebbero risultare dall'art. 1 DPA.

18 Se il responsabile del trattamento non si attiene ai principi dell'art. 1 LPD, ad esempio se non determina la necessità di protezione dei dati personali secondo i criteri previsti dal cpv. 1 o se non tiene conto dei criteri pertinenti nella valutazione del rischio come previsto dal cpv. 2 o se non rivede le sue misure "per l'intero periodo di trattamento" come previsto dal cpv. 5, ciò non indica che i dati non sono sicuri. 5, ciò non indica una violazione dei "requisiti minimi" per la sicurezza dei dati: da un lato, l'art. 1 LPD non definisce tali requisiti, ma contiene solo linee guida su come possono essere raggiunti, e dall'altro, un responsabile del trattamento può anche implementare misure efficaci per garantire un'adeguata sicurezza dei dati senza seguire rigorosamente l'art. 1 LPD.

3. Violazione degli obiettivi dell'art. 2 DPA

19 La disposizione dell'art. 2 LPD definisce gli obiettivi di protezione della sicurezza dei dati che il responsabile del trattamento e l'incaricato del trattamento devono raggiungere mediante misure tecniche e organizzative: Riservatezza (lett. a), Disponibilità (lett. b), Integrità (lett. c) e Tracciabilità (lett. d).

20 Questi obiettivi di protezione sono identici a quelli previsti dall'art. 6 cpv. 2 della Legge federale del 18 dicembre 2020 sulla sicurezza delle informazioni nella Confederazione (Legge sulla sicurezza delle informazioni). Come i principi di cui all'art. 1 LPD, anche gli obiettivi di cui all'art. 2 LPD sono molto generali (come si evince dal solo titolo "Obiettivi") e da essi non si possono ricavare "requisiti minimi" per la sicurezza dei dati ai sensi dell'art. 8 cpv. 3. Non è chiaro quali misure tecniche e organizzative concrete debbano essere attuate. Meyle/Morand/Vasella mettono giustamente in dubbio la giustiziabilità anche di questa disposizione.

4. Violazione della disposizione sulle misure tecniche e organizzative (art. 3 DPA)

21 La disposizione dell'art. 3 LPD contiene specifiche per le misure tecniche e organizzative e concretizza quindi la sicurezza dei dati. Tuttavia, essa non contiene alcun "requisito minimo" per la sicurezza dei dati ai sensi dell'art. 8

cpv. 3 (nemmeno); invece, l'art. 3 RPD si limita a concretizzare gli obiettivi di protezione contenuti nell'art. 2 RPD.

In un'interpretazione ampia, l'art. DPO potrebbe essere letto come "requisiti minimi", in quanto secondo questa disposizione gli obiettivi di protezione ai sensi dell'art. 2 DPO devono essere "garantiti". Tuttavia, una simile interpretazione significherebbe che ogni violazione di un obiettivo di protezione sarebbe la prova della mancanza di una misura adeguata. Ciò a sua volta non sarebbe compatibile con l'approccio basato sul rischio riconosciuto nel settore della sicurezza dei dati. A questo proposito, il termine "garantire" deve essere interpretato come "adoperarsi". 22

L'art. 3 LPD, insieme agli artt. 1 e 2 LPD, deve essere letto come una concretizzazione del concetto di sicurezza dei dati, senza che da esso si possano ricavare "requisiti minimi" per la sicurezza dei dati. Inoltre, il responsabile del trattamento e l'incaricato del trattamento non devono necessariamente tenere conto di tutti gli obiettivi di protezione ai sensi dell'art. 3 LPD per le loro misure tecniche e organizzative. Anche la giustiziabilità di questa disposizione è giustamente messa in discussione da Meyle/Morand/Vasella. 23

5. Omissione della registrazione ai sensi dell'art. 4 DPA

La disposizione dell'art. 4 LPD riprende il precedente art. 10 LPD. Lo scopo della registrazione è quello di garantire la limitazione degli scopi. 24

Di norma, la registrazione non è un "requisito minimo per la sicurezza dei dati" come indicato nell'art. 61 lett. c (anche se l'art. 4 LPD è elencato nella prima sezione della LPD, "Sicurezza dei dati") e l'omissione della registrazione non può essere punita a tale riguardo. La responsabilità penale sarebbe ipotizzabile in via eccezionale se l'autorità giudiziaria potesse dimostrare, in un caso specifico, che la registrazione come misura di tracciabilità era indirettamente finalizzata anche alla sicurezza dei dati e che l'imputato ne era consapevole, almeno a grandi linee. 25

6. Mancata elaborazione di un regolamento sul trattamento dei dati ai sensi dell'art. 5 f. LPD. LPD

Le disposizioni dell'art. 5 f. DPA riprendono i precedenti art. 11 LDP e art. 21 LDP. Nella relazione esplicativa sulla LPD, lo stesso Consiglio federale 26

afferma che la creazione di norme sul trattamento dei dati riguarda la responsabilità, ossia non la sicurezza dei dati. Ciò non cambia il fatto che l'obbligo di redigere tali regolamenti sussiste solo in caso di aumento del rischio.

27 Un "requisito minimo per la sicurezza dei dati", come indicato nell'art. 61 lett. c, è la creazione di "norme sul trattamento" (anche se l'art. 5 f. FADP non lo menziona nella prima sezione "sicurezza dei dati"). Le norme sul trattamento dei dati sono elencate nella prima sezione "sicurezza dei dati" della LPD) e l'omissione di redigerle non può essere punita a questo riguardo.

7. Considerazione dei costi nella determinazione di un'adeguata sicurezza dei dati e di misure appropriate

28 Ai sensi dell'art. 1 cpv. 1 RGPD, per garantire un'adeguata sicurezza dei dati, il responsabile del trattamento e l'incaricato del trattamento devono determinare la necessità di protezione dei dati personali e stabilire "le misure tecniche e organizzative adeguate in considerazione del rischio". L'art. 1 cpv. 2 della FADP descrive i criteri per valutare la necessità di protezione dei dati personali e l'art. 1 cpv. 3 della FADP descrive i criteri per valutare il rischio per la personalità o i diritti fondamentali dell'interessato. Più alta è la necessità di protezione dei dati personali e/o più alto è il rischio menzionato, più severi sono i requisiti per le misure. Ai sensi dell'art. 1 cpv. 4 LADP, nel determinare le misure tecniche e organizzative si deve tenere conto anche dei "costi di attuazione".

29 Secondo il Consiglio federale, i costi di attuazione devono essere intesi in senso lato e comprendono non solo le risorse finanziarie necessarie, ma anche le risorse di personale e di tempo. I costi devono essere presi in considerazione già al momento di determinare quali misure sono "appropriate" e quali no. Meyle/Morand/Vasella sottolineano giustamente che l'opinione del Consiglio federale secondo cui i responsabili e gli incaricati del trattamento dei dati "non possono esimersi dall'obbligo di garantire un'adeguata sicurezza dei dati a causa dei costi eccessivi" renderebbe priva di senso la disposizione dell'art. 1, cpv. 4, della LPD: è richiesta "solo" una sicurezza "adeguata" e i costi devono essere inclusi come criterio per determinare l'adeguatezza.

I "requisiti minimi per la sicurezza dei dati" non vengono quindi violati (e non sono punibili) se il responsabile del trattamento o l'incaricato del trattamento tengono conto anche dei costi nel determinare l'adeguata sicurezza dei dati e le misure appropriate. 30

III. REATO SOGGETTIVO

Dal punto di vista soggettivo, il reato di cui all'art. 61 richiede il dolo, mentre è sufficiente il dolo eventuale. L'autore del reato agisce con dolo eventuale se, pur non sapendo con certezza che il suo comportamento violerà le disposizioni sull'esportazione dei dati (art. 16 cpv. 1 e 2; art. 17) o sul trasferimento del trattamento dei dati a un incaricato del trattamento (art. 9 cpv. 1 e 2) o se non rispetta i requisiti minimi per la sicurezza dei dati (art. 8 cpv. 3 in combinato disposto con gli artt. 1 e segg. della FADP), accetta o ammette di poter commettere una violazione. 31

Nel caso del reato di cui all'art. 61 lett. b, sussiste il dolo eventuale se l'autore del reato, nel trasferire il trattamento dei dati a un incaricato del trattamento, accetta almeno che l'incaricato del trattamento (i) tratti i dati in violazione della legge o (ii) non garantisca la sicurezza dei dati. Decisive per rispondere alla domanda se tale accettazione esista sono le circostanze in cui l'incaricato del trattamento dei dati in questione è stato "esaminato" e infine scelto. Le disposizioni dell'art. 9 sono molto aperte e formulate in modo vago (soprattutto rispetto alla disposizione parallela dell'art. 28 del DSGVO), il che in pratica dovrebbe rendere difficile per le autorità penali provare la condotta criminale nei singoli casi (a parte il fatto che per quanto riguarda la giustiziabilità della variante del reato di inosservanza intenzionale dei requisiti minimi di sicurezza dei dati, esistono comunque dubbi fondati, cfr. supra n. 17 e seguenti). D'altro canto, si ipotizzerebbe una mera negligenza (non punibile) se l'autore del reato, sulla base di una consulenza legale esterna (sulla quale non dovevano sorgere dubbi), ritenesse che un determinato contratto per il trattamento dei dati fosse giuridicamente sufficiente, ma questo si rivelasse insufficiente. 32

IV. ILLEGALITÀ E COLPEVOLEZZA

Cfr. OK-Gassmann sull'art. 60, n. 26 e segg.

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 62 LPD

Un commentario di Jonas D. Gassmann

CITAZIONE SUGGERITA

Jonas D. Gassmann, Kommentierung zu Art. 62 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Gassmann, N. XXX zu Art. 62 DSG.

Art. 62 Violazione dell'obbligo del segreto

[1] Chiunque rivela intenzionalmente dati personali segreti dei quali è venuto a conoscenza nell'esercizio di una professione che richiede la conoscenza di tali dati, è punito, a querela di parte, con la multa fino a 250 000 franchi.

[2] È passibile della stessa pena chiunque intenzionalmente rivela dati personali segreti dei quali è venuto a conoscenza nell'ambito dell'attività svolta per conto della persona sottostante all'obbligo del segreto o in occasione della sua formazione presso tale persona.

[3] La rivelazione di dati personali segreti è punibile anche dopo la cessazione dei rapporti di lavoro o della formazione.

STRUTTURA

In breve 799
I. Aspetti generali 799
II. Violazione del segreto professionale 800
A. Cerchia dei trasgressori 800
B. Elementi oggettivi del reato 801
C. Elementi soggettivi del reato 803
III. Illegittimità e colpevolezza 803
IV. Delimitazione e concorrenza 804
Bibliografia 804
I Materiali 805

IN BREVE

La disposizione dell'art. 62 riguarda il cosiddetto "segreto professionale minore". Essa punisce la divulgazione intenzionale di dati personali segreti appresi nell'esercizio di una professione. Rispetto alla legge precedente, il reato di "violazione del segreto professionale" è notevolmente ampliato. Se viene commesso questo reato, può essere comminata una multa fino a 250.000 franchi.

I. ASPETTI GENERALI

La disposizione dell'art. 62 si basa sull'art. 35 aDSG, ma amplia notevolmente il reato di "violazione del segreto professionale". Non si tratta più solo di divulgare "dati personali segreti o profili della personalità che richiedono una particolare protezione", ma piuttosto "dati personali segreti" in generale. Il Consiglio federale ha giustificato questa estensione della protezione del segreto a tutti i tipi di dati personali con l'ulteriore sviluppo delle tecnologie dell'informazione e della comunicazione e la conseguente massiccia espansione della raccolta di dati. L'art. 62 mira a proteggere la privacy delle persone che affidano i propri dati personali a terzi. 1

La disposizione penale dell'art. 62 è un reato di applicazione. 2

Secondo il Consiglio federale, l'art. 62 mira a colmare le lacune "dovute alla ristretta cerchia di autori di reati di cui agli articoli 320 e 321 CP (reati speciali)". L'obbligo di riservatezza dovrebbe applicarsi anche alle persone che non rientrano negli articoli 320 o 321 CP. Il legislatore ha preferito questa soluzione a un ampliamento delle disposizioni penali (generali), non ritenendo opportuno ampliare anche il diritto di non testimoniare, che le leggi processuali prevedono generalmente per le professioni di cui all'art. 321 CP. Dal punto di vista terminologico, tuttavia, il "segreto professionale minore" si basa sul segreto professionale "maggiore" ai sensi dell'art. 321 CP (che si applica in particolare a medici, avvocati, ecclesiastici, ecc.) e sul segreto bancario ai sensi dell'art. 47 LBC. 3

Il Consiglio federale si era già astenuto dal menzionare la divulgazione dei dati trattati a fini commerciali nella preparazione della bozza. Le Camere parlamentari hanno mantenuto questa disposizione. 4

5 Il progetto preliminare prevedeva ancora una pena detentiva fino a tre anni o una multa in caso di violazione del segreto professionale (art. 52 LPD). Secondo la relazione esplicativa VE-DSG, l'inasprimento è stato voluto perché una multa non corrisponderebbe più alla gravità dei possibili interventi, soprattutto per quanto riguarda l'art. 321 CP. In sede di consultazione, tuttavia, diversi partecipanti hanno ritenuto la sanzione troppo elevata, motivo per cui è stata introdotta una multa di 250.000 franchi. Alla fine la multa massima di 250.000 franchi è stata mantenuta, poiché la maggioranza ha ritenuto che tale importo fosse proporzionato e sufficientemente dissuasivo.

6 Nel complesso, è sorprendente che la disposizione dell'art. 62, insolitamente severa in considerazione dell'ampio campo di applicazione e della gamma di ammende, soprattutto nel confronto internazionale, sia stata poco discussa (in termini di contenuto) nelle deliberazioni parlamentari.

II. VIOLAZIONE DEL SEGRETO PROFESSIONALE

A. Cerchia dei trasgressori

7 L'art. 62 LPD non copre tutte le persone che divulgano dati personali segreti di un'altra persona. Secondo la formulazione, esso riguarda le persone che esercitano una professione che richiede la divulgazione di dati personali segreti. L'art. 62 LPD è quindi concepito come un reato speciale. A differenza dell'art. 321 CP, tuttavia, non è richiesta una specifica appartenenza professionale. Per essere soggetti all'obbligo di riservatezza (che va oltre i segreti commerciali e di fabbricazione definiti nell'art. 321a cpv. 4 CO), dall'introduzione dell'art. 62 i dipendenti non devono più avere uno status particolare come quello di avvocati, medici, impiegati di banca o funzionari pubblici: è sufficiente che siano venuti a conoscenza di "dati personali segreti" nell'ambito della loro attività professionale. In virtù dell'art. 2 cpv. 1, anche i membri delle autorità federali rientrano nella disposizione penale dell'art. 62.

8 Ai sensi dell'art. 62 cpv. 3 non è coperto solo l'esercizio corrente della professione, ma la protezione del segreto continua anche se le persone obbligate hanno abbandonato la professione o hanno completato la relativa formazione. Ciò corrisponde al regolamento dell'art. 35 cpv. 3 aDSG. Si può presumere che ciò significhi (per analogia con l'art. 321 CP) che l'obbligo professionale di riservatezza continua a sussistere fino alla morte della

persona tenuta al segreto, indipendentemente dalla prosecuzione del rapporto d'affari.

Ai sensi dell'art. 62 cpv. 2, anche le persone ausiliarie (dipendenti; incaricati del trattamento dei dati) e i tirocinanti (compresi gli stagisti) sono soggetti alla responsabilità penale. Questa estensione corrisponde alla disposizione dell'Art. 35 cpv. 2 aDSG. I terzi che agiscono al posto del detentore principale dei segreti sono, secondo il parere qui espresso, soggetti all'obbligo di mantenere il segreto come persone ausiliarie. 9

Una persona non è perseguibile ai sensi dell'art. 62 se divulga dati personali segreti che la persona che detiene il segreto o una persona ausiliaria le ha rivelato in violazione dell'art. 62. 10

L'art. 62 LPD non prevede la responsabilità penale diretta dell'azienda. Per ovviare a ciò, la responsabilità penale degli organi direttivi è stata aumentata applicando l'art. 6 del Codice penale in aggiunta all'art. 29 del Codice penale. 11

B. Elementi oggettivi del reato

Ai sensi dell'art. 62 cpv. 1, è perseguibile "chiunque, intenzionalmente, divulghi dati personali segreti di cui sia venuto a conoscenza nell'esercizio della propria professione che richiede la conoscenza di tali dati". Gli elementi oggettivi del reato richiedono innanzitutto che i dati personali siano "segreti". Per dati personali si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile (art. 5 lett. a). L'art. 62 non definisce quali dati personali siano considerati "segreti", ma il messaggio fa riferimento al concetto materiale di segreto nel diritto penale. Un segreto protetto dal diritto penale esiste se (i) il fatto non è generalmente noto o accessibile, (ii) la persona che mantiene il segreto ha un interesse degno di protezione nella conoscenza limitata e (iii) ha anche la volontà di farlo. 12

Inoltre, l'autore del reato deve essere venuto a conoscenza dei dati personali nell'esercizio della sua professione. Ciò include, da un lato, i dati che il cliente/titolare del segreto ha affidato alla persona che detiene il segreto e, dall'altro, i dati che la persona che detiene il segreto ha ottenuto da sola nell'esercizio della sua professione. 13

Il termine "divulgazione" di dati personali segreti corrisponde a quello degli articoli 320 e 321 CP: La divulgazione si verifica quando la persona che 14

detiene il segreto porta i dati personali segreti a conoscenza di un terzo che non è autorizzato a farlo, o consente a quest'ultimo di prendere conoscenza dei dati, mentre è irrilevante il modo in cui ciò avviene (ad esempio, trasmissione diretta di dati personali segreti o conservazione insufficiente di file in modo che il terzo sia in grado di prendere conoscenza dei dati). Se i dati vengono effettivamente anonimizzati, pseudonimizzati o crittografati prima di essere trasmessi in modo che il terzo non possa prenderne conoscenza, ciò non costituisce divulgazione ai sensi del reato.

D'altro canto, anche la divulgazione di dati personali segreti a un dipendente interno o a un fornitore di servizi esterno costituisce un reato. Possono essere problematiche le situazioni in cui terzi rivelano dati personali a un dipendente in relazione a una richiesta di stretta riservatezza. Ad esempio, un dipendente del reparto risorse umane di un'azienda che viene informato da un altro dipendente di un'irregolarità all'interno dell'azienda e quest'ultimo chiede che la sua identità venga tenuta segreta. Da un lato, il dipendente del reparto risorse umane può essere perseguito se (comunque) divulga l'identità all'interno dell'azienda; dall'altro, l'azienda dovrà accettare il merito della conoscenza di alcuni dipendenti. In questo caso, sono necessarie regole chiare su come gestire tali segnalazioni e su cosa comunicare, a chi, quando e come.

15 Non è chiaro né dalla formulazione dell'art. 62, né dal messaggio, chi sia il titolare del segreto protetto da questa disposizione. Secondo il dispaccio, tuttavia, la disposizione dell'art. 62 è esplicitamente collegata al segreto professionale dell'art. 321 CP, motivo per cui è giustificato intendere l'art. 62 come "segreto professionale" e non come una norma puramente di protezione dei dati: La persona che ha affidato al professionista il suo segreto per l'esercizio della sua professione è il titolare del segreto. Di conseguenza, la fiducia del titolare del segreto nella riservatezza della comunicazione al professionista è protetta, e solo la violazione di questa fiducia (cioè non ogni violazione della protezione dei dati) è punibile. L'art. 62 tutela la fiducia riposta in un professionista affinché mantenga il segreto affidatogli per l'esercizio della sua professione, indipendentemente dall'esistenza di un rapporto contrattuale diretto con la persona a cui il segreto è affidato. Secondo il punto di vista adottato in questa sede, solo la divulgazione di dati personali che avviene in violazione di una giustificata aspettativa del titolare del segreto di essere trattato in modo confidenziale può costituire un reato.

Un'azienda può gestire le aspettative del cliente/titolare del segreto elencando le categorie di terzi a cui l'azienda divulga i dati personali nella sua politica sulla privacy. A condizione che il riferimento nella dichiarazione sulla privacy sia "sufficientemente chiaro", il titolare del segreto non potrà più rivendicare una "legittima aspettativa" che i dati personali in questione siano trattati in modo confidenziale.

Anche se l'art. 62 viene inteso in questo senso più ristretto, questa disposizione è comunque molto ampia e indeterminata: Non è stato chiarito (né lo era ai sensi dell'art. 35 aDSG) quando si possa presumere una fiducia nella riservatezza protetta dal diritto penale. Ciò che è chiaro, tuttavia, è che non tutti i fatti comunicati a un professionista che non sono generalmente noti meritano questa protezione. Con Rosenthal/Gubler (p. 61), è necessario (in considerazione dei requisiti per una disposizione penale derivanti dal requisito della certezza ai sensi dell'art. 1 CP) che (i) sia stata suscitata nel titolare del segreto una giustificata aspettativa che la sua volontà di mantenere il segreto sarà rispettata e (ii) il segreto sia stato rivelato al titolare del segreto o alla sua organizzazione in questo contesto. Ciò significa che deve esistere almeno un accordo tacito di riservatezza. 16

C. Elementi soggettivi del reato

Dal punto di vista soggettivo, è necessario il dolo dell'autore del reato, ossia che questi sia consapevole del dovere di riservatezza, della natura segreta dei dati personali e della divulgazione. È sufficiente che l'autore del reato ritenga possibile che terzi possano venire a conoscenza dei dati personali, ma agisca comunque perché lo accetta (dolo eventuale). In pratica, non è raro che la responsabilità penale venga meno perché non è possibile dimostrare la conoscenza dell'obbligo di riservatezza e della natura segreta dei dati personali, in particolare se non vi sono indicazioni che l'azienda in questione abbia trasmesso le relative conoscenze ai propri dipendenti. 17

III. ILLEGITTIMITÀ E COLPEVOLEZZA

Cfr. OK-Gassmann sull'art. 60, n. 26 s. La divulgazione può essere giustificata in particolare dal consenso del titolare del segreto, per cui si applicano, mutatis mutandis, i principi sviluppati dalla giurisprudenza e dalla dottrina nell'art. 321 n. 2 CP. Vengono chiamate in causa anche le norme giuridiche che consentono la divulgazione (art. 14 CP) o addirittura la rendono 18

obbligatoria. In questo caso si potrebbe pensare a un obbligo di cooperazione procedurale.

IV. DELIMITAZIONE E CONCORRENZA

20 Oltre all'art. 320 CP (violazione del segreto d'ufficio) e all'art. 321 CP (violazione del segreto professionale), l'art. 62 protegge anche il titolare di un segreto dalla divulgazione illecita di dati segreti a terzi. Tuttavia, l'art. 62 colma la lacuna creata dal reato ristretto e di conseguenza si pone in una concorrenza ideale e irreale con le due disposizioni del Codice penale. Analogamente all'art. 35 aDSG, la violazione della segretezza dei dati è assorbita negli artt. 320 e 321 CP (consumo).

21 Se sono soddisfatte anche le condizioni dell'Art. 47 BankA, questo ha la precedenza come norma speciale.

L'autore desidera ringraziare sentitamente l'avvocato Antonia Straden per il suo aiuto nel commentare questo articolo.

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 63 LPD

Un commentario di Jonas D. Gassmann

CITAZIONE SUGGERITA

Jonas D. Gassmann, Kommentierung zu Art. 63 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Gassmann, N. XXX zu Art. 63 DSG.

Art. 63 Inosservanza di decisioni

È punito con la multa fino a 250 000 franchi il privato che intenzionalmente non ottempera a una decisione dell'IFPDT, o a una decisione delle autorità di ricorso, notificatagli sotto comminatoria della pena prevista nel presente articolo.

STRUTTURA

In breve 809
I. Aspetti generali 809
II. inosservanza di un ordine dell'IFPDT o di una decisione di un organo di ricorso 810
A. Fatti oggettivi 810
1. Ordinanza dell'IFPDT o decisione di un organo di ricorso 810
2. Inosservanza 811
B. Elementi soggettivi del reato 812
III. Illiceità e colpevolezza 812
Bibliografia 812
I Materiali 812

IN BREVE

La disposizione dell'art. 63 rende punibile l'inosservanza deliberata di un ordine dell'IFPDT o di una decisione di un organo di ricorso. Per essere punibile, l'ordine o la decisione devono essere accompagnati da una corrispondente minaccia di punizione e il destinatario deve essere sufficientemente chiaro su ciò che deve fare o astenersi dal fare. Se questo requisito è soddisfatto, può essere comminata una multa fino a 250.000 franchi.

I. ASPETTI GENERALI

L'art. 63 è un reato di disobbedienza concepito come disposizione generale. Disposizioni penali analoghe si trovano spesso nel diritto penale derivato, anche se con pene molto più basse. In quanto lex specialis, la disposizione dell'art. 63 prevale sulla disposizione dell'art. 292 CP (disobbedienza agli ordini ufficiali) contenuta nel diritto penale fondamentale. 1

La disposizione dell'art. 63 è stata aggiunta alla legge solo dopo la consultazione. Secondo il legislatore, il ricorso all'art. 292 CP non sarebbe stato sufficiente perché la minaccia di pena era troppo bassa. Durante il processo di consultazione, sono state espresse diverse critiche sul fatto che le nuove disposizioni penali fossero formulate in modo troppo aperto. L'art. 63 consente ora all'LPD di ordinare il rispetto degli obblighi previsti dalla LPD e di collegarlo a una minaccia di pena. L'obbligo può quindi essere specificato nell'ordine nella misura in cui è sufficientemente chiaro per il destinatario cosa deve fare o astenersi dal fare. 2

La disposizione penale dell'art. 63 è un reato d'ufficio. 3

La disposizione dell'art. 63 ha lo scopo, da un lato, di compensare l'omissione di disposizioni penali (relative alle segnalazioni all'IFPDT) rispetto alla LPD e, dall'altro, di tenere conto "delle questioni relative al principio nulla poena sine lege, poiché sono state frequentemente sollevate in sede di consultazione". 4

Secondo il Consiglio federale, la soluzione creata con l'art. 63 consente "di continuare a redigere le disposizioni corrispondenti dell'e-DSA in forma sufficientemente generale senza entrare in conflitto con i requisiti di diritto penale per la precisione di una norma giuridica". Inoltre, secondo il Consiglio 5

federale, facilita il lavoro delle autorità di perseguimento penale competenti, che terranno conto delle preoccupazioni espresse in parte nella consultazione.

6 Questa disposizione è finalizzata all'esecuzione delle ordinanze dell'IFPDT ai sensi dell'art. 51, che l'IFPDT emette dopo lo svolgimento di un'indagine, e all'esecuzione delle decisioni degli organi di ricorso. Per contro, la minaccia di multa di cui all'art. 60 cpv. 2 riguarda la fornitura intenzionale di informazioni false e il rifiuto deliberato di collaborare a un'indagine dell'IFPDT.

7 Il reato di cui all'art. 63 è un reato speciale: solo coloro che sono destinatari di una decisione dell'IFPDT o di una decisione di una corte d'appello possono essere considerati autori del reato. Le altre persone possono essere considerate solo come istigatori. Se l'ordine dell'IFPDT o la decisione di un'istanza d'appello sono indirizzati a una società, la responsabilità penale sorge sulla base dell'art. 29 CP nel caso di un dirigente: L'obbligo che grava sulla società e che dà origine al reato è attribuito alla persona fisica. Una persona che non impedisce le violazioni da parte dei dipendenti subordinati o che non ne annulla gli effetti si qualifica come autore di reato (art. 6 cpv. 2 e 3 VStrR in combinato disposto con l'art. 64 cpv. 1 LPD).

II. INOSSERVANZA DI UN ORDINE DELL'IFPDT O DI UNA DECISIONE DI UN ORGANO DI RICORSO

A. Fatti oggettivi

1. Ordinanza dell'IFPDT o decisione di un organo di ricorso

8 Una sanzione ai sensi dell'art. 63 presuppone che un'ordinanza o una decisione validamente emessa e notificata prescriva un comportamento sufficientemente specifico per una determinata persona, con la minaccia di una sanzione ai sensi di questa disposizione in caso di inosservanza. Non vi è alcun obbligo da parte dell'IFPDT o degli organi d'appello di allegare la minaccia di sanzione di cui all'art. 63 alle loro ordinanze o decisioni. Tuttavia, per rendere più probabile l'osservanza delle ordinanze o delle decisioni, l'IFPDT o gli organi d'appello dovrebbero ricorrere regolarmente a questa possibilità.

Per ordine dell'IFPDT si intende un atto ufficiale indirizzato dall'IFPDT a una persona specifica sulla base dell'art. 51, con il quale viene regolato in modo giuridicamente vincolante ed esecutivo un determinato rapporto giuridico di diritto amministrativo. Come nel caso dell'art. 292 CP, è necessario che l'ordine contenga un'istruzione concreta di comportamento (fare, tollerare o astenersi dal fare qualcosa); un semplice ordine dichiarativo non soddisfa questo requisito. Anche un ordine generico non è un oggetto di reato adeguato. Un ordine specifico di agire comprende, ad esempio, un ordine di adeguare o cessare un determinato trattamento di dati personali o di astenersi dal divulgare dati personali all'estero (cfr. OK-Fanger/Oehri sull'art. 51 LPD). L'ordine deve essere "giuridicamente esistente" (cioè non deve contenere alcun grave difetto che lo renda nullo), deve essere stato effettivamente ricevuto dal destinatario e deve essere formalmente definitivo. 9

Per decisione di un'autorità di ricorso si intende una decisione di un tribunale che decide su un ricorso contro un'ordinanza dell'IFPDT, ossia una decisione del Tribunale amministrativo federale (art. 33 lett. d VGG) o del Tribunale federale (art. 86 cpv. 1 lett. a LTF). 10

Secondo l'art. 1 CP, la pena può essere presa in considerazione solo se la disposizione penale applicabile soddisfa il requisito della certezza. Poiché l'art. 63 non descrive il reato, ma si riferisce all'ordinanza dell'IFPDT o alla decisione di un organo d'appello, anche l'ordinanza o la decisione oggetto della sanzione deve soddisfare i requisiti del principio di certezza. Il principio di legalità richiede che l'obbligo imposto nell'ordine o nella decisione sia "sufficientemente chiaramente circoscritto" (cfr. supra, n. 9); in altre parole, deve essere chiaro al destinatario dell'ordine o della decisione quale sia il comportamento specifico che gli viene richiesto. 11

2. Inosservanza

Il reato di cui all'articolo 63 richiede che il destinatario dell'ordine o della decisione non si conformi all'ordine o alla decisione. Il significato di inosservanza dipende dal contenuto dell'ordine o della decisione. Ad esempio, se l'IFPDT ordina di vietare la divulgazione di dati personali all'estero, la divulgazione in questione costituisce una "inosservanza"; se l'autore del reato divulga più volte i dati personali all'estero nonostante il divieto, realizza più volte il reato di cui all'art. 63. 12

B. Elementi soggettivi del reato

13 Dal punto di vista soggettivo, il reato di cui all'articolo 63 richiede il dolo, mentre è sufficiente il dolo eventuale. L'autore del reato agisce con dolo eventuale se, pur non sapendo con certezza che il suo comportamento violerà l'ordine o la decisione, accetta o ammette di poter commettere una violazione.

III. ILLICEITÀ E COLPEVOLEZZA

Cfr. OK-Gassmann, art. 60 LPD, n. 26 e segg.

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 64 LPD

Un commentario di Jonas D. Gassmann

CITAZIONE SUGGERITA

Jonas D. Gassmann, Kommentierung zu Art. 64 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Gassmann, N. XXX zu Art. 64 DSG.

Art. 64 Infrazioni commesse nell'azienda

[1] Alle infrazioni commesse nell'azienda sono applicabili gli articoli 6 e 7 della legge federale del 22 marzo 1974 sul diritto penale amministrativo (DPA).

[2] Se la multa applicabile non supera i 50 000 franchi e se la determinazione delle persone punibili secondo l'articolo 6 DPA esige provvedimenti d'inchiesta sproporzionati all'entità della pena, l'autorità può prescindere da un procedimento contro dette persone e, in loro vece, condannare al pagamento della multa l'azienda (art. 7 DPA).

STRUTTURA

In breve 817
I. Aspetti generali 817
II. Reati negli esercizi commerciali 818
A. Applicabilità degli artt. 6 e 7 del Codice penale (cpv. 1) 818
B. Condanna dell'impresa a una multa (cpv. 2) 819
1. Generale 819
2. Reato nell'esercizio dell'attività commerciale 820
3. Multa di un massimo di 50.000 franchi 820
4. Le misure investigative per identificare le persone colpevoli sarebbero sproporzionate 821
5. Trasmissione dell'ammenda 822
Bibliografia 822
I Materiali 822

IN BREVE

Facendo riferimento a due disposizioni isolate della Legge federale sul diritto penale amministrativo (LSR), la LPD introduce la responsabilità dell'imprenditore. L'art. 64 consente, in determinate circostanze, di trasmettere all'azienda una multa da infliggere alla persona fisica responsabile in caso di reato in uno stabilimento commerciale, se tale multa ammonta a un massimo di 50.000 franchi svizzeri.

I. ASPETTI GENERALI

Poiché spetta ai Cantoni perseguire e giudicare i reati penali ai sensi del Capitolo 8 (art. 65 cpv. 1), la Legge federale del 22 marzo 1974 sul diritto penale amministrativo (AoA) non è in linea di principio applicabile (art. 1 AoA e contrario). Tuttavia, l'art. 64 cpv. 1 fa ora espresso riferimento agli artt. 6 e 7 del Codice di procedura penale per quanto riguarda i reati negli esercizi commerciali. 1

Con il riferimento all'art. 6 del Codice di procedura penale (determinazione del responsabile di un reato in un esercizio commerciale) e all'art. 7 del Codice di procedura penale (responsabilità sussidiaria dell'esercizio commerciale), la responsabilità del committente viene introdotta nella LPD. Ciò ha lo scopo di consentire "un'appropriata attribuzione della responsabilità penale nelle aziende", ossia al livello dirigenziale (persone di gestione con poteri decisionali e direttivi). 2

L'importo massimo dell'ammenda ai sensi del cpv. 2 (che modifica la disposizione dell'art. 7 del Codice penale), fino al quale l'impresa (anziché la persona fisica) può essere condannata al pagamento dell'ammenda, era ancora fissato a 100.000 franchi nell'art. 53 LPD. Le dichiarazioni controverse emerse durante il processo di consultazione hanno portato alla fine a fissare l'ammenda massima a 50.000 franchi. La multa massima notevolmente più alta rispetto all'art. 7 del Codice Penale si spiega con il fatto che la gamma di multe per le violazioni della LPD (multe fino a 250.000 franchi) supera di gran lunga l'importo previsto dall'art. 7 del Codice Penale (5.000 franchi), e la multa massima ha dovuto essere aumentata in modo che nella pratica ci sia ancora spazio per l'applicazione della disposizione dell'art. 64 cpv. 2. 3

II. REATI NEGLI ESERCIZI COMMERCIALI

A. Applicabilità degli artt. 6 e 7 del Codice penale (cpv. 1)

4 L'art. 64 cpv. 1 fa riferimento agli artt. 6 e 7 c.p. per i "reati negli esercizi commerciali", e quindi a due articoli isolati all'interno del c.p.. La valutazione della multa, ad esempio, non si basa sull'art. 8 ACC, ma sull'art. 106 cpv. 3 CP. Poiché il Codice di Procedura Penale, in base al suo art. 1, non è in linea di principio applicabile ai reati previsti dalla LPD, questo riferimento esplicito è necessario se si vuole introdurre una sorta di "responsabilità del committente" nella LPD (cfr. anche sopra, n. 1 e segg.).

5 Qualsiasi attività imprenditoriale in cui il capitale e il lavoro vengono utilizzati attivamente per partecipare alla vita economica è considerata una "operazione commerciale". Si tratta quindi di reati penali nell'esercizio di attività economiche in una società. L'art. 6 cpv. 1 del Codice Penale non contempla gli atti commessi solo in occasione dell'esercizio di attività economiche.

6 L'art. 6 cpv. 1 CPI stabilisce il cosiddetto principio dell'autore: l'autore è colui che ha commesso il reato. Ad esempio, un dipendente che, non richiesto e non autorizzato da un superiore, utilizza uno strumento di un fornitore di servizi online per lo svolgimento delle sue mansioni, nel corso del quale vengono elaborati dati personali, ma che non si è preoccupato di concludere un contratto legalmente sufficiente per l'elaborazione dei dati, è perseguibile penalmente (responsabilità penale ai sensi dell'art. 61 cpv. 1 lett. b). Un altro esempio potrebbe essere la divulgazione non autorizzata di dati personali segreti da parte di un dipendente a terzi nell'esercizio della sua professione (responsabilità penale ai sensi dell'art. 62).

7 Il prerequisito per la responsabilità del committente (responsabilità principale ai sensi dell'art. 6 cpv. 2 ACC) è, da un punto di vista oggettivo, l'esistenza di un dovere del garante, che non può essere desunto dall'art. 6 cpv. 2 ACC, ma deriva "dalla responsabilità per l'azienda come fonte di pericolo e/o dalla responsabilità per la condotta dei subordinati". Si potrebbe pensare a un responsabile della conformità che è contrattualmente responsabile di garantire il rispetto dei requisiti di protezione dei dati nell'azienda o al responsabile delle risorse umane che è contrattualmente responsabile del trattamento dei dati personali. La delega di responsabilità è consentita dalla

legge, ma il delegante rimane responsabile della selezione, dell'istruzione e della supervisione della persona in questione. Un altro prerequisito è l'esistenza di un potere da parte del committente: affinché si applichi la responsabilità del committente, quest'ultimo deve aver avuto la possibilità di impedire il reato o di annullarne gli effetti. Dal punto di vista soggettivo, è richiesto il dolo o la negligenza ai sensi dell'art. 6 cpv. 2 VStrR. Nel caso di reati che (come le disposizioni penali del capitolo 8 della LPD) sono strutturati come reati intenzionali, si discute tuttavia se per l'applicabilità della responsabilità del committente e quindi per la sua responsabilità penale sia sufficiente che quest'ultimo abbia semplicemente omesso per negligenza di impedire il reato o di annullarne gli effetti. Secondo l'opinione espressa in questa sede, per l'applicabilità della responsabilità del committente è necessario che quest'ultimo abbia almeno eventualmente violato intenzionalmente l'obbligo del garante. Se l'autore diretto (che ha commesso il reato) ha agito per mera negligenza, la responsabilità del committente per tali reati accidentali è esclusa fin dall'inizio.

Se il committente, il datore di lavoro, il cliente o la persona rappresentata è una persona giuridica, una società in nome collettivo o in accomandita semplice, un'impresa individuale o un gruppo di persone senza personalità giuridica, l'art. 6 cpv. 2 c.p. si applica "agli organi, ai membri degli organi, ai soci amministratori, alle persone effettivamente responsabili o ai liquidatori" (art. 6 cpv. 3 c.p.; cfr. anche art. 29 CP). 8

B. Condanna dell'impresa a una multa (cpv. 2)

1. Generale

L'art. 64 cpv. 2 si basa sulla disposizione dell'art. 7 cpv. 1 CPI, ma adatta il campo di applicazione alla pena pecuniaria massima prevista dalla LPD e parla più genericamente di "impresa" anziché di "persona giuridica", "società in nome collettivo o in accomandita" e "impresa individuale" (cfr. anche sopra, n. 3 e n. 5). 9

Ai sensi dell'art. 64 cpv. 2, una multa può essere comminata a un'azienda (invece che alle persone fisiche colpevoli) nel caso di un reato commesso 10

nell'ambito di un'attività commerciale (commesso da una o più persone fisiche; cfr. infra, n. 11 s.) se

- è ammessa una multa non superiore a 50.000 franchi (cfr. infra, n. 13 s.) e (cumulativamente)
- le indagini sulle persone perseguibili ai sensi dell'articolo 6 del Codice di procedura penale richiederebbero misure investigative sproporzionate rispetto alla pena comminata (cfr. infra, n. 15 s.).

2. Reato nell'esercizio dell'attività commerciale

11 Per comminare un'ammenda a un'impresa, è necessario innanzitutto che vi sia un "reato nell'esercizio dell'attività". Devono essere soddisfatti tutti gli elementi oggettivi e soggettivi del reato per il quale l'azienda deve essere multata e non devono sussistere motivi di giustificazione o di esclusione della colpevolezza. Per il termine "stabilimento commerciale" si veda sopra, n. 5.

12 In pratica, tuttavia, non sarà possibile provare gli elementi soggettivi del reato, poiché le persone fisiche colpevoli non sono precisamente identificabili. Per superare questo ostacolo e non escludere fin dall'inizio l'applicazione dell'art. 64, la colpevolezza deve essere "oggettivizzata" o i requisiti per provare gli elementi soggettivi del reato devono essere attenuati, ad esempio accontentando l'autorità penale dell'affermazione "che l'intenzione risulta chiaramente dal reato commesso". In ogni caso, tuttavia, non c'è spazio per l'applicazione dell'art. 64 se si stabilisce che gli elementi soggettivi del reato non sono soddisfatti nel caso delle persone presumibilmente punibili all'interno dell'impresa.

3. Multa di un massimo di 50.000 franchi

13 Ai sensi dell'art. 7 cpv. 1 CPI, il limite massimo della multa che può essere inflitta a una società anziché a una persona fisica è di 5.000 franchi. Questo limite massimo corrisponde alla metà della multa massima di 10.000 franchi prevista dall'art. 106 cpv. 1 CP. In deroga all'art. 106 cpv. 1 CP, l'importo massimo della multa nel campo di applicazione della LPD (ai sensi degli artt. 60-63) è di 250.000 franchi. Alla luce di questo importo massimo significativamente più elevato, si è proposto anche un aumento del limite massimo dell'importo della multa fino al quale è possibile una condanna di

un'impresa. Secondo l'art. 64 cpv. 2, questo limite massimo è di 50.000 franchi, che corrisponde a 1/5 della multa massima di 250.000 franchi.

Ai sensi dell'art. 106 cpv. 3 CP, il tribunale deve tenere conto delle circostanze dell'autore del reato nel determinare l'ammontare della multa "in modo che l'autore subisca la pena adeguata alla sua colpa". Poiché l'autore del reato non può essere identificato, l'ammenda deve essere valutata sulla base della colpevolezza oggettiva. Le circostanze del reato specifico, come la mancanza di una divisione interna in singole aree di responsabilità, sono decisive. 14

4. Le misure investigative per identificare le persone colpevoli sarebbero sproporzionate

Le circostanze del singolo caso sono rilevanti anche quando si esamina se le misure investigative per identificare gli autori del reato sarebbero sproporzionate rispetto alla pena inflitta. Poiché l'art. 64 cpv. 2 è una "disposizione facoltativa", le autorità giudiziarie hanno un margine di discrezionalità relativamente ampio nel determinare se tale disposizione debba essere applicata (e quindi anche nel rispondere alla domanda se le misure investigative per identificare gli autori del reato siano sproporzionate). Non esiste un diritto all'applicazione dell'art. 64 cpv. 2, né l'autorità penale può semplicemente scegliere se procedere contro le persone fisiche colpevoli o contro l'operazione commerciale. Prima che l'autorità penale competente possa considerare di punire l'attività commerciale sulla base dell'art. 64, deve eseguire "un minimo di misure investigative" per identificare le persone fisiche colpevoli; non è accettabile che l'autorità penale si basi sull'art. 64 per pura convenienza. Quando le (ulteriori) misure investigative sarebbero sproporzionate deve essere valutato anche in considerazione dell'importo della multa (potenzialmente) confiscata, per la quale le indagini devono in ogni caso essersi spinte a tal punto da poterne stimare almeno approssimativamente l'ammontare. 15

Nel caso di violazioni della LPD soggette a sanzioni, sarà spesso chiaramente determinato dal punto di vista organizzativo o almeno relativamente facile determinare nel caso specifico chi ha eseguito le azioni in questione (ad esempio, la risposta a una richiesta di informazioni o il rilascio della dichiarazione sulla protezione dei dati). A questo proposito, è probabile che la rilevanza pratica della disposizione dell'art. 64 sia piuttosto bassa; le condanne 16

delle imprese al pagamento di una multa rimarranno probabilmente un'eccezione.

5. Trasmissione dell'ammenda

17 Se le condizioni sopra descritte sono soddisfatte, l'autorità penale competente può trasferire l'ammenda all'impresa. Per determinare l'importo dell'ammenda, sono determinanti la colpevolezza e le condizioni finanziarie della persona o delle persone fisiche che hanno effettivamente commesso il reato, e non quelle dell'impresa.

18 Se è possibile identificare solo alcune persone fisiche responsabili dell'illecito, ma non altre, è discutibile se sia possibile trasferire l'ammenda applicabile alle persone non identificate. L'approccio corretto è quello di richiedere che il trasferimento sia possibile anche in questa costellazione.

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 65 LPD

Un commentario di Jonas D. Gassmann

CITAZIONE SUGGERITA

Jonas D. Gassmann, Kommentierung zu Art. 65 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Gassmann, N. XXX zu Art. 65 DSG.

Art. 65 Competenza

[1] Il perseguimento e il giudizio dei reati competono ai Cantoni.

[2] L'IFPDT può sporgere denuncia presso l'autorità di perseguimento penale competente e avvalersi nel procedimento dei diritti dell'accusatore privato.

STRUTTURA

In breve 827
I. Aspetti generali 827
II. competenza per l'azione penale e giurisdizione 828
A. Competenza cantonale (cpv. 1) 828
B. Giurisdizione multipla 828
III. diritti dell'IFPDT (cpv. 2) 829
A. Diritto di denuncia 829
B. Costituzione come procuratore privato 829
Bibliografia 829
I Materiali 830

IN BREVE

Come già previsto dalla Costituzione federale e dal Codice di procedura penale, il perseguimento e il giudizio dei reati penali sono di competenza dei Cantoni ai sensi del capitolo 8 della Legge sulla protezione dei dati. L'IFPDT ha il diritto di sporgere denuncia e può costituirsi come procuratore privato in un procedimento penale.

I. ASPETTI GENERALI

La disposizione dell'art. 65 cpv. 1 deriva dall'art. 123 cpv. 2, della Costituzione federale, secondo cui la competenza per la giurisdizione in materia penale e per l'esecuzione di pene e misure spetta in primo luogo e principalmente ai Cantoni. Coincide con la disposizione dell'art. 22 del Codice di procedura penale. L'art. 65 cpv. 1 è di natura puramente dichiarativa, in quanto questa disposizione non stabilisce una competenza federale e quindi non si discosta dalla competenza cantonale già prevista dalle disposizioni citate. Anche in assenza di una norma esplicita, in altre parole, i Cantoni sarebbero competenti per il perseguimento e il giudizio dei reati previsti dal Capitolo 8. 1

La disposizione dell'art. 65 cpv. 1 era già prevista in questo modo nel progetto preliminare. Nel corso della procedura di consultazione, la maggioranza dei Cantoni si è opposta all'idea che il perseguimento e il giudizio degli atti punibili continuassero a essere di competenza dei Cantoni. Il motivo di questa opposizione era il timore che i procedimenti penali potessero aumentare a causa del maggior numero di atti illeciti e delle sanzioni più severe, che avrebbero richiesto l'impiego di personale specializzato. È stato inoltre sostenuto che la giurisdizione cantonale renderebbe più difficile l'applicazione uniforme della legge sulla protezione dei dati. 2

L'art. 65 cpv. 2 rafforza la posizione dell'IFPDT conferendogli espressamente il diritto di sporgere denuncia penale e di costituirsi in un procedimento penale come parte civile ai sensi dell'art. 118 CCP e segg. 3

La disposizione dell'art. 65 cpv. 2 non era ancora stata inserita nel progetto preliminare, ma solo nella bozza. Nel corso del processo di consultazione sono state avanzate diverse richieste di conferire all'IFPDT la facoltà di imporre sanzioni amministrative. In contrasto con il diritto europeo, tuttavia, 4

si è deciso di non dare all'IFPDT la possibilità di imporre sanzioni. La mancanza di competenza per imporre sanzioni amministrative è stata invece compensata dall'introduzione di altre disposizioni nella LPD. Tra queste figurano l'art. 65 cpv. 2, in base al quale l'IFPDT può sporgere denuncia presso le autorità penali cantonali ed esercitare i diritti di un querelante privato in un procedimento penale, o le disposizioni penali di cui all'art. 60 cpv. 2 e all'art. 63.

II. COMPETENZA PER L'AZIONE PENALE E GIURISDIZIONE

A. Competenza cantonale (cpv. 1)

5 Sia l'azione penale che il giudizio sui reati di cui al capitolo 8 sono di competenza dei Cantoni (la cosiddetta giurisdizione cantonale originaria).

6 In linea di principio, non è quindi applicabile la legge federale del 22 marzo 1974 sul diritto penale amministrativo (la cui applicabilità richiederebbe che la suddetta giurisdizione spetti a un'autorità amministrativa della Confederazione, art. 1 LAC). Tuttavia, in virtù di un esplicito riferimento all'art. 64 cpv. 1, gli articoli 6 e 7 del Codice di procedura penale si applicano ai reati commessi negli esercizi commerciali. Questo riferimento non modifica la giurisdizione cantonale di cui sopra.

7 La giurisdizione locale è regolata dalle norme generali sulla giurisdizione di cui agli artt. 31 e seguenti del Codice di procedura penale. Codice di procedura penale.

B. Giurisdizione multipla

8 L'art. 65 non si pronuncia sulla situazione in cui in un caso penale esistono sia la giurisdizione cantonale che quella federale. In questo caso, si tratta di un autore di reato che viola non solo uno o più reati del capitolo 8, ma anche uno o più reati soggetti alla giurisdizione federale.

9 In assenza di una disposizione esplicita, si deve applicare l'art. 26 cpv. 2 del Codice di procedura penale: In base ad esso, il Ministero pubblico della Confederazione "può ordinare l'unificazione dei procedimenti in mano alle autorità federali o cantonali".

III. DIRITTI DELL'IFPDT (CPV. 2)

A. Diritto di denuncia

L'IFPDT ha il diritto (ma non l'obbligo) di presentare una denuncia all'autorità giudiziaria competente. Tuttavia, non ha il diritto di presentare una denuncia penale. Il diritto di sporgere denuncia penale spetta solo all'interessato i cui diritti (come il diritto all'informazione, il diritto all'accesso, il diritto alla sicurezza del trasferimento dei propri dati personali a terzi) sono stati violati. 10

Spetta all'autorità giudiziaria penale competente avviare un'indagine penale se ha indizi concreti che possa essere stato commesso un reato (art. 7 cpv. 1 CCP). Ai sensi dell'art. 8 CCP, il pubblico ministero può astenersi dall'esercitare l'azione penale e, in particolare, interrompere un procedimento penale già avviato, ad esempio se il caso è di lieve entità o se l'autore del reato ha riparato il danno causato e non vi sono interessi in conflitto con l'interruzione del procedimento penale. 11

B. Costituzione come procuratore privato

L'IFPDT ha anche il diritto di partecipare al procedimento penale cantonale come parte civile (e quindi come parte, art. 104 cpv. 1 lett. b CCP) ai sensi dell'art. 118 CCP. Se lo ritiene necessario ai fini di un'applicazione uniforme della LPD, l'Ufficio federale di polizia può ad esempio 12

- impugnare gli ordini di cessazione (art. 322 cpv. 2 CCP) e ricorrere contro le sentenze cantonali (art. 382 cpv. 1 CCP);
- chiedere la consultazione di fascicoli (art. 101 cpv. 1 Codice di procedura penale);
- partecipare agli atti processuali (Art. 107 cpv. 1 lett. b CCP) e all'assunzione di prove (Art. 147 e segg. CCP); e
- presentare richieste di prova (art. 107 cpv. 1 lett. e CCP).

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 66 LPD

Un commentario di Jonas D. Gassmann

CITAZIONE SUGGERITA

Jonas D. Gassmann, Kommentierung zu Art. 66 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Gassmann, N. XXX zu Art. 66 DSG.

Art. 66 Prescrizione dell'azione penale

L'azione penale si prescrive in cinque anni.

STRUTTURA

In breve 833
I. Aspetti generali 833
II. Termine di prescrizione per l'esercizio dell'azione penale 833
A. Durata 833
B. Inizio 834
C. Reati ripetuti 834
III. Limitazione dell'esecuzione 835
Bibliografia 835
I Materiali 835

IN BREVE

I reati contro la legge sulla protezione dei dati sono reati minori. In deroga alla disposizione generale dell'art. 109 CP, il termine di prescrizione per l'azione penale non è di tre anni, ma di cinque anni. Questo perché le indagini su possibili violazioni della legge sulla protezione dei dati sono di solito tecnicamente complesse, richiedono conoscenze specialistiche e il procedimento penale non dovrebbe fallire a causa di un periodo di prescrizione troppo breve. Il termine di prescrizione per l'esecuzione, che è di tre anni, deve essere distinto dal termine di prescrizione per l'azione penale.

I. ASPETTI GENERALI

L'art. 66 stabilisce un termine di prescrizione speciale per il perseguimento delle violazioni della legge sulla protezione dei dati. La disposizione si applica alle violazioni della legge sulla protezione dei dati punite ai sensi del capitolo 8 (artt. 60-63). Rispetto ai reati "ordinari", il termine è di due anni più lungo. Questo per tenere conto della natura tecnica di questi reati e dell'esperienza solitamente limitata delle autorità giudiziarie cantonali competenti in materia di protezione dei dati. 1

L'art. 66 è nuovo. Secondo la legge precedente, l'azione penale ai sensi dell'art. 333 cpv. 1 CP si prescriveva dopo tre anni in base alla relativa disposizione del diritto penale generale (art. 109 CP). Durante la procedura di consultazione, alcuni partecipanti si sono espressi contro l'estensione della prescrizione. La formulazione della bozza preliminare è rimasta invariata dopo le delibere parlamentari. 2

II. TERMINE DI PRESCRIZIONE PER L'ESERCIZIO DELL'AZIONE PENALE

A. Durata

I reati contro la legge sulla protezione dei dati, punibili ai sensi del capitolo 8, prevedono una sanzione pecuniaria e sono pertanto qualificati come trasgressioni ai sensi dell'art. 333 cpv. 3 CP. 3

4 Ai sensi dell'art. 109 CP, il termine di prescrizione per il perseguimento penale delle violazioni è di tre anni. Le indagini su eventuali violazioni della legge sulla protezione dei dati richiedono regolarmente la conoscenza dei processi tecnici sottostanti e non di rado sono complesse. Le autorità cantonali preposte all'applicazione delle disposizioni penali di cui all'art. 65 cpv. 1 (a differenza, ad esempio, delle autorità di controllo della protezione dei dati responsabili dell'imposizione di sanzioni pecuniarie ai sensi del DSGVO) hanno spesso poca o nessuna esperienza in materia di diritto della protezione dei dati (cfr. anche sopra, n. 1). Per garantire che i corrispondenti procedimenti penali non falliscano a causa di termini di prescrizione eccessivamente brevi, il termine di prescrizione per l'azione penale è stato aumentato di due anni, portandolo a cinque anni rispetto alla disposizione generale dell'art. 109 CP.

B. Inizio

5 Ai sensi dell'art. 104 CP, la decorrenza del termine di prescrizione dell'azione penale è disciplinata dall'art. 98 CP: Nel caso di reati concepiti come reati di attività, il termine di prescrizione decorre dal giorno in cui il reato è stato commesso o dall'ultimo giorno in cui è stato commesso. Se si tratta di un reato continuato, il termine di prescrizione decorre dal giorno in cui termina la condotta criminosa. Nel caso di reati omissivi, il termine di prescrizione non decorre finché l'omissione continua; il punto decisivo è la data in cui termina l'obbligo di agire. Se più persone sono coinvolte in un reato, il termine di prescrizione inizia a decorrere uniformemente per tutti i partecipanti con l'ultimo atto parziale.

C. Reati ripetuti

6 I reati ripetuti che sono diretti contro lo stesso oggetto giuridico devono essere distinti dai reati continuati. Questi ultimi si prescrivono singolarmente dopo la scadenza del termine di prescrizione di cinque anni. Ad esempio, se l'autore del reato affida ripetutamente il trattamento dei dati a un incaricato del trattamento ai sensi dell'art. 61 lett. b LPD senza soddisfare i requisiti di cui all'art. 9 cpv. 1 e 2 LPD, i singoli reati si prescrivono uno dopo l'altro, indipendentemente l'uno dall'altro.

III. LIMITAZIONE DELL'ESECUZIONE

L'art. 66 disciplina solo la prescrizione dell'azione penale, non anche quella dell'esecuzione. Quest'ultimo è disciplinato dalla disposizione generale dell'art. 109 CP. Il termine è di tre anni a partire dal giorno in cui la decisione che impone la multa diventa esecutiva (art. 333 cpv. 1 in combinato disposto con l'art. 109 e l'art. 100 CP), ossia dal giorno in cui la decisione diventa definitiva. Il ricorso al Tribunale federale contro la decisione di multa non ha effetto sospensivo (cfr. art. 103 LTF), per cui la decisione di multa diventa giuridicamente vincolante non appena viene emessa dall'ultima istanza cantonale. 7

BIBLIOGRAFIA

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.

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 67 LPD

Un commentario di Nula Katharina Frei

CITAZIONE SUGGERITA

Nula Frei, Kommentierung zu Art. 67 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Frei, N. XXX zu Art. 67 DSG.

Capitolo 9: Conclusione di trattati internazionali

Art. 67

Il Consiglio federale può concludere trattati internazionali concernenti:

a. la cooperazione internazionale tra le autorità incaricate della protezione dei dati;

b. il riconoscimento reciproco della protezione adeguata nel caso di comunicazione di dati personali all'estero.

STRUTTURA

In breve 839
I. Aspetti generali 839
A. Scopo dell'art. 67 LDP 839
B. Storia delle origini 840
II. Competenza del Consiglio federale a concludere trattati internazionali 841
A. Cooperazione internazionale tra autorità di protezione dei dati (lett. a) 843
1. Cooperazione 844
2. Autorità di protezione dei dati 846
B. Riconoscimento reciproco di un livello di protezione adeguato (lett. b) 847
C. Trattati di Stato per altri scopi 849
Bibliografia 850
I Materiali 852

IN BREVE

Alla luce dei flussi di dati sempre più internazionali, una protezione dei dati efficace deve disciplinare anche le questioni transfrontaliere. Ciò può richiedere accordi con altri Stati o organizzazioni internazionali. Per facilitare la conclusione di tali accordi, l'art. 67 LDP conferisce al Consiglio federale il potere di concludere trattati internazionali senza l'approvazione del Parlamento per due specifiche aree tematiche, in particolare ai fini della cooperazione tra le autorità di protezione dei dati e del riconoscimento reciproco di un livello adeguato di protezione dei dati. La norma di delega deve essere interpretata in modo restrittivo.

I. ASPETTI GENERALI

A. Scopo dell'art. 67 LDP

Nell'era della rete elettronica onnipresente, il trattamento transfrontaliero dei dati personali è diventato parte della vita quotidiana. Da tempo la protezione dei dati ha quindi anche una dimensione internazionale ed è quindi diventata oggetto di politica estera. 1

La Svizzera ha concluso numerosi accordi bilaterali e multilaterali nel settore della protezione dei dati. Si può distinguere tra accordi generali, che standardizzano o costituzionalizzano la protezione dei dati in tutti i settori del diritto, e accordi specifici, che stabiliscono norme per singoli ambiti di cooperazione. Solo la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato dei dati personali (ETS 108), di cui la Svizzera ratificherà presto la versione aggiornata (ETS 108+), rientra attualmente nella prima categoria. Regolamenti specifici sulla protezione dei dati si trovano in numerosi accordi nell'ambito della cooperazione di polizia e dell'assistenza giudiziaria in materia penale, del rilascio di visti, della gestione dell'immigrazione e della riammissione di cittadini stranieri, della cooperazione in materia di asilo e dello scambio di dati sui passeggeri aerei. 2

Un attore importante nella protezione dei dati è l'Unione europea. La sua legge sulla protezione dei dati ha un'influenza significativa sul diritto svizzero. A parte le influenze indirette e l'effetto extraterritoriale del Regolamento 3

generale sulla protezione dei dati (GDPR), che non saranno discussi in modo approfondito in questa sede, esistono anche diversi accordi tra la Svizzera e l'UE con contenuti relativi alla protezione dei dati. Il più importante dal punto di vista pratico è l'Associazione Schengen, in base alla quale la Svizzera adotta alcuni atti giuridici dell'UE, in particolare la direttiva 2016/680 sulla protezione dei dati nei settori della polizia e della giustizia, che deve essere attuata dalla Confederazione e dai Cantoni.

4 Rispetto al regolamento generale sulla conclusione di trattati internazionali in Svizzera (infra n. 10 e segg.), l'art. 67 LPD facilita la conclusione di trattati internazionali conferendo al Consiglio federale la competenza di concludere trattati autonomamente senza l'approvazione dell'Assemblea federale in due ambiti tematici specifici, ossia ai fini della cooperazione tra le autorità di protezione dei dati e del riconoscimento reciproco di un livello adeguato di protezione dei dati.

B. Storia delle origini

5 L'art. 67 LDP sostituisce l'art. 36 cpv. 5 aDSG, considerato troppo vago in base agli attuali principi di delega, ossia il divieto di deleghe in bianco. L'art. 36 cpv. 5 aDSG prevedeva che il Consiglio federale potesse concludere trattati internazionali sulla protezione dei dati se conformi ai principi della LADP.

6 I restanti paragrafi dell'art. 36 aDSG, che autorizzavano il Consiglio federale a emanare disposizioni di attuazione sia di carattere generale che in relazione a specifici ambiti tematici, non sono stati ripresi nella nuova LADP.

7 Nel processo legislativo, l'art. 67 LDP non è stato oggetto di controversie. Il suggerimento di limitare l'autorità del Consiglio federale di concludere accordi al fine di non concludere accordi di diritto internazionale sull'esecuzione in Svizzera di sanzioni imposte da autorità di vigilanza straniere, avanzato in alcuni casi durante il processo di consultazione, non è stato ascoltato né nel messaggio né nelle deliberazioni parlamentari. Rispetto al progetto preliminare e al progetto del Consiglio federale, l'art. 67 (ad eccezione della numerazione) non ha subito modifiche nelle deliberazioni parlamentari e, secondo i verbali del Consiglio, non è stato discusso.

II. COMPETENZA DEL CONSIGLIO FEDERALE A CONCLUDERE TRATTATI INTERNAZIONALI

Un trattato internazionale è un accordo concluso per iscritto tra due o più soggetti di diritto internazionale ai sensi dell'art. 38 cpv. 1 lett. a dello Statuto della CIG e dell'art. 2 cpv. 1 lett. a della Convenzione di Vienna sul diritto dei trattati. 8

Mentre l'art. 67 LADP utilizza il termine "trattato internazionale", à l'art. 16 cpv. 2 lett. a LADP parla di "trattato internazionale". Nonostante la diversa terminologia, il significato è lo stesso. 9

In linea di principio, il Consiglio federale e l'Assemblea federale sono congiuntamente responsabili della conclusione di trattati internazionali in Svizzera. Mentre il Consiglio federale, nell'ambito delle sue competenze di politica estera, negozia e firma i trattati internazionali (art. 184 cpv. 1 e 2 BV), il Parlamento approva i trattati mediante un decreto federale (art. 166 cpv. 2 frase 1 BV) prima che il Consiglio federale possa ratificarli (art. 184 cpv. 2 BV). Ciò si spiega con il fatto che i trattati internazionali, proprio come le leggi federali, contengono disposizioni legislative e quindi richiedono almeno una successiva legittimazione democratica. In alcuni casi, oltre all'approvazione parlamentare, è previsto il referendum facoltativo o obbligatorio sui trattati internazionali. Se un trattato internazionale è soggetto a referendum, se riguarda interessi importanti dei Cantoni o se è di grande importanza politica, finanziaria, economica, ecologica, sociale o culturale, deve essere effettuata una consultazione preventiva. 10

Il Parlamento può tuttavia rinunciare a questa competenza mediante delega. Di conseguenza, l'obbligo di approvazione non si applica ai trattati la cui conclusione è stata delegata dal Parlamento al Consiglio federale mediante una legge federale o un trattato internazionale approvato dal Parlamento. L'idea è quella di sollevare l'Assemblea federale dall'approvazione di trattati "non meritevoli di approvazione parlamentare" e di occuparsi solo di questioni che richiedono una maggiore legittimità democratica. 11

Questa competenza indipendente a concludere trattati è illustrata in modo più dettagliato nell'art. 7a RVOG, che indica tre costellazioni in cui il Consiglio 12

federale può ratificare un trattato senza l'approvazione preventiva del Parlamento.

- In primo luogo, sulla base di un'autorizzazione contenuta in una legge federale specifica (art. 7a cpv. 1 RVOG). L'art. 67 LDP è un'autorizzazione di questo tipo. In questo caso, sono decisivi i principi paralleli a quelli delle deleghe legislative al Consiglio federale: le valutazioni essenziali di politica legale devono essere fatte con sufficiente certezza nella legge parlamentare. Le cosiddette "deleghe in bianco" non sono compatibili con il principio di legalità, perché potrebbero avere l'effetto di sottrarre all'obbligo di approvazione un numero imprevedibile di trattati internazionali con contenuti diversi.
- In secondo luogo, un'autorizzazione in un trattato internazionale approvato dall'Assemblea federale (art. 7a cpv. 1 RVOG). In questo caso si applicano principi di delega sostanzialmente analoghi a quelli delle deleghe di competenza in un atto federale.
- In terzo luogo, il Consiglio federale può ratificare i cosiddetti trattati di portata limitata senza la previa approvazione del Parlamento (art. 7a cpv. 2 RVOG). Si tratta di una clausola generale sussidiaria, in quanto si applica a tutti i trattati di portata limitata, indipendentemente dal settore in questione. Secondo l'art. 7a cpv. 3 RVOG, i contratti di portata limitata comprendono i contratti che non creano nuovi obblighi o non comportano una rinuncia a diritti esistenti (art. 7a cpv. 3 lett. a RVOG), i contratti che servono solo ad eseguire contratti approvati dall'Assemblea federale e si limitano a precisare i diritti, gli obblighi o i principi organizzativi già stabiliti nel contratto di base (lett. b), e i contratti che sono rivolti alle autorità e regolano questioni tecnico-amministrative (lett. c). Questo elenco è esemplificativo: se un contratto ha effettivamente un ambito di applicazione limitato deve essere determinato dall'interpretazione. La legge specifica anche quali contratti non sono in linea di principio considerati di portata limitata (art. 7a cpv. 4 RVOG). Questo è il caso, in particolare, se il trattato è soggetto a referendum facoltativo sul trattato di Stato ai sensi dell'art. 141 cpv. 1 lett. d della Costituzione federale (lett. a), se contiene disposizioni che rientrano nelle competenze cantonali (lett. b) o se comporta spese elevate (lett. c). Altri criteri sono se un trattato interferisce con gli interessi giuridicamente protetti dei privati, se richiede

una modifica della legge o se si inserisce "senza problemi" nel contesto generale della politica interna ed estera e dell'economia.

In termini puramente quantitativi, la stragrande maggioranza (oltre il 90%) dei trattati stipulati dalla Svizzera è conclusa autonomamente dal Consiglio federale. Il Consiglio federale presenta ogni anno all'Assemblea federale un rapporto sui trattati conclusi autonomamente (art. 48a cpv. 2 RVOG). In questa forma, il controllo parlamentare è esercitato retroattivamente. 13

Il Consiglio federale può anche delegare la competenza di concludere trattati internazionali a un dipartimento. Se il trattato ha una portata limitata ai sensi dell'art. 7a cpv. 2 RVOG, può inoltre delegare tale competenza a un gruppo o a un ufficio federale (art. 48a cpv. 1 RVOG). 14

La disposizione precedente, l'art. 36 cpv. 5 aDSG, stabiliva che il Consiglio federale può concludere autonomamente trattati internazionali "a condizione che siano conformi ai principi della legge". Tale disposizione è stata interpretata dalla dottrina nel senso che i trattati internazionali dovevano rispettare i principi generali della protezione dei dati, ossia i principi di legalità, buona fede, riconoscibilità, proporzionalità, limitazione delle finalità, esattezza dei dati, sicurezza dei dati, tutela dei diritti delle persone interessate e divieto di divulgazione dei dati all'estero in caso di rischio di gravi violazioni della personalità. Sebbene questo requisito non sia stato incorporato nella nuova disposizione, per l'art. 67 LADP deriva comunque dalla natura della delega e, in ultima analisi, dal principio della separazione dei poteri: in assenza di una disposizione esplicita, il Consiglio federale non è autorizzato a concludere accordi che contraddicano le disposizioni generali della legge senza l'approvazione del Parlamento. Poiché i principi della protezione dei dati derivano direttamente dalla Costituzione (artt. 5, 13, 36 Cost.) e dalle disposizioni di diritto internazionale della Convenzione sulla protezione dei dati (art. 5 STE 108+), anche l'approvazione parlamentare non cambierebbe il fatto che i trattati internazionali che contraddicono i principi della protezione dei dati non possono essere conclusi in linea di principio. 15

A. Cooperazione internazionale tra autorità di protezione dei dati (lett. a)

Secondo l'art. 67 lett. a LDP, il Consiglio federale può concludere trattati internazionali che regolano la cooperazione internazionale tra le autorità di 16

protezione dei dati. Si pongono questioni di delimitazione per quanto riguarda il termine "cooperazione" (a) e la cerchia delle autorità coinvolte (b).

1. Cooperazione

17 La natura sempre più transfrontaliera del trattamento dei dati rende indispensabile la cooperazione internazionale tra le autorità di protezione dei dati. La cooperazione è pertanto una delle pietre miliari della moderna Convenzione del Consiglio d'Europa ETS 108+, che obbliga gli Stati contraenti del Capitolo V a cooperare e a prestarsi reciproca assistenza (cfr. art. 16 cpv. 1 ETS 108+). Analogamente, l'Unione europea, nella sua legislazione modernizzata sulla protezione dei dati, pone grande enfasi sulla cooperazione istituzionalizzata tra le autorità nazionali di protezione dei dati (cfr. art. 60 e segg. GDPR e art. 50 e segg. della direttiva sulla protezione dei dati - che è vincolante per la Svizzera nel settore della polizia e del perseguimento penale). DIRETTIVA 2016/680).

18 La cooperazione tra le autorità di protezione dei dati può assumere varie forme. L'art. 17 della Convenzione ETS 108+ elenca le seguenti forme di cooperazione come esempi: La fornitura di assistenza reciproca, in particolare sotto forma di scambio di informazioni, coordinamento di indagini o operazioni o attuazione di misure congiunte, nonché la fornitura reciproca di informazioni e documentazione sul diritto nazionale e sulla prassi amministrativa.

19 La Convenzione ETS 108+ obbliga le parti contraenti a formare una rete di autorità di vigilanza per organizzare la loro cooperazione (art. 17 cpv. 3). Gli ulteriori dettagli della cooperazione, in particolare per quanto riguarda le forme e le procedure e le lingue da utilizzare, devono essere stabiliti direttamente tra le Parti contraenti interessate (art. 21 cpv. 3). La conclusione di trattati internazionali è necessaria per regolare tali questioni. L'art. 67 lett. a LFPR consente al Consiglio federale di concludere tali accordi in modo semplificato, attuando così anche l'obbligo previsto dalla Convenzione ETS 108+.

20 In termini di diritto interno, uno dei compiti giuridicamente definiti dell'IFPDT è quello di collaborare con le autorità estere responsabili della protezione dei dati (à art. 58 cpv. 1 lett. b LDP). In pratica, l'IFPDT collabora con singole autorità nazionali e sovranazionali per la protezione dei dati, in

particolare con le autorità per la protezione dei dati degli Stati membri di Schengen e con il Comitato europeo per la protezione dei dati (EDSA). È inoltre coinvolto in organismi internazionali come il Consiglio d'Europa, la Conferenza europea e internazionale dei commissari per la protezione dei dati, l'Associazione francofona delle autorità di protezione dei dati e l'OCSE.

L'IFPDT ha anche la competenza di fornire assistenza amministrativa alle autorità straniere per la protezione dei dati, a condizione che siano soddisfatti i requisiti dell'art. 55 LDP. A tal fine può essere necessario un trattato di diritto internazionale, che il Consiglio federale può concludere più facilmente ai sensi dell'art. 67 lett. a. 21

In relazione alle suddette competenze giuridiche della DFP, l'art. 67 lett. a LADP fornisce la base giuridica nel caso in cui la cooperazione internazionale vada al di là di una cooperazione puramente informale (ad esempio lo scambio di buone pratiche) e debba quindi essere posta su una base formale. La conclusione di un trattato internazionale è particolarmente necessaria se si vogliono stabilire diritti e obblighi reciproci su base permanente e se si vogliono scambiare con altri Stati dati personali o dati altrimenti protetti (come i segreti aziendali). Per il trasferimento di dati personali, devono essere osservati anche i requisiti dell'art. 16 LADP. 22

Finora non sono stati conclusi accordi di cooperazione di questo tipo nel settore della protezione dei dati. Come modello per un accordo di cooperazione, il dispaccio cita anche un accordo di un altro settore giuridico, ovvero l'accordo del 17 maggio 2013 tra la Confederazione Svizzera e l'Unione Europea sulla cooperazione nell'applicazione del loro diritto della concorrenza. Il contenuto di questo accordo fornisce un'anticipazione dei possibili contenuti di futuri accordi di cooperazione nel settore della protezione dei dati: ad esempio, le parti contraenti si impegnano a informarsi reciprocamente sulle misure di esecuzione che ritengono possano pregiudicare interessi rilevanti dell'altra parte contraente (art. 3), a coordinare le misure di esecuzione in relazione a transazioni interconnesse (art. 4) o a richiedere l'avvio di misure di esecuzione (art. 6). 23

Ricadono nell'ambito di applicazione dell'art. 67 lett. a LADP anche gli accordi che delimitano le competenze delle diverse autorità di protezione dei dati. Un accordo di questo tipo avrebbe rilevanza pratica per quanto riguarda la delimitazione delle competenze tra le autorità di protezione dei dati 24

svizzere e quelle europee, poiché il GDPR si applica anche ai responsabili del trattamento o agli incaricati del trattamento non stabiliti nell'UE, il che significa che le competenze delle autorità di controllo degli Stati membri dell'UE si estendono ai responsabili del trattamento in Svizzera, ma non possono intraprendere alcuna azione esecutiva in Svizzera. Una mozione parlamentare che chiedeva la conclusione di un corrispondente accordo di coordinamento con l'UE è già stata adottata dai Consigli nel 2017, ma non è ancora stata attuata, il che è probabilmente dovuto principalmente al fatto che attualmente non è possibile concludere nuovi accordi con l'UE prima che siano state chiarite le questioni istituzionali. In ogni caso, il Consiglio federale potrebbe concludere un accordo di coordinamento corrispondente sulla base dell'art. 67 LPD senza l'approvazione del Parlamento.

2. Autorità di protezione dei dati

25 L'autorizzazione a facilitare la conclusione di accordi di cooperazione di diritto internazionale ai sensi dell'art. 67 LPD riguarda esclusivamente la cooperazione tra "autorità di protezione dei dati". Sia la Convenzione ETS 108 (art. 1 Protocollo aggiuntivo del 2001 e art. 12bis ETS 108+) che la Direttiva UE 2016/180 (art. 41 Direttiva 2016/680), vincolante per la Svizzera, obbligano gli Stati contraenti a istituire una o più autorità di controllo indipendenti per la protezione dei dati.

26 Invece, ciò significa che la base di abilitazione dell'art. 67 lett. a LPD non si estende ai contratti di cooperazione in materia di protezione dei dati tra altre autorità, come lo scambio di dati personali tra autorità giudiziarie, di polizia o di migrazione. Tali contratti richiedono l'autorizzazione del Parlamento, a meno che non vi sia un'autorizzazione in un'altra legge federale.

27 La competenza a concludere l'accordo di cooperazione è riservata al Consiglio federale. Secondo la formulazione della legge, l'IFPDT, anche se è la parte direttamente interessata da tali contratti, non è competente a concluderli autonomamente. Anche se il Consiglio federale avrebbe la possibilità di subdelegare all'IFPDT la sua competenza di concludere autonomamente trattati internazionali (cfr. art. 48a cpv. 1 RVOG e sopra, n. 14), finora non l'ha fatto. In questo senso, l'IFPDT dipende per le sue attività dalla conclusione dei contratti corrispondenti da parte del Consiglio federale, il che è in una certa tensione con la sua indipendenza istituzionale (à art. 43 cpv. 4 LDP).

B. Riconoscimento reciproco di un livello di protezione adeguato (lett. b)

Il secondo scopo per il quale il Consiglio federale può concludere trattati internazionali senza la previa approvazione del Parlamento è il riconoscimento reciproco di un livello di protezione adeguato ai sensi dell'art. 67 lett. b LADP. 28

Questa disposizione va intesa in relazione all'art. 16 LADP, che regola le condizioni per la divulgazione di dati personali all'estero. Una di queste possibilità è l'esistenza di un trattato internazionale: secondo l'art. 16 cpv. 2 lett. a, la divulgazione all'estero è possibile se un trattato internazionale garantisce un'adeguata protezione dei dati. 29

Anche la Convenzione sulla protezione dei dati modernizzata del Consiglio d'Europa riconosce la possibilità di garantire l'esistenza di un livello di protezione adeguato in un Paese terzo mediante un accordo internazionale (cfr. art. 12 cpv. 3 lett. b ETS 108+). Analogamente, il diritto dell'UE prevede norme corrispondenti (cfr. art. 46 cpv. 2 lett. a GDPR e art. 37 cpv. 2 lett. a della Direttiva 2016/680, vincolante per la Svizzera). 30

Un trattato internazionale ai sensi dell'art. 16 cpv. 2 lett. a LPD può essere un accordo generale sulla protezione dei dati, come la Convenzione ETS 108+, o qualsiasi altro accordo settoriale in un ambito specifico che regoli il trasferimento di dati personali tra le parti contraenti. Va notato che un trattato internazionale è coperto dall'autorizzazione di cui all'art. 67 lett. b LADP solo se si limita allo scopo di riconoscere reciprocamente un livello di protezione adeguato; se va oltre, il Consiglio federale non può concludere il trattato in modo indipendente o richiede una base di autorizzazione diversa. 31

La possibilità di riconoscere un livello di protezione adeguato mediante un trattato internazionale è rilevante se la legislazione dello Stato interessato o dell'organismo internazionale non fornisce una protezione adeguata ai sensi dell'art. 16 cpv. 1 LADP e non esiste quindi una corrispondente decisione dichiarativa del Consiglio federale. Mediante un accordo, gli Stati interessati possono concordare un sistema di protezione dei dati nell'ambito di un trattato internazionale che compensi le carenze dell'ordinamento giuridico nazionale, in modo da rendere possibile il riconoscimento reciproco di un livello di protezione adeguato. 32

33 L'esempio più importante di applicazione è rappresentato dagli accordi con gli Stati Uniti, il cui livello di protezione dei dati non è considerato adeguato ai sensi dell'art. 16 cpv. 1 della FADP, tra l'altro a causa degli ampi diritti di accesso del presidente americano e dei servizi segreti nazionali ai dati detenuti dalle società americane e delle limitate possibilità di tutela giuridica per i cittadini non statunitensi. Allo stesso tempo, però, gli accordi con gli Stati Uniti illustrano i limiti degli accordi internazionali sugli standard di protezione dei dati, ovvero la difficoltà, in termini di realpolitik, di modificare la distribuzione delle competenze all'interno degli Stati attraverso il diritto internazionale: Il Safe Harbor Framework tra Stati Uniti e Svizzera (modellato sul Safe Harbor UE-USA, che ha dovuto essere sostituito a causa della sentenza della Corte di giustizia europea nella causa Schrems), che era ancora citato come esempio nel rapporto esplicativo sul progetto preliminare della FADP (ma non più nel messaggio), non è più stato riconosciuto dall'IFPDT come base per i trasferimenti di dati verso gli Stati Uniti a seguito della sentenza Schrems. Dopo che anche il successivo Scudo per la privacy UE-USA è stato giudicato insufficiente dalla Corte di giustizia europea nella causa Schrems II, lo Scudo per la privacy Svizzera-USA è ancora formalmente in vigore, ma è ritenuto insufficiente anche dall'IFPDT. Nel marzo 2022 l'UE e gli USA hanno annunciato di aver raggiunto un accordo su un quadro transatlantico per la privacy dei dati; tuttavia, la Svizzera dovrà prima concordare un accordo parallelo con gli USA. Resta da vedere se il quadro transatlantico sulla privacy dei dati supererà davvero le suddette difficoltà di realpolitik.

34 Il riconoscimento reciproco di un livello adeguato di protezione dei dati è possibile anche nell'ambito di accordi settoriali. Così, nel contesto delle convenzioni sulla doppia imposizione con Paesi che non dispongono di un'adeguata protezione dei dati, le parti contraenti possono dichiarare che la protezione dei dati in relazione alla concessione di assistenza amministrativa in materia fiscale è considerata adeguata, almeno per quanto riguarda i dati fiscalmente rilevanti, sulla base delle garanzie fornite dal trattato statale. Lo stesso vale per il trasferimento di dati personali nell'ambito della cooperazione tra polizia, dogana, forze dell'ordine o autorità migratorie, in cui la Svizzera ha concluso numerosi accordi. Come già detto, la base di autorizzazione dell'art. 67 lett. b LADP è limitata alla questione del riconoscimento reciproco di un livello di protezione equivalente. Gli accordi di cooperazione, che in pratica regolano di solito altre questioni di più ampia

portata, necessitano quindi di un'autorizzazione preventiva da parte del Parlamento, a meno che un'altra legge federale non fornisca una base di autorizzazione.

C. Trattati di Stato per altri scopi

La base per l'autorizzazione di cui all'art. 67 LADP è limitata ai due scopi di cui alle lettere a e b. La norma di delega deve essere interpretata in modo restrittivo. La norma di delega deve essere interpretata in modo restrittivo. 35

Il Consiglio federale può concludere trattati internazionali anche per altri scopi nell'ambito della protezione dei dati, ma la competenza non si basa su questo articolo, bensì sulle disposizioni generali (cfr. sopra, n. 10 e segg.). Ciò significa che se il trattato ha una portata limitata o se esiste una disposizione di abilitazione in una legge federale diversa dalla FADP, il Consiglio federale può ratificarlo anche senza l'approvazione del Parlamento. In tutti gli altri casi, l'approvazione parlamentare è necessaria prima della ratifica. 36

A mio avviso, i trattati che comportano il trasferimento di dati personali ad autorità estere non sono di portata limitata, in quanto interferiscono con gli interessi giuridicamente protetti dei privati. Tra questi figurano i numerosi accordi di cooperazione nei settori della polizia, della giustizia, dell'assistenza giudiziaria, della migrazione e della fiscalità che la Svizzera ha concluso con altri Stati e che contengono disposizioni sullo scambio di dati. Rientrano in questa categoria anche i trattati tra Stati o gli scambi di note per l'attuazione dell'ulteriore sviluppo dell'acquis di Schengen (nella misura in cui regolano più di semplici dettagli tecnici), nonché gli accordi con altri Stati sull'accesso ai dati del codice di prenotazione (PNR). Poiché l'art. 67 non prevede alcuna autorizzazione per tali accordi, è sempre necessaria una delega in una legge federale settoriale o un'approvazione parlamentare. Correttamente, il Consiglio federale ha ottenuto anche l'approvazione preventiva dell'Assemblea federale prima di ratificare la Convenzione ETS 108+ e l'adozione della Direttiva 2016/680. Entrambi gli atti giuridici sono strumenti di grande portata, come definito dall'elenco esemplare dell'art. 7a cpv. 4 RVOG. 37

Va notato che la base di autorizzazione di cui all'art. 67 LDP autorizza il Consiglio federale a concludere trattati di portata limitata e più ampia nell'ambito degli scopi dichiarati. A mio avviso, l'opinione giuridica espressa 38

dalla dottrina sulla vecchia norma di delega di cui all'art. 36 cpv. 5 aDSG, secondo cui questa comprenderebbe solo trattati di portata limitata, non riconosce il rapporto tra le diverse basi di autorizzazione di cui all'art. 7a RVOG. Una delega settoriale in una legge federale costituisce una lex specialis e consente a maggior ragione la conclusione di trattati di portata limitata e di trattati di portata più ampia.

39 Il Consiglio federale decide se esiste un trattato di portata limitata o se rientra nella delega di cui all'art. 67 lett. a e b. Il Consiglio federale è tenuto a controllare se ha esercitato i suoi poteri. Per verificare che non ecceda i suoi poteri, l'art. 48a cpv. 2 RVOG obbliga il Consiglio federale a riferire annualmente all'Assemblea federale sui contratti conclusi, modificati e risolti da esso, dai dipartimenti, dai raggruppamenti o dagli uffici. Se l'Assemblea federale non è d'accordo con la suddivisione effettuata dal Consiglio federale, può chiedere con una mozione che il Consiglio federale sottoponga il contratto a una successiva approvazione.

BIBLIOGRAFIA

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.

I MATERIALI

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+).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 69 LPD

Un commentario di Rehana C. Harasgama / Dario Haux

CITAZIONE SUGGERITA

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

Breve citazione: OK-Harasgama/Haux, N. XXX zu Art. 69 DSG.

Art. 69 Disposizione transitoria relativa ai trattamenti in corso

Gli articoli 7, 22 e 23 non si applicano ai trattamenti di dati avviati prima dell'entrata in vigore della presente legge, sempreché lo scopo del trattamento resti immutato e non siano raccolti nuovi dati.

STRUTTURA

In breve 857
I. Aspetti generali 857
A. Panoramica 857
B. Storia delle origini 857
C. Scopo della norma 858
II. Contenuto 858
A. Requisiti 858
B. Sfide 861
Bibliografia 861
I Materiali 862

IN BREVE

La LPD completamente rivista entrerà in vigore il 1° settembre 2023 senza un periodo di transizione generale. Tuttavia, l'art. 69 stabilisce che alcuni articoli selezionati non sono applicabili a determinate operazioni di trattamento dei dati. La norma stabilisce che ciò si applica, tuttavia, solo se queste operazioni di trattamento dei dati sono iniziate prima dell'entrata in vigore della LPD totalmente rivista e non è stato modificato lo scopo del trattamento né sono stati ottenuti nuovi dati dopo la sua entrata in vigore. In questo senso, l'articolo esclude le misure preventive degli articoli 7, 22 e 23 in alcuni casi. In questo modo, il legislatore ha voluto evitare la possibilità che i responsabili possano essere chiamati a rispondere retroattivamente, sostenendo così sforzi e costi aggiuntivi.

I. ASPETTI GENERALI

A. Panoramica

La LPD completamente rivista non contiene periodi transitori che dovrebbero essere presi in considerazione dai responsabili del trattamento dei dati o da altre persone interessate. In linea di principio si applica a partire dal 1° settembre 2023. Tuttavia, il 10° capitolo, le disposizioni finali, contiene alcune disposizioni transitorie rilevanti. Queste sono contenute in particolare negli articoli da 69 a 72. L'articolo 69 prevede specificamente che gli articoli 7, 22 e 23 non si applichino al trattamento dei dati in determinati casi. Ciò si applica ai trattamenti iniziati prima dell'entrata in vigore della LPD rivista, il 1° settembre 2023, e la cui finalità di trattamento non è stata modificata né sono stati aggiunti nuovi dati al processo di trattamento dei dati dopo la sua entrata in vigore. 1

B. Storia delle origini

Con l'entrata in vigore della LPD completamente rivista il 1° settembre 2023, le norme si applicano in tutta la Svizzera e sono quindi applicabili, a condizione che siano soddisfatti gli artt. 2 e 3 cpv. 1. Tuttavia, come di consueto in altre leggi, sono previste eccezioni a questo principio o almeno disposizioni transitorie volte a semplificare la transizione tra il vecchio e il 2

nuovo catalogo di norme. Quest'ultimo è stato previsto dall'art. 64 della LPD. Quest'ultimo era previsto dall'art. 64 del RGPD, che prevedeva tre eccezioni, ossia l'effetto retroattivo del diritto all'informazione dell'interessato in caso di trattamento dei dati già completato (cpv. 1), un periodo transitorio per l'adeguamento del trattamento dei dati in corso (cpv. 2) e la non applicabilità di alcune disposizioni in caso di trattamento dei dati in corso immutato (cpv. 3). Nel cpv. 4 è stato stabilito il principio della validità delle disposizioni al momento dell'entrata in vigore. Alla fine, tuttavia, tutti i cpv. sono stati eliminati, ad eccezione del citato cpv. 3, che si trova ora nell'attuale art. 69.

C. Scopo della norma

3 L'art. 69 garantisce che l'applicazione retroattiva degli artt. 7, 22 e 23 sia impedita se sono soddisfatte determinate condizioni. In questo modo, il legislatore facilita la transizione tra la LPD esistente e quella totalmente rivista, risparmiando alle parti responsabili sforzi e costi aggiuntivi. Inoltre, l'articolo garantisce che non vengano imposti obblighi successivi ai responsabili del trattamento. Si evita così un problematico effetto retroattivo della legge in singoli casi. Allo stesso tempo, l'importanza di questo articolo è limitata, soprattutto perché la LPD in generale non prevede periodi di transizione rilevanti.

II. CONTENUTO

A. Requisiti

4 In termini di contenuto, l'art. 69 fa riferimento agli artt. 7, 22 e 23. Mentre l'art. 7 sancisce i principi della privacy by design (protezione dei dati attraverso la tecnologia) e della privacy by default (protezione dei dati attraverso le impostazioni predefinite) (cfr. in dettaglio le clausole OC sull'art. 7 LPD), gli artt. 22 e 23 si riferiscono alla valutazione d'impatto sulla protezione dei dati (DIA) (cfr. su questo OK Harasgama/Haux sull'art. 22 LPD). L'art. 22 stabilisce la base per l'esecuzione della DIA e l'art. 23 stabilisce alcuni requisiti per la consultazione dell'IFPDT se nel corso di una DIA viene riconosciuto un rischio elevato per la personalità o i diritti fondamentali della persona interessata nonostante le misure di attenuazione del rischio adottate.

5 Questi obblighi devono sempre essere presi in considerazione prima del trattamento dei dati e non devono essere imposti al responsabile del

trattamento in modo retroattivo attraverso questa disposizione transitoria. Ai fini del divieto di retroattività, la norma presuppone che il trattamento dei dati sia iniziato prima dell'entrata in vigore. Deve quindi essere iniziato prima del 1° settembre 2023 e non deve essere né pianificato (secondo la definizione dell'articolo 7, paragrafo 1, LPD) né già completato. Mentre la demarcazione tra la mera pianificazione e l'effettiva attuazione del trattamento dei dati può essere determinata nei singoli casi, si pone la questione di come distinguere l'attuazione dalla cessazione del trattamento dei dati. Va tenuto presente che la cessazione può avvenire solo quando lo scopo del trattamento è stato raggiunto. Equivalente è la situazione in cui la finalità non è di fatto più raggiungibile.

Come secondo prerequisito, la finalità del trattamento precedentemente definita deve rimanere invariata. Ciò significa che la finalità è stata sufficientemente determinata e specificata all'inizio del trattamento dei dati e continua a sussistere immutata al momento dell'entrata in vigore della LPD totalmente rivista (cfr. in dettaglio il commento all'art. 6 cpv. 3 LPD sulla determinazione della finalità del trattamento). In questo contesto, si pone la questione di cosa si applica se solo alcune finalità di trattamento vengono mantenute, mentre altre vengono abbandonate. Questo sarebbe il caso se, ad esempio, una banca dati con dati di pazienti provenienti da sperimentazioni cliniche venisse inizialmente elaborata per ulteriori sperimentazioni cliniche nello stesso settore di ricerca (finalità 1) e per l'addestramento di uno strumento di prognosi basato sull'intelligenza artificiale (IA) (finalità 2), e dopo l'entrata in vigore della LPD completamente rivista, l'elaborazione dei dati avvenisse solo per le sperimentazioni cliniche, cioè per la finalità 1. L'ipotesi che ciò rientri nella formulazione dell'art. 69 è supportata dal fatto che in ogni caso non vi è un ampliamento delle finalità del trattamento. Piuttosto, quelle esistenti vengono perseguite ulteriormente, anche se in forma ridotta. 6

In terzo luogo, lo stock di dati del trattamento in questione deve continuare a esistere inalterato. Secondo la formulazione della legge, "non possono essere acquisiti nuovi dati". Il processo di "acquisizione" è "un atto attivo, mirato e deliberato di raccolta dei dati personali in questione". Il fattore decisivo è l'atto attivo e mirato. L'ottenimento passivo dei dati, invece, non è incluso. Altri autori giungono a una conclusione simile concentrandosi sulla natura pianificata del processo. 7

8 Tuttavia, non è chiaro come debba essere interpretata la frase "nessun nuovo dato". Un'interpretazione restrittiva porterebbe a una situazione in cui la disposizione transitoria non si applicherebbe a un processo di elaborazione costante dei dati con categorie di dati fisse, a condizione che vengano ottenuti dati aggiuntivi (punti) su altre persone con categorie di dati costanti. Ciò sarebbe indipendente dal modo in cui questi dati aggiuntivi (punti) influenzano il processo di trattamento o la finalità. Questa valutazione potrebbe essere giustificata dal fatto che lo stock di dati o la portata dei dati esistenti verrebbero modificati o aumentati. Ad esempio, uno strumento HR basato sull'intelligenza artificiale di un'azienda che elabora dati (punti) aggiuntivi dai nuovi candidati dopo il 1° settembre 2023. Lo stock di dati o l'ambito di questo stock verrebbero quindi modificati o aumentati, cosicché se gli altri requisiti dell'art. 69 sono soddisfatti, una valutazione d'impatto sulla protezione dei dati dovrebbe essere effettuata nuovamente in base a questa interpretazione restrittiva. Sebbene il messaggio suggerisca certamente una simile interpretazione, un'interpretazione così restrittiva non corrisponde al senso e allo scopo della disposizione. Infatti, ciò significherebbe che tutte le operazioni di trattamento dei dati in corso in cui è possibile che vengano ottenuti dati su altre persone dopo il 1° settembre 2023 non sarebbero coperte dalla disposizione. L'ambito di applicazione dell'articolo 69 sarebbe quindi trascurabilmente ridotto. Questa interpretazione restrittiva non viene seguita in questo caso. In questo contesto, sono possibili due interpretazioni: (1) l'art. 69 si applica solo se vengono acquisite nuove categorie di dati, ma non in caso di semplice modifica o ampliamento dell'ambito di applicazione delle stesse categorie o punti di dati. Questo sarebbe il caso, ad esempio, se un modulo online fornito per un concorso dopo il 1° settembre 2023 non raccogliesse più solo il nome, i dati di contatto e la risposta alla domanda del concorso, ma chiedesse ulteriori informazioni su interessi e hobby. Oppure: (2) l'art. 69 non è applicabile a nessun trattamento di dati se - secondo il Messaggio, interpretato in senso restrittivo - la quantità di dati o il volume di dati in sé viene aumentato o modificato, sebbene le categorie di dati acquisite rimangano invariate e non si possa escludere una conseguente modifica della finalità o del processo di trattamento.

9 Si discute anche se i dati già ottenuti in precedenza, ma aggiunti successivamente, escludano l'applicabilità dell'art. 69 LPD. Sulla base della formulazione, alcuni autori sostengono che il trattamento di questi dati rientra nell'eccezione, almeno nella misura in cui sono stati ottenuti per lo stesso

scopo. Tuttavia, ciò è contraddetto dal fatto che l'ambiente del trattamento dei dati è così profondamente influenzato dalle innovazioni tecnologiche che l'eccezione dell'art. 69 LPD dovrebbe applicarsi solo in condizioni ristrette e dovrebbe quindi essere interpretata in modo restrittivo. Se nuovi dati vengono aggiunti al patrimonio di dati, difficilmente il patrimonio di dati può essere definito "immutato", cioè rimanere lo stesso, se questi dati sono già stati ottenuti nel contesto di un'altra finalità di trattamento dei dati. Tuttavia, sembra lecito chiedersi se la questione acquisterà importanza e contorni nell'applicazione pratica, soprattutto perché nel complesso si può ritenere che la rilevanza pratica di questo standard sia piuttosto bassa. Ciò è particolarmente vero in quanto il principio dell'art. 7 era già in parte in vigore prima dell'entrata in vigore degli artt. 4 e 7 dell'aDSG, e alcuni responsabili del trattamento erano obbligati a farlo anche a causa del DSGVO. Lo stesso vale per gli articoli 22 e 23 (si veda in dettaglio il commento di Harasgama/Haux sull'articolo 22 LPD).

B. Sfide

Con l'entrata in vigore della LPD completamente rivista, i responsabili del 10
trattamento dei dati si trovano ad affrontare numerose sfide. Sebbene la formulazione dell'art. 69 LPD sia solo breve e rischi di cadere nel dimenticatoio, in questo contesto occorre dedicarle la necessaria attenzione. Mentre i trattamenti di dati avvenuti prima dell'entrata in vigore e che soddisfano gli altri requisiti rientreranno senza dubbio nell'esenzione, è sempre necessario richiedere una consulenza legale su questioni dettagliate e sull'applicazione di nuove tecnologie nei processi di trattamento dei dati che erano già stati pianificati e/o testati prima dell'entrata in vigore della LPD completamente rivista. In questo caso, è importante capire esattamente se i dati o lo scopo del trattamento rimangono effettivamente invariati o se sono state apportate o devono essere apportate delle modifiche. In tal caso, in caso di dubbio, si dovrebbe ritenere che la norma non sia applicabile.

BIBLIOGRAFIA

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).

I MATERIALI

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.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 72 LPD

Un commentario di Danielle Schneider / Carl Jauslin

CITAZIONE SUGGERITA

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 72 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Schneider/Jauslin, N. XXX zu Art. 72 DSG.

Art. 72 Disposizione transitoria relativa all'elezione dell'Incaricato e alla cessazione del suo mandato

[1] Sino al termine della legislatura in corso all'entrata in vigore della presente legge, l'elezione dell'Incaricato e la cessazione del suo mandato sono rette dal diritto anteriore.

[2] Se in occasione della prima elezione da parte dell'Assemblea federale plenaria è eletto l'Incaricato uscente, il nuovo mandato dello stesso inizia il giorno successivo all'elezione.

STRUTTURA

In breve 865
I. Aspetti generali 865
II. Diritto transitorio in materia di elezione e cessazione del mandato (cpv. 1) 865
III. Diritto transitorio relativo all'eventuale rielezione dell'attuale titolare del mandato (cpv. 2) 866
Materiali 867

IN BREVE

La nuova legge sulla protezione dei dati entrerà in vigore il 1° settembre 2023. Tuttavia, la legge precedente continuerà ad applicarsi all'elezione e alla cessazione del mandato del Commissario fino alla fine della 51a legislatura. In base a ciò, l'Assemblea federale unitaria è l'organo elettorale ed è responsabile delle decisioni più importanti del datore di lavoro.

I. ASPETTI GENERALI

La revisione totale della LPD modifica la procedura di nomina del Commissario. L'Assemblea federale unitaria è ora l'unico organo elettivo ed è responsabile delle decisioni più importanti del datore di lavoro. In questo modo, l'indipendenza e la legittimità democratica del Commissario saranno rafforzate. Sono pertanto necessarie disposizioni transitorie per l'elezione e la cessazione del mandato del Commissario. 1

L'art. 72 cpv. 1 LPD è stato introdotto nell'ambito delle consultazioni parlamentari sulla revisione totale della LPD. La disposizione non era ancora stata inserita nella bozza del Consiglio federale, che aveva mantenuto la precedente procedura di nomina dell'Incaricato (elezione da parte del Consiglio federale e approvazione da parte dell'Assemblea federale ai sensi dell'art. 26 cpv. 1 lett. a LPD) e le precedenti responsabilità per le decisioni del datore di lavoro (in particolare l'art. 26a cpv. 3 relativo alla revoca del mandato da parte del Consiglio federale). 2

L'art. 72 cpv. 2 LPD è stato inserito nella LPD completamente rivista solo nel corso dei lavori sull'iniziativa parlamentare SPK-N 21.443. Ciò si è reso necessario per colmare una lacuna involontaria relativa alla possibile rielezione del precedente Commissario (cfr. n. 6 s.). 3

II. DIRITTO TRANSITORIO IN MATERIA DI ELEZIONE E CESSAZIONE DEL MANDATO (CPV. 1)

L'art. 72 cpv. 1 LPD prevede che l'elezione del commissario e la cessazione del suo mandato continuino a essere disciplinati dal diritto precedente fino alla fine della legislatura in cui entrerà in vigore la LPD totalmente rivista. 4

5 Il Consiglio federale ha stabilito che la nuova legge sulla protezione dei dati entrerà in vigore il 1° settembre 2023. Ciò significa che il Commissario potrà essere eletto per la prima volta dall'Assemblea federale unitaria a partire dalla sessione invernale del 2023. La Commissione giudiziaria ha annunciato che intende eleggere il Commissario per il prossimo mandato nella sessione invernale del 2023. In questo caso, il nuovo mandato del commissario inizierebbe in linea di principio il 1° gennaio 2024 (cfr. art. 44 cpv. 1, seconda frase RPF).

III. DIRITTO TRANSITORIO RELATIVO ALL'EVENTUALE RIELEZIONE DELL'ATTUALE TITOLARE DEL MANDATO (CPV. 2)

6 L'attuale commissario è stato confermato dal Consiglio federale il 10 aprile 2019 per un secondo mandato fino alla fine della 51a legislatura, il 4 dicembre 2023. Si candida per un terzo (e ultimo) mandato. L'elezione deve essere effettuata dall'Assemblea federale unitaria (art. 43 cpv. 1 LPD). In caso di rielezione, l'inizio del mandato il 1° gennaio 2024 comporterebbe una lacuna involontaria (soprattutto dal punto di vista del diritto del personale). Infatti, tra il 4 dicembre 2023 e il 1° gennaio 2024, l'attuale titolare della carica non avrebbe un rapporto di lavoro come commissario. Di conseguenza, in linea di principio, non avrebbe nemmeno i diritti e gli obblighi derivanti dal rapporto di lavoro (in particolare non avrebbe diritto allo stipendio).

7 Per la prima elezione da parte dell'Assemblea federale unitaria, l'art. 72 cpv. 2 LPD anticipa quindi eccezionalmente l'inizio del mandato al giorno successivo all'elezione. Tuttavia, ciò si applica solo in caso di rielezione dell'attuale presidente. Certo, anche questa soluzione non consente di ottenere una transizione senza soluzione di continuità. Tuttavia, l'attuale incaricato potrebbe almeno riprendere il suo lavoro il prima possibile. Durante il periodo di transizione, l'FDPIC sarebbe guidato dal sostituto del commissario.

Le opinioni espresse riflettono il parere personale degli autori e non sono vincolanti per l'Ufficio federale di giustizia.

MATERIALI

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).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 72a LPD

Un commentario di Danielle Schneider / Carl Jauslin

CITAZIONE SUGGERITA

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 72a DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Breve citazione: OK-Schneider/Jauslin, N. XXX zu Art. 72a DSG.

Art. 72a Disposizione transitoria relativa al rapporto di lavoro dell'Incaricato

Il rapporto di lavoro dell'Incaricato costituito secondo il diritto anteriore è retto dal diritto anteriore.

STRUTTURA

In breve 871
I. Aspetti generali 871
II. Disposizioni transitorie relative al rapporto di lavoro del commissario 871
Materiali 872

IN BREVE

Con la revisione totale della LPD, l'Assemblea federale diventa il corpo elettorale e il datore di lavoro del Commissario. Ciò ha implicazioni per il rapporto di lavoro. Le nuove disposizioni sul rapporto di lavoro dell'Incaricato si applicheranno solo dopo la prima elezione da parte dell'Assemblea federale unita. Dopo l'entrata in vigore della nuova legge sulla protezione dei dati, il 1° settembre 2023, la legge precedente continuerà quindi ad applicarsi al rapporto di lavoro fino all'elezione del Commissario da parte dell'Assemblea federale unitaria.

I. ASPETTI GENERALI

Con la revisione totale della LPD, l'Assemblea federale diventa l'organo elettivo e il datore di lavoro dell'Incaricato. È quindi responsabile della regolamentazione del suo rapporto di lavoro (cfr. art. 43 cpv. 3bis LPD). Nell'ambito dell'iniziativa parlamentare SPK-N 21.443, ha emanato le relative disposizioni attuative. Inoltre, la LPD contiene anche diverse norme sul rapporto di lavoro del commissario, in particolare per quanto riguarda la durata del mandato e la sua cessazione (art. 44 LPD), il diritto disciplinare (art. 44a LPD) o il lavoro accessorio (art. 47 LPD). L'art. 72a LPD chiarisce quando queste nuove disposizioni si applicano al Commissario. 1

II. DISPOSIZIONI TRANSITORIE RELATIVE AL RAPPORTO DI LAVORO DEL COMMISSARIO

L'elezione del commissario e la cessazione del suo mandato sono ancora soggetti alla legge precedente fino alla fine della legislatura in cui entra in vigore la LPD (art. 72 cpv. 1 LPD). Solo quando il commissario sarà eletto dall'Assemblea federale unitaria, il suo rapporto di lavoro potrà essere regolato dalla nuova legge. L'art. 72a LPD prevede quindi che il rapporto di lavoro del commissario instaurato in base alla legge precedente sia regolato dalla legge precedente. 2

Ciò significa che, dopo l'entrata in vigore della nuova legge sulla protezione dei dati il 1° settembre 2023, la legge precedente continua ad applicarsi al rapporto di lavoro dell'Incaricato fino alla prima elezione da parte 3

dell'Assemblea federale unitaria. Successivamente, si applicheranno le disposizioni totalmente riviste o create ex novo sul rapporto di lavoro dell'Incaricato.

Le opinioni espresse riflettono il parere personale degli autori e non sono vincolanti per l'Ufficio federale di giustizia.

MATERIALI

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).