Federal Act on Data Protection

Last change: 27.07.2026

PDF generated on: 20.09.2026

ONLINE COMMENTARY
THE OPEN ACCESS
LEGAL COMMENTARY

TABLE OF CONTENTS

COMMENTARY ON

Vorb. zu Art. 1 FADP

A commentary by Sandra Husi-Stämpfli

SUGGESTED CITATION

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

Short citation: OK-Husi-Stämpfli, N. XXX zu Vorb. zu Art. 1 DSG.

CONTENT

IN A NUTSHELL

Data protection law has its origins in (ancient) professional secrecy as first developed by Hippocrates: The idea was to keep information about patients secret. From this concept, with the increasing technical progress, the associated complexity and globalization of the exchange of information, the first overall codifications of data protection law developed from 1970 onwards - first in individual countries, then gradually also across borders by international organizations and finally by the European Community. Switzerland's first data protection law came into force in 1992, the totally revised (new) data protection law on September 1, 2023.

I. THE HIPPOCRATIC OATH AS THE FIRST PROFESSIONAL SECRET

The first codified regulation on the protection of personal data can be traced back to the period between 460 and 370 BC: With the Hippocratic Oath, physicians undertake to this day to keep information about their patients secret. This was followed by various professional secrets, such as the midwife's secret, the confessional secret or the lawyer's secret. 1

II. 20TH CENTURY: DATA PROTECTION LAW MAKES ITS WAY INTO THE LEGAL SYSTEMS

The originally profession-related requirements for the protection of personal information, such as medical secrecy, midwifery secrecy, or even attorney-client privilege, are based on the conviction that violations can be detected immediately and that the responsible persons can also be held accountable without further effort. 2

This concept of clear responsibilities was already overtaken by technological progress, the associated complexity and increasing globalization of information exchange in the last century. Thus, in the 1970s, the first questions arose about how to deal with "automated" data processing, i.e. the use of computers and the associated responsibilities and challenges for data security - suddenly, for example, it was no longer "just" the doctor who made a handwritten note in the physical patient file - the data was stored on a PC, which was at best 3

maintained by an external IT company, and so on. The new challenges this presented heralded the creation of the first overall codifications of data protection law around 1970 - first in individual countries, then gradually across borders by international organizations, and finally by the European Community.

4 Examples:

- 1973: Sweden.
- 1977: Federal Republic of Germany.
- 1978: Austria and France.
- 1980: OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data.
- 1981: Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
- 1995: EU Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- 2000: EU Charter of Fundamental Rights (EU-GRC) with Art. 8 "Protection of personal data".

In Switzerland, the codification movement began at both the cantonal and federal levels in the 1970s and finally culminated in the Federal Data Protection Act in 1992.

III. 21ST CENTURY: DATA PROTECTION AND DIGITIZATION

5 Still stemming from a time when "automated data processing" was the exception, the FADP was increasingly unable to meet the requirements of the digitized world. The revision of the FADP was significantly influenced by the data protection revision in the EU:

A. Impetus: Data Protection Revision in the EU

6 The European Union launched deliberations on modern data protection law in 2012. After intensive negotiations, the European Parliament and the Coun-

cil of the European Union finally adopted the EU General Data Protection Regulation (DSGVO) and Directive 2016/680 in 2016.

- The DSGVO mainly regulates the protection of data processed within the European single market, but also applies to the public sector. It entered into force on May 25, 2018.
- Directive 2016/680 is designed to protect personal data processed for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection against and the prevention of threats to public security. Directive 2016/680 is aligned with the wording of the DSGVO in order to achieve a consistent basic vocabulary throughout the EU area regarding the general principles. It entered into force on May 5, 2016.

B. The Swiss path to a modern data protection law

On December 9, 2011, the Federal Council approved a report on the evaluation of the FADP and instructed the Federal Department of Justice and Police (FDJP) to consider legislative measures to strengthen data protection, taking into account the results of the evaluation and ongoing developments in the EU and the Council of Europe. At the time, the Federal Council was faced with the question of the extent to which transparency about data processing should be increased and the persons concerned should be made more aware of the new risks. In particular, the review of the need for legal action should also take into account the fact that minors are particularly vulnerable when it comes to the processing of their data. At the same time, however, the Federal Council also emphasized that the review of legislative measures must also take into account the fact that data protection measures may conflict with other interests. Therefore, in addition to the protection of privacy, the interests of the economy, the right to freedom of opinion and information, and other private and public interests must also be taken into account. This work was carried out with the involvement of an advisory group, which defined the need for legislative action by 2014. 7

After the Federal Council took note of the report of the advisory group on April 1, 2015, it instructed the FDJP to prepare a preliminary draft for a revision of the FADP by the end of August 2016 at the latest. This preliminary 8

draft for a total revision of the FADP and for amending other enactments on data protection was sent out for consultation on December 21, 2016.

9 The Federal Council finally adopted the dispatch on the "new" Data Protection Act on September 15, 2017. The Federal Council's goal was to "adapt data protection to the Internet age and strengthen the position of citizens. At the same time, the Swiss data protection level was to be brought into line with that of the EU in order to preserve the adequacy decision, which is important for the free transfer of data between Swiss companies and those in the EU.

10 The parliamentary deliberations were difficult; in some cases, there were fundamentally divergent opinions as to how far the new data protection law should go. At the same time, however, time was of the essence: individual provisions of the new data protection law were "Schengen-relevant" and had to be implemented within two years of the entry into force of the corresponding Schengen law. Parliament therefore decided to split the bill: The so-called "Schengen Data Protection Act" was passed on September 28, 2018, and entered into force on March 1, 2019. It was repealed or re-integrated into the Data Protection Act when the new Data Protection Act came into force. The "Schengen Data Protection Act" regulated the processing of personal data by federal bodies for the purpose of preventing, investigating, or prosecuting criminal offenses or the execution of sentences, including the protection against and the prevention of threats to public security.

11 In a second stage, those aspects of the data protection revision were then discussed that were not relevant to the Schengen area and were strongly influenced by the DSGVO. These included in particular the innovations for the processing of personal data by private individuals (i.e. primarily companies). The discussions focused on the following topics:

- Strengthening the rights of data subjects: Extension of the right to information (OC-Steiger on Art. 25 FADP) and introduction of a right to data portability (see OC commentary on Art. 28 FADP).
- Extension of the obligations of data controllers and processors: introduction of the principle of privacy by design and default (OC Claus on Art. 7 FADP) and the obligation to conduct a data protection impact assessment for certain forms of data processing (OC Harasgama on Art. 22 FADP) and

to report breaches of data subject protection to the supervisory authority (OC de la Cruz on Art. 24 FADP).

- Introduction of a catalog of sanctions (OK-Gassmann on Art. 60 ff. FADP) and strengthening the competences of the FDPIC (OK-Reinle on Art. 49 FADP; OK-Fanger/Oehri on Art. 50 FADP).

Finally, after three years, the revised Data Protection Act could be adopted on September 25, 2020. The referendum passed unused, which is why the law entered into force on September 1, 2023, together with the implementing ordinance (DSV), which was also totally revised. 12

The author gives her personal assessment in this commentary.

BIBLIOGRAPHY

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

COMMENTARY ON

Art. 1 FADP

A commentary by Sandra Husi-Stämpfli

SUGGESTED CITATION

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

Short citation: OK-Husi-Stämpfli, N. XXX zu Art. 1 DSG.

Chapter 1
Purpose, Scope of Application and Federal Supervisory Authority

Art. 1 Purpose

This Act has the purpose of protecting the personality and fundamental rights of natural persons whose personal data is processed.

CONTENT

IN A NUTSHELL

Together with the protection of personality under civil law, data protection law ensures the implementation of the protection of personality under fundamental law: the FADP serves to protect the personality and fundamental rights of natural persons, but no longer to protect legal persons, as was still the case under the old FADP. The purpose of the FADP is thus narrower than that of the DSGVO, for example, which also aims to enable the free movement of data. With the chosen wording, the Swiss legislator makes clear that data protection law is personality protection avant tout, and not protection of economic operators, public security or other interests.

I. PRELIMINARY: THE DIFFERENT FORMS OF PERSONAL DATA PROTECTION

Data protection law, together with the protection of personality under civil law (Art. 27 and Art. 28 et seq. of the Civil Code, see below, n. 3), ensures the implementation of the protection of personality under fundamental law (Art. 10 FC, see below, n. 2), and as its manifestation of privacy or informational self-determination (Art. 13 para. 2 FC, see below, n. 2). The interaction of these elements of the protection of personality is as follows: 1

A. Constitutional protection of informational self-determination within the meaning of Art. 13 para. 2 FC

Article 13 FC protects the private sphere as a space for the development and unfolding of the individual personality. Every person, regardless of gender, origin, age, etc., is entitled to respect for their private and family life, their home and their correspondence. Art. 13 para. 2 FC, as a special aspect of the right to privacy, grants a right to protection against misuse of personal data. According to case law, the wording of para. 2 is too narrow: "fundamental right data protection" must in principle cover any handling of personal data by the state. 2

B. Protection of personality under civil law

3 The personality rights protected in Art. 27 and Art. 28 et seq. CC, which form part of the fundamental right of personal freedom in Art. 10 FC, belong to the individual for his or her own sake and are inseparably linked to his or her person. The area protected by Art. 28 CC is thereby divided in the majority of doctrine into three categories: the physical personality, the affective personality and the social personality.

- The physical personality concerns the physical integrity and the physical freedom of movement.
- Affective or psychological personality protects the mental-emotional sphere of a person's life.
- Social personality protection contributes to the harmonious organization of social and societal relations and protects all the goods to which a person must be entitled in order to enable him or her to live harmoniously in society: These include, in particular, the right to one's name, the right to honor, the right to one's image, data protection, economic freedom, and the right to have one's private life respected and honored.

4 The basic provisions for protection under private law in Art. 27 et seq. CC apply when a violation of personality rights has occurred by another private person and the case cannot be regulated by a special norm of private law. A two-stage examination scheme is then derived from Art. 28 CC:

- First, it is examined whether there has been a violation of personality rights.
- Then, in a second step, it must be examined whether there is a justification under Art. 28 para. 2 CC, so that the violation can be assessed as not unlawful. If, however, there is no justification after the examination of Art. 28 para. 2 CC, one speaks of an unlawful violation of personality.

II. PROTECTION OF PERSONALITY UNDER DATA PROTECTION LAW

A. History of FADP Art. 1

Article 1 of the FADP was taken over unchanged from the old FADP, although at least during the consultation process various parties expressed the wish that, analogous to Article 1 of the FADP, cross-border data traffic and the protection of competitiveness should also be included in the purpose of the FADP. However, the provision was uncontested in the parliamentary debate. 5

B. Purpose of the FADP

Both the FADP and the cantonal (information and) data protection laws state in their purpose provisions that data protection must not be understood as an end in itself, but rather as an instrument for safeguarding the fundamental rights or protecting the personality of natural persons whose data are processed - data of legal persons are no longer covered by the FADP (see OK-Husi-Stämpfli Art. 2 n. 12). 6

In this self-understanding, Swiss data protection law clearly differs from the DSGVO, which, in addition to the protection of personality, also designates the free movement of data as the purpose of the regulation. In other words, Swiss data protection law is precisely personality protection avant tout, and not protection of economic operators, public security or other interests. 7

The protection of personality is primarily aimed at data processing by private parties, while the protection of fundamental rights is aimed at protection against interference by state authorities. In view of the fact that, from a constitutional point of view, the protection of personality is a consequence of the state's duty to protect and to implement fundamental rights not only by the state but also between private individuals (Art. 35 para. 3 FC), it would have been more consistent from a legal point of view to list the protection of fundamental rights first and then the protection of personality. 8

The "fundamental rights" mentioned in Art. 1 FADP do not only include Art. 13 para. 2 FC or Art. 8 ECHR. Rather, Art. 1 FADP must be understood to include all fundamental rights that may be affected by data processing, such as free- 9

dom of expression, prohibition of discrimination, etc. State action must not only comply with the FADP, but also with fundamental rights (Art. 36 FC).

C. Legal nature of Art. 1 FADP

10 Art. 1 FADP is a programmatic provision: it does not establish rights and obligations, but it is to be understood as a guideline for the interpretation of subsequent provisions.

The author gives her personal assessment in this commentary.

BIBLIOGRAPHY

Fey Marco, Kommentierung zu Art. 1 FADP, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (eds.), Datenschutzgesetz, Stämpflis Handkommentar, 2nd edition, Bern 2023.

Biaggini Giovanni, Kommentar zur Bundesverfassung der Schweizerischen Eidgenossenschaft, 2nd edition, Zurich 2017.

Maurer-Lambrou Urs/ Kunz Simon, Kommentierung zu Art. 1 FADP, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (eds.), Datenschutzgesetz / Öffentlichkeitsgesetz, Basler Kommentar, 3rd edition, Basel 2014.

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

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.

COMMENTARY ON

Art. 2 FADP

A commentary by Sandra Husi-Stämpfli

SUGGESTED CITATION

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

Short citation: OK-Husi-Stämpfli, N. XXX zu Art. 2 DSG.

Art. 2 Personal and material scope of application

[1] This Act applies to the processing of personal data of natural persons by:

a. private persons;

b. federal bodies.

[2] It does not apply to:

a. personal data being processed by a natural person exclusively for personal use;

b. personal data being processed by the Federal Assembly and parliamentary committees as part of their deliberations;

c. personal data being processed by institutional beneficiaries under Article 2 paragraph 1 of the Host State Act of 22 June 2007 who enjoy immunity from jurisdiction in Switzerland.

[3] The applicable procedural law regulates the processing of personal data and the data subject`s rights in court proceedings and in proceedings governed by federal procedural regulations. This Act applies to first instance administrative proceedings.

[4] The public registers for private legal transactions, and in particular the access to these registers and the data subject`s rights, shall be regulated by the specific provisions of the applicable federal law. If the specific provisions do not contain any rules, this Act applies.

CONTENT

IN A NUTSHELL

The FADP applies to the processing of data of natural persons by federal bodies and private persons. However, the FADP does not apply absolutely: certain cases, in particular data processing exclusively for personal use or in the context of ongoing judicial or federal proceedings, are excluded from the FADP or are governed by separate, specific (procedural) provisions.

I. GENERAL

A. Norm Purpose

1 Article 2 FADP defines the scope of application of the Federal Data Protection Act and the corresponding exceptions. The scope of the FADP was partially expanded in the revision, in particular to meet the requirements of ERK 108+: Thus, the exceptions relating to pending civil proceedings, criminal proceedings, international mutual legal assistance proceedings, and proceedings under state and administrative law (Art. 2 para. 2 lit. c FADP) and the one relating to public registers of private legal transactions (Art. 2 para. 2 lit. d FADP) have been adapted.

B. Regulatory competence

2 The competence to regulate data protection law derives from the general federal system of competences: under Articles 3 and 42 FC, the Confederation has a limited individual power, while the cantons exercise all tasks that are not assigned to the Confederation.

3 The Confederation is thus entitled to regulate data processing in those areas in which it may in principle legislate - in particular within the framework of the organization and procedure of the federal authorities (Art. 164 para. 1 lit. g FC). In the ingress of the FADP, reference is made to Art. 95 ("Private sector activity"), Art. 122 ("Civil law") and Art. 173 para. 2 FC ("Other tasks and powers"). Even if these articles do not explicitly mention the federal government's competence in the area of data protection, it is undisputed that they include the competences to enact data protection provisions.

Whether the processing of personal data satisfies the requirements of data protection law is determined, on the one hand, by the provisions of the (information and) data protection laws (so-called "general" data protection law) and, on the other hand, by the provisions in those special laws that regulate data processing in specific cases of application ("special" data protection law). 4

In a first step, both public bodies and private individuals must be guided by "general" data protection law if they wish to process personal data: 5

- Federal bodies and private persons must be guided by the processing requirements of the federal data protection law.
- If cantonal public bodies process personal data, the cantonal (information and) data protection laws must be followed in each case.

The "general" data protection law regulates - at the cantonal and federal level - the following topics, among others: Legislative purpose, scope, definitions, processing principles, rules on accountability, rights of data subjects, etc. In accordance with its nature as basic legislation, the "general" data protection law also generally contains exceptional provisions that define in which cases special legal requirements take precedence. 6

In a second step, public bodies must check whether they are permitted to process the personal data in question for the purpose of fulfilling their legal duties, i.e. whether the relevant substantive laws (the area-specific, "special" data protection law) specifically regulate data processing. 7

The subject law or the "special" data protection law must meet the requirements of general data protection law and, in addition to the purpose of the processing (i.e., the specific task for the fulfillment of which personal data must be processed), must specify, among other things, the responsibilities and any requirements for disclosure. 8

Private individuals, for their part, must ensure in this second step that they have a justification for the data processing in question, insofar as the processing violates personal rights. 9

II. PERSONAL SCOPE OF APPLICATION (ART. 2 PARA. 1 FADP)

10 Federal data protection law applies to the processing of data of natural persons by federal bodies (see N. 11 Commentary on Art. 5 lit. i and OK-Zysset Art. 34 FADP) and private persons (see OK-dal Molin on Art. 30 FADP). The respective cantonal (information and) data protection law applies to the processing of personal data by cantonal public bodies (see n. 5).

III. MATERIAL SCOPE OF APPLICATION: DATA OF NATURAL PERSONS

11 Every human being is considered a natural person in the legal sense, and every human being has legal capacity (Art. 11 para. 1 CC). Every human being thus has the capacity to have rights and obligations (Art. 11 para. 2 CC) - these rights also include the right of personality from the perspective of civil law as well as data protection law (Art. 28 ff. CC or Art. 1 in particular in conjunction with Art. 30 FADP and Art. 34 FADP).

12 With the last data protection revision, the material scope was restricted: Data of legal entities are no longer covered by the FADP, but this is in any case insignificant in practice, because legal entities can still claim personality violations based on Art. 28 et seq. ZGB (such as damage to reputation). They also enjoy the protection of the Federal Act against Unfair Competition, the Copyright Act or the specific provisions on professional, trade or manufacturing secrets.

IV. EXCEPTIONS

13 The FADP does not apply absolutely. Art. 2 para. 2-4 FADP mention various exceptions for which the FADP does not apply.

A. Use for private purposes (Art. 2 para. 2 lit. a FADP)

14 The FADP does not apply if the personal data in question is processed by a natural person exclusively for personal use (Art. 2 para. 2 let. a FADP). An example of this is the collection of letters or e-mails that a married couple has written to each other over many years and which also contains remarks and anecdotes about other people. Also exempt from the FADP are private photo

albums with pictures of family celebrations, vacation acquaintances, etc., as long as the photos are not further disseminated (e.g. digitized and published).

B. Processing by the Federal Assembly and parliamentary committees (Art. 2 para. 2 lit. b FADP)

Personal data are processed by the Federal Councils and parliamentary commissions in the course of their deliberations (Art. 2 para. 2 let. b FADP). This provision was taken over unchanged from the old FADP. According to the dispatch, the reason for the exception from the FADP is that parliament would not be able to perform its constitutional duties if it had to observe the data protection principles in every case - the dispatch explicitly mentions the requirements for the disclosure of personal data here. However, it seems far more plausible to argue that the special law governing the business of the Councils (the "special data protection law") contains detailed provisions on the handling of information (and thus personal data), which is why subordination to the FADP is simply not necessary. 15

C. Data processing by diplomatic missions and international organizations (Art. 2 para. 2 lit. c FADP)

Also not covered by the FADP are those processing operations carried out by a diplomatic or consular representation of another state or an international organization. Covered by this exception are, in other words, the institutional beneficiaries under Article 2(1) of the Host State Act of 22 June 2007, which enjoy immunity from jurisdiction in Switzerland: based on international law and the DPA, they enjoy independence and freedom of action so that they can perform their international functions; accordingly, they cannot be expected to submit to the rules of Swiss law with respect to the data processed by their diplomatic or consular representations. 16

D. Ongoing legal or federal proceedings (Art. 2 para. 3 FADP)

The FADP also does not apply to ongoing court proceedings or proceedings under federal law, as these are governed by the respective procedural law, which contains detailed provisions on the handling of personal data (of the parties, plaintiffs, etc.). 17

18 The term "court proceedings" includes all proceedings before cantonal and federal criminal, civil and administrative courts, but also before arbitration courts with their seat in Switzerland. Unlike the aDSG, Art. 2 para. 3 FADP does not use the term "pending proceedings", since only civil procedural law refers to lis pendens and this term has sometimes led to problems of delimitation.

19 The only decisive factor is now whether proceedings take place before a court or are governed by a federal procedural code. Proceedings take place before a court when the court is seized of a case for the first time by instituting proceedings under the relevant rules of procedure. A proceeding is governed by federal rules of procedure as soon as a particular matter is dealt with by an authority in accordance with the provisions in one of these laws.

20 The federal procedural codes that contain provisions on the handling of personal data or on the rights of the persons concerned in the context of these proceedings include in particular

- the Federal Act on Administrative Procedure of 20 December 1968 (APA, insofar as it does not concern first-instance administrative proceedings),
- the Code of Civil Procedure of 19 December 2008 (CPC),
- the Federal Act of 11 April 1889 on Debt Collection and Bankruptcy (SchKG),
- the Code of Criminal Procedure of October 5, 2007 (StPO),
- the Federal Law on Administrative Criminal Law of March 22, 1974 (VStrR), or else
- the Federal Act on International Mutual Assistance in Criminal Matters of 20 March 1981 (IMAC).

21 Data processing by the administrative services of courts and authorities does not fall within the scope of the relevant procedural law, so Art. 2 para. 3 FADP does not apply.

22 As a rule, the relevant procedural code remains applicable even after the conclusion of the proceedings: For example, special requirements apply to file maintenance, file inspection, rectification or file retention. However, it is not

excluded that the applicable procedural law declares the FADP applicable after the conclusion of the proceedings (cf. Art. 99 Criminal Procedure Code).

E. Public registers of private legal transactions

Finally, data processing in the context of those public registers of private legal transactions that are maintained on the basis of federal law and by federal bodies are excluded from the scope of application of the FADP. The respective special law applies here. These registers include in particular 23

- the Zefix electronic civil status register
- the aircraft register of the Federal Office of Civil Aviation, and
- the registers of the Swiss Federal Institute of Intellectual Property (in particular the register of trademarks, patents and designs).

The public registers of private legal transactions, for which the cantons are responsible, are subject to cantonal data protection law. The cantonal registers include, for example. 24

- the land register
- the shipping register,
- the commercial registers and
- the debt enforcement and bankruptcy registers.

The author gives her personal assessment in this commentary.

BIBLIOGRAPHY

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.

COMMENTARY ON

Art. 3 FADP

A commentary by Sandra Husi-Stämpfli

SUGGESTED CITATION

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

Short citation: OK-Husi-Stämpfli, N. XXX zu Art. 3 DSG.

Art. 3 Territorial scope of application

[1] This Act applies to circumstances that have an effect in Switzerland, even if they were initiated abroad.

[2] For rights under private law, the Federal Act of 18 December 1987 on Private International Law applies. In addition, the provisions on the territorial scope of application of the Criminal Code are reserved.

CONTENT

IN A NUTSHELL

Art. 3 FADP establishes the so-called "impact principle", according to which the provisions of the FADP apply if the respective data processing operations are "noticeable" in Switzerland. This means that not only purely "Swiss" data processing operations are covered by the scope of application of the FADP, but also those constellations in which data processing is initiated abroad, but the consequences of the processing have an impact in Switzerland.

I. GENERAL

A. Background and purpose of the norm

Public law does not have a codified conflict of laws, unlike private and criminal law. In practice, therefore, the principle of territoriality applies to cross-border public law constellations: Swiss public law always applies when a factual situation occurs in Switzerland. 1

The criteria used to determine the applicable law include, in particular, the place of domicile or residence, the place of activity or the place of effect. According to the case law of the Federal Supreme Court, the so-called principle of effect is a "special manifestation" of the principle of territoriality: Facts that have occurred abroad can be taken into account by Swiss authorities if they have a "sufficient impact on the territory of Switzerland." However, the practice does not uniformly define when a sufficient connection to Switzerland exists within the meaning of the impact principle: generally, it is necessary that the impact is perceptible, significant, substantial or considerable. 2

Art. 3 FADP regulates the local application of the FADP in accordance with the general principles of application of public law and in particular the principle of impact. 3

B. History of origins

The old FADP did not contain any provisions on local application, nor did the draft for the new FADP. During the parliamentary deliberations, however, it was demanded that a provision on the territorial scope of application - which would ideally correspond to Art. 3 para. 1 and 2 DSGVO - be introduced. Ac- 4

cordingly, the FADP should also have applied if a controller or processor with an establishment outside of Switzerland processes data of persons in Switzerland in order to offer them goods or services (against payment or free of charge) or to monitor their behavior in Switzerland.

5 Based on the already existing conflict-of-law rules, in particular in private law, the legislator came to the conclusion during the consultation that the concerns of the persons affected by (international) data processing could be sufficiently taken into account by anchoring the principle of effect defined by case law as well as an explicit reference to the provisions of the Federal Act of 20 March 1981 on International Mutual Assistance in Criminal Matters (IMAC, SR 351.1) or criminal law. Accordingly, the discussed regulation analogous to Art. 3 para. 1 and 2 DSGVO was dropped.

II. APPLICABILITY OF THE FADP ACCORDING TO THE PRINCIPLE OF EFFECT (ART. 3 PARA. 1 FADP)

6 The provisions of the FADP apply on the basis of the effect principle if the respective data processing operations have an effect in Switzerland. Thus, not only purely "Swiss" data processing operations are covered by the scope of application of the FADP, but also those constellations in which data processing is initiated abroad, but the consequences of the processing are "noticeable" in Switzerland.

III. CONFLICT OF LAWS IN DATA PROCESSING OPERATIONS UNDER PRIVATE LAW (ART. 3 PARA. 2 FADP)

7 In the context of private law, the PILA regulates which law is applicable for Swiss courts in international relations; in the context of data protection law, Art. 139 para. 1 PILA must be observed. According to this, the aggrieved person has a broad right to choose the law applicable to his or her case. Specifi-

cally, the aggrieved person has the option to decide whether the law of the state applies,

- in which he or she has his or her habitual residence (para. 1 lit. a),
- in which the author of the infringement has his establishment or habitual residence (para. 1 lit. b), or
- in which the success of the infringing act occurs (para. 1 lit. c).

Thus, the injured person has the possibility to choose the law that is most favorable to him. In order to preserve this advantage, the FADP explicitly states that the PILA shall apply to private law claims. 8

IV. CRIMINAL LAW CONFLICT OF LAWS (ART. 3 PARA. 2 FADP)

The criminal provisions of the FADP (Art. 60 et seq.) are part of the secondary criminal law, which means that their territorial application is determined by the principles of the SCC (cf. Art. 333 para. 1 in conjunction with Art. 104 and Art. 3 et seq. SCC): According to the individual protection principle enshrined in the SCC, anyone who violates the legal interests of Swiss nationals abroad is in principle liable to prosecution. In view of this already existing conflict-of-laws rule, the FADP refers to the Criminal Code and does not contain its own specifications on the territorial scope of application in the criminal law context. 9

The author gives her personal assessment in this commentary.

BIBLIOGRAPHY

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.

COMMENTARY ON

Art. 4 FADP

A commentary by Michael Reinle

SUGGESTED CITATION

Michael Reinle, Commentary to art. 4 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Reinle, art. 4 FADP N. XXX.

Art. 4 Federal Data Protection and Information Commissioner

[1] The Federal Data Protection and Information Commissioner (FDPIC) supervises the application of the federal data protection regulations.

[2] The following are exempted from supervision by the FDPIC:

a. the Federal Assembly;

b. the Federal Council;

c. the federal courts;

d. the Office of the Attorney General of Switzerland in relation to processing personal data as part of criminal proceedings;

e. federal authorities in relation to processing personal data in terms of a judicial activity or proceedings for international mutual assistance in criminal matters.

CONTENT

IN A NUTSHELL

The FDPIC supervises the application of federal data protection provisions. Private individuals and legal entities as well as federal authorities are subject to the FDPIC's supervision. There are exceptions to the supervision of federal authorities based on the principle of separation of powers and to ensure the independence of the judiciary. Exemption from supervision does not mean that the exempt federal authorities are not required to comply with the provisions of the FADP when processing data. Exceptions to the material scope of the FADP are regulated in Art. 2 FADP.

I. GENERAL

A. Purpose of the standard and background

1 The general supervision of the FDPIC over the application of federal data protection provisions does not represent a change compared to the previous FADP (Art. 27 para. 1 aFADP). The main change is that Art. 4 FADP refers to the FDPIC and no longer to the commissioner, as was the case in Art. 27 aFADP. This is due to the fact that the revised FADP distinguishes between the FDPIC as an authority and the commissioner as the head of the authority. However, the term "commissioner" is not defined until Art. 43 para. 1 FADP.

2 Art. 4 FADP derives its significance primarily from the exceptions to the FDPIC's supervision in Art. 4 para. 2 FADP. Under the previous law, only the Federal Council was exempt from FDPIC supervision (Art. 27 para. 1 aDSG). The exception to FDPIC supervision now applies not only to the Federal Council, but also to other federal bodies. The list of exceptions in Art. 4 para. 2 FADP is exhaustive. The FADP does not provide for any exceptions to the FDPIC's supervision of private data processors.

3 The Federal Council was exempted from supervision by the FDPIC because the FDPIC cannot be the supervisory body of its own supervisory and electoral authority.

4 The exceptions for the Federal Assembly, the federal courts, the Office of the Attorney General of Switzerland and other federal authorities in relation to specific data processing operations, which have been newly added in para. 2,

are based on similar considerations. They serve to implement the principle of separation of powers and are intended to guarantee the independence of the judiciary.

B. History

In the draft bill for the revision of the Data Protection Act of October 29, 2014, the supervision of federal bodies by the FDPIC was discussed, but the question of exceptions to this supervision was not addressed at that time. 5

Art. 2 para. 3 and 4 of the draft FADP contained exceptions to the FDPIC's supervision for the federal courts (para. 3) and the Federal Council and the Federal Assembly (para. 4). The exception for federal courts was justified on the grounds that, under the draft FADP, the FDPIC was to be given the power to issue rulings against federal bodies. This could have impaired the independence of the courts and the separation of powers. In addition, the Federal Administrative Court and the Federal Supreme Court are the appeal bodies for rulings issued by the FDPIC. This could have led to a situation where these two courts would have had to review decisions of the FDPIC against themselves. 6

In addition, according to Art. 2 para. 2 lit. c VE-DSG, the processing of personal data by independent federal judicial authorities in the exercise of their judicial functions should be exempted from the FADP and thus also from supervision by the FDPIC. This exception was also justified on the grounds that subjecting these judicial authorities to the supervision of the FDPIC could undermine the principle of separation of powers and the independence of the judiciary. 7

Art. 2 para. 2 lit. c and 3 and 4 VE-DSG were discussed and criticized during the consultation process. Among other things, it was criticized that certain terms were unclear ("independent judicial authorities"), that the exceptions would contradict the SEV 108 Convention, that the FDPIC should continue to supervise the courts but only be able to make recommendations to them, and that the exceptions in Art. 2 para. 3 and 4 VE-DSG should be systematically regulated in the section on the FDPIC and not in connection with the material scope of the FADP. 8

The criticisms raised in the consultation on the draft FADP were taken into account in that a new Art. 3 E-FADP was introduced in the 2017 FADP mes- 9

sage, which deals exclusively with supervision by the FDPIC. This decision separated the issue of supervision from the issue of the material scope of the FADP, which is also correct from a dogmatic point of view. The content of Art. 3 E-DSG corresponds without deviation to the new Art. 4 FADP.

10 Art. 3 E-FADP and Art. 4 FADP were not discussed in the parliamentary deliberations. Instead, the Federal Council's proposal (Art. 3 E-FADP) was accepted without comment.

II. SUPERVISION BY THE FDPIC

A. Supervision of the application of federal data protection provisions (para. 1)

11 Art. 4 para. 1 FADP stipulates that the FDPIC is responsible for supervising the application of federal data protection provisions. Private natural persons and legal entities as well as federal authorities are subject to the supervision of the FDPIC.

12 The wording “federal data protection provisions” emphasizes that the FDPIC does not only supervise the application of the provisions of the FADP. As under Art. 27 para. 1 aDSG, the FDPIC also monitors the sector-specific data protection provisions of the Confederation in accordance with Art. 4 para. 1 FADP. This refers to provisions relevant to data protection in other federal enactments as well as international treaties specific to data protection law.

13 The question of the FDPIC's supervision of federal bodies must be distinguished from the substantive application of the FADP to specific data processing operations carried out by federal bodies. Federal bodies may be subject to supervision by the FDPIC even if some of their data processing operations are excluded from the scope of the FADP under Art. 2 FADP. Conversely, certain federal bodies may be exempt from supervision by the FDPIC (Art. 4 para. 2 FADP), even if their data processing operations are not excluded from the material scope of the FADP under Art. 2 FADP. This applies, for example, to the Federal Council. The Federal Council is exempt from supervision by the FDPIC under Art. 4 para. 2 lit. b FADP, but must comply with the FADP for certain data processing operations. The same applies to the Federal Assembly. The Federal Assembly is now exempt from supervision. Under Art. 2 para. 2 lit. b FADP, certain data processing operations carried out by the

Federal Assembly are also excluded from the material scope of the FADP, but not all.

B. Exceptions to supervision (para. 2)

1. Federal Assembly (lit. a)

The Federal Assembly is exempt from supervision by the FDPIC because otherwise the principle of separation of powers could be impaired. 14

With regard to the exemption of the Federal Assembly from supervision by the FDPIC, the question arises as to how far this exemption extends. The materials do not comment on this question. 15

With regard to Art. 2 para. 2 lit. b FADP, it is striking that the legislature distinguishes between the Federal Assembly, the federal councils and parliamentary commissions when referring to parliament. This suggests that the Federal Assembly refers to the collegiate body pursuant to Art. 148 FC. According to Art. 148 para. 2 FC, the Federal Assembly comprises the National Council and the Council of States. Therefore, the Federal Assembly should not only refer to the joint Federal Assembly as a specific body, but also to the National Council, the Council of States, and the joint Federal Assembly. 16

It is unclear whether the parliamentary commissions and the parliamentary services are also exempt from supervision by the FDPIC. The deliberations of the parliamentary commissions are exempt from the FADP (Art. 2 para. 2 lit. b FADP). However, this exemption only applies to the deliberations themselves and not, for example, to reports on these deliberations or publications. In view of the reasoning behind the exemption of the Federal Assembly, it nevertheless makes sense to also exempt the parliamentary commissions from the supervision of the FDPIC. With regard to the parliamentary services, the decisive factor is whether the data processing is directly related to parliamentary activities. Data processing that is not directly related to parliamentary activities is subject to supervision by the FDPIC. 17

2. Federal Council (lit. b)

According to the dispatch, the Federal Council was exempted from supervision by the FDPIC because otherwise the principle of separation of powers could be impaired. 18

19 The Federal Council refers to the collegiate body. The departments and the Federal Chancellery, on the other hand, are subject to supervision by the FDPIC.

20 The exemption of the Federal Council from supervision by the FDPIC was justified in Art. 27 para. 1 aDSG on the grounds that the electoral body of the Commissioner should not be subject to its supervision. However, the Commissioner is now elected by the United Federal Assembly (Art. 43 f. DSG). Art. 39 E-DSG also provided that the Commissioner was to be appointed by the Federal Council, subject to approval by the Federal Assembly. Therefore, Art. 3 para. 2 E-DSG exempted both the Federal Council and the Federal Assembly from supervision. However, a majority in the National Council then voted in favor of election by the Federal Assembly rather than by the Federal Council. The Council of States followed suit. Since the Federal Council is no longer the body responsible for electing the Commissioner, it is not clear why the Federal Council should continue to be exempt from supervision by the FDPIC. The fact that the Federal Council continues to be exempt from supervision by the FDPIC under Art. 4 para. 2 lit. b FADP is probably due to the fact that Parliament had adopted Art. 3 E-FADP before it dealt with the election of the Commissioner.

3. Federal courts (lit. c)

21 The federal courts are exempt from supervision by the FDPIC because otherwise the separation of powers and the independence of the judiciary could be impaired. This is because the FDPIC now has the power to issue orders to federal bodies (Art. 51 FADP). In addition, the Federal Administrative Court and the Federal Supreme Court are the appeal bodies for decisions of the FDPIC. Without the exemption from supervision, they would have to rule on FDPIC decisions against themselves as the appeal body.

22 In order to meet the requirements of Directive (EU) 2016/680 and E-SEV 108, the federal courts must establish their own independent data protection supervisory authority. This supervisory authority should be structured in the same way as the FDPIC, unless the specific circumstances require otherwise.

4. Office of the Attorney General (lit. d)

23 The Office of the Attorney General is only excluded from supervision by the FDPIC when it processes personal data in the context of criminal proceed-

ings. For other data processing (e.g. in the area of human resources), the Office of the Attorney General is subject to supervision by the FDPIC. The exception is again justified on the grounds of the separation of powers and the independence of the judiciary.

The federal police authorities remain subject to supervision by the FDPIC, even when acting on behalf of the Office of the Attorney General. The FDPIC applies the data protection provisions of the applicable procedural law (Art. 2 para. 3 FADP). 24

5. Federal authorities in relation to judicial activities or international mutual assistance in criminal matters (lit. e)

This exception is also justified by the principle of separation of powers and the independence of the judiciary. 25

Furthermore, the exception was justified in the legislative work on the grounds that the rights of the parties and those involved in proceedings are governed by procedural law, which offers them protection equivalent to that provided by the FADP. 26

Data processing that is not specifically related to judicial activities or international mutual assistance in criminal matters is not covered by the exception and is therefore subject to supervision by the FDPIC. Data processing by the administrative services of these authorities, such as the processing of personnel data, is therefore subject to supervision by the FDPIC. 27

The term “judicial activity” replaces the term “pending proceedings” in Art. 2 para. 2 lit. c aDSG. 28

The exception mainly concerns the Office of the Attorney General and the Federal Office of Justice. According to the Federal Council's declaration on Article 1 of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959, the Federal Office of Justice is to be regarded as a Swiss judicial authority within the meaning of the Convention. However, the exception is of limited scope. The FDPIC may review the lawfulness of data processing if a data subject asserts their rights under Article 11c E-IMAC. 29

Data processing by federal authorities in the context of administrative criminal proceedings is not covered by this exception. 30

BIBLIOGRAPHY

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.

MATERIALS

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, BBl 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.

COMMENTARY ON

Art. 5 lit. c FADP

A commentary by Franziska Sprecher

SUGGESTED CITATION

Franziska Sprecher, Commentary to art. 5 lit. c FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Sprecher, art. 5 lit. c FADP N. XXX.

Chapter 2 General Provisions

Section 1 Definitions and Principles

Art. 5 Definitions

In this Act:

c. *sensitive personal data* means:

data relating to religious, philosophical, political or trade union-related views or activities,
data relating to health, the private sphere or affiliation to a race or ethnicity,
genetic data,
biometric data that uniquely identifies a natural person,
data relating to administrative and criminal proceedings or sanctions,

data relating to social assistance measures;

CONTENT

IN A NUTSHELL

Sensitive personal data is a specific subcategory of personal data that requires special protection due to the increased risk of discrimination or stigmatization. Its processing is only permitted under strict legal conditions, such as with explicit consent, after conducting a prior data protection impact assessment, or on the basis of a formal law in the case of processing by a public authority.

I. GENERAL

1 Sensitive personal data is a **privileged subcategory of personal data** (Art. 5 lit. a FADP). It is classified as particularly sensitive in view of the protection of the fundamental rights and personality of data subjects (risk of discrimination or stigmatization based on these characteristics) (see N. 6 ff.). Art. 5 lit. c FADP lists the categories of particularly sensitive personal data *in an exhaustive manner*. Subject to special legal provisions, particularly sensitive personal data is included wherever the law refers to personal data.

2 The **permissibility of processing** this privileged type of personal data is subject to special conditions imposed by the legislator. For example, the legislator imposes higher requirements on consent to the processing of particularly sensitive personal data. In particular, consent must be given *expressly* (e.g. Art. 6 para. 7 lit. a FADP). In addition, there is an obligation to carry out a *data protection impact assessment* (e.g., Art. 22 para. 2 lit. a FADP). Federal authorities require a *legal basis in the formal sense* for the processing of particularly sensitive personal data (Art. 34 para. 2 lit. a FADP).

A. Purpose of the standard and background

3 In creating the *abstract, formal categories* of particularly sensitive personal data, the legislator assumes that there are certain types or categories of data that are particularly sensitive due to their close connection to a person's private life or confidential matters. The **sensitivity** of this data poses a particular risk to the personal rights of the persons concerned (e.g., risk of stigmatization based on characteristics), which makes this data particularly worthy of protection. This view is shared by the FADP with ER-Konv-108+ (Art. 6) and with Directive 2016/680 (Art. 10) and the DSGVO (Art. 9).

B. History

The category of particularly sensitive personal data was already included in the aDSG (Art. 3 lit. c aDSG) and, according to the Federal Council, should be retained even after the total revision of the FADP. In the context of the revision, the Federal Council considered the protection of "sensitive personal data" to be central to "maintaining the EU's adequacy decision" and emphasized that "the Federal Council's catalog [...] therefore meets the minimum requirements of the Data Protection Convention 108 plus and the Schengen-relevant EU Directive on data protection in criminal matters." 4

Attempts to shorten the catalog already existing under the aDSG failed in parliamentary deliberations (see N. 12, N. 32). Instead, as part of the total revision of the FADP, the concept of particularly sensitive personal data was extended to include **genetic data** and **biometric data** that uniquely identify an individual, as well as **data on ethnic origin**, thereby aligning the FADP with Art. 6 para. 1 ER-Conv-108+ and Art. 10 Directive EU 2016/680. 5

II. SENSITIVE PERSONAL DATA IN GENERAL

Sensitive personal data is **formally and abstractly categorized** in the FADP. The legislator assumes that the personal data designated as particularly sensitive in Art. 5 lit. c FADP particularly affect the personal rights of the data subject due to their *sensitivity*, as they originate from the secret sphere or private life of the person and/or can significantly influence their reputation. The classification as particularly sensitive personal data is not based on the existence of a specific risk to the personality or fundamental rights, but rather on the fact that the information in question relates to an aspect of life that belongs to one of the areas protected by law. 6

This approach, which is based on a *definitive*, formal-abstract categorization, is *controversial*. The risk to personal rights does not arise from specific formal legal types of data, but from their use for a specific purpose or in a specific context, the scope of processing, etc. (**context of use**). The focus should be on the *actual sensitivity* of data with regard to the protection of the privacy of a specific data subject. 7

In addition, the terms used to definitively describe the categories of particularly sensitive personal data are **vague**, and the selection appears static, anti- 8

quated, and incomplete. Although this criticism already existed under aDSG, the formal, abstract categorization was retained in the total revision. *Rudin* rightly emphasizes: "It is not the data itself, but its use in a specific context (the **context of use**) that poses the risk."

9 Since the total revision of the FADP, data relating to legal entities no longer falls within the scope of the law. Accordingly, the term "personal data" (Art. 5 lit. a FADP) and thus also that of "sensitive personal data" (Art. 5 lit. c FADP) applies only to **natural persons**.

III. DATA ON RELIGIOUS, IDEOLOGICAL, POLITICAL, OR TRADE UNION VIEWS OR ACTIVITIES (NO. 1)

10 According to Art. 5 lit. c no. 1 FADP, **data on religious, ideological, political or trade union views or activities** are considered particularly sensitive personal data. The provision also refers to membership in relevant associations. No. 1 thus covers data on a person's religious beliefs or denomination, their party affiliation, or their membership in an employee organization, a free church, or an association that represents a particular political or ideological stance (including Masonic associations and religious youth organizations). For *Glass*, it is unclear how broadly the term "religious or ideological data" should be interpreted. However, with regard to the protection of freedom of belief and conscience, it seems plausible to include all data that allows conclusions to be drawn about a person's beliefs, conscience, or ideological stance. The provision was taken over unchanged from the old law and corresponds to Art. 3 lit. c no. 1 aDSG.

11 In view of the sometimes far-reaching consequences that the processing of particularly sensitive personal data can have (N. 3), it is necessary to examine in each case whether the processing of such data is actually necessary and whether it can be dispensed with (e.g., by not including religious affiliation in the personnel file).

12 During the political deliberations on the FADP, an unsuccessful attempt was made to remove trade union views or activities from the list in Art. 5 lit. c no. 1 FADP.

IV. DATA CONCERNING HEALTH, PRIVACY, OR RACIAL OR ETHNIC ORIGIN (NO. 2)

According to Art. 5 lit. c no. 2 FADP, data concerning health, privacy, or racial or ethnic origin are also considered particularly sensitive personal data. 13

According to the message on aDSG (message 1988), under the old law, **data on health** included all information that in a broad sense constituted a medical finding and "could have a negative effect on the persons concerned." In view of today's understanding of health and medical and technological advances, this (historical) understanding of health data, in particular the requirement of a negative impact on health, is too narrow. Furthermore, the characteristic of negative effects is hardly taken into account in practice. Consequently, a broader definition of health data must be assumed today. *Vokinger* points out that health data used to arise mainly from the doctor-patient relationship. Today, patients themselves are increasingly collecting data via apps, wearables, or social media. Companies outside the traditional healthcare sector (Google, Amazon, Apple, etc.) are also increasingly processing health data. Consequently, this data is not limited to clinical information, but increasingly also includes (genetic) information that may be available even before a clinical manifestation. Whether certain data can be classified as health data does not depend directly on the data itself, but rather on the context in which it is used. Identical information—such as the number of steps taken each day—may be considered lifestyle data for a healthy person, but may be considered health data for a patient with diabetes mellitus or heart failure, for example. 14

The DSGVO also takes a **broad view of the term "health data"**: "Personal health data should include all data relating to the health status of a data subject and from which information about the past, present, and future physical or mental health status of the data subject can be derived." 15

A broad understanding of health data makes sense because in healthcare—especially under the influence of rapidly developing information technologies—the boundaries between therapy and lifestyle are becoming increasingly blurred (keywords: real-world data and real-world evidence). Accordingly, information about a person's state of health does not only qualify as health data within the meaning of Art. 5 lit. c no. 2 FADP if it relates to a negative state of health. Similarly, depending on the context, information that a person is *not* affected by a disease or leads a certain lifestyle may now constitute health 16

data within the meaning of Art. 5 lit. c no. 1 FADP. Even the *accuracy* of such data is not relevant for its classification as particularly sensitive health data, as it is precisely inaccurate information (e.g., an incorrect diagnosis automatically generated by an incorrect interpretation of data or an inaccurate correlation) that can jeopardize a person's personal rights.

17 The term "health data" is also found in the HRA. In **Art. 3 lit. f Human Research Act**, *health-related personal data* is defined as "information about an identified or identifiable person relating to their health or illness, including their genetic data." According to the HRA message, personal data is health-related if it "relates to a physical or mental illness or provides information about the structure and function of the body of the person concerned." According to the HRA message, the concept of health data coincides with that of the FADP.

18 The **sphere of intimacy** includes data "that a person only shares with a select few and that is of great emotional significance to them." The sphere of intimacy goes beyond sexual life, but does not extend to financial circumstances, for example. The private sphere includes, among other things, information about therapies, fears or other feelings, addictive behavior, etc. The concept of the private sphere is based on the Federal Supreme Court's "three-sphere theory," which distinguishes between the intimate or secret sphere, the private sphere, and the public sphere. The private sphere covers the personal affairs of the person concerned, which should in principle remain unknown to third parties unless the persons concerned themselves disclose the information. According to the message, a person's gender identity can – depending on the situation – be classified as either part of the private sphere or as health data.

19 Even in the revised version, the FADP retains the term "data on membership of a race" in Art. 5 lit. c no. 2 FADP. The dispatch emphasizes – with reference to the EU – that retaining the term "racial affiliation" does not mean that the legislature approves of racial theory, which assigns people to a "race" in a judgmental, racially ideological manner based on their external characteristics. The term was retained primarily in accordance with Art. 6 para. 1 ER-Conv-108+, Art. 10 Directive EU 2016/680, and Art. 9 para. 1 DSGVO, and was accepted by Parliament without discussion.

20 The concept of race in Art. 5 lit. c no. 2 FADP was supplemented by **data on ethnicity** during the total revision. This was done in accordance with Art. 10

of Directive (EU) 2016/680 and Art. 9 para. 1 DSGVO. Ethnic origin refers to membership of a group of people who feel connected to each other on the basis of their history, language, customs, culture, traditions, etc., and who perceive themselves as a community that is different from the rest of the population and/or is perceived as different by the rest of the population. *Rudin* cites the terms "Tamil" and "Kurd" as examples. Ethnicity is not the same as nationality. In some cases (e.g., "Serbs"), the latter may coincide with ethnicity.

V. GENETIC DATA (NO. 3)

Since the total revision of the FADP, **genetic data** has been explicitly included in the category of particularly sensitive personal data under Art. 5 lit. c FADP. Genetic data is *information about the genetic makeup of a person* that is obtained through genetic testing. According to the dispatch, the term "genetic data" in the FADP corresponds to the definition in Art. 3 lit. l aGUMG, which has now been adopted in Art. 3 lit. k GUMG. According to Art. 3 lit. g HRA, "genetic data" is "information obtained through genetic testing about characteristics inherited or acquired during the embryonic phase." 21

Genetic data can be obtained from almost all types of biological material (blood, hair, saliva, etc.) using **genetic testing**. According to Art. 3 lit. a GUMG, genetic testing refers to "cytogenetic and molecular genetic testing to determine characteristics of human genetic material, as well as all other laboratory tests directly aimed at obtaining such information about human genetic material." 22

Genetic data also includes **DNA profiles** in accordance with Art. 3 lit. j GUMG: A DNA profile refers to "specific characteristics of a person's genetic material that are determined by genetic testing and used to clarify their ancestry or to identify that person." 23

According to *Rudin*, Art. 5 lit. c no. 3 FADP is based on a **broad understanding** of genetic data. This means that it covers not only data obtained by sequencing individual genomes, but also, among other things, information obtained through the use of genetic markers (e.g., in oncology). However, only genetic data that qualifies as personal data in accordance with Art. 5 lit. a FADP falls within the scope of the FADP and, in particular, under the definition of particularly sensitive personal data. Cell material and biological samples do not constitute genetic data as long as no information about the genetic 24

makeup of the persons concerned has been obtained from them. In this context, *Rudin* rightly raises the question of the extent to which, according to the current and future state of science, "genetic data in a specific context does not actually allow conclusions to be drawn about a specific person."

VI. BIOMETRIC DATA THAT UNIQUELY IDENTIFIES A NATURAL PERSON (NO. 4)

25 During the total revision of the FADP, **biometric data** was newly included in the catalog of particularly sensitive personal data in Art. 5 lit. c.

26 Biometric data are **physical characteristics** that are recorded, measured, and documented. This is personal data "obtained by a specific technical process relating to the physical, physiological, or behavioral characteristics of an individual and which enables or confirms the unique identification of that person." It can only be changed with great effort (e.g., surgical intervention). Typically, digital fingerprints, hand vein patterns, voice recordings, facial images, or images of the iris fall under biometric characteristics.

27 The use of biometric data carries the risk that a person's behavior can be tracked and a comprehensive profile created, or that it may allow conclusions to be drawn about particularly sensitive personal data in accordance with Art. 3 lit. c aDSG. In addition, biometric data is **permanently compromised** if misused, for example through identity fraud. Accordingly, even before the revision and explicit inclusion in the catalog of particularly sensitive personal data, biometric data could already be considered particularly sensitive data within the meaning of the aDSG.

28 Not all biometric data is considered particularly sensitive personal data. In order for biometric data to fall under Art. 5 lit. c no. 4 FADP, it must be collected using a special technical procedure that allows the **unique identification or authentication of a person**. For this reason, according to the message, ordinary photographs of a person, faces, or simple body parts are not covered. Unless they have been processed using a special technical procedure that allows for unambiguous personal identification (e.g., facial recognition software). Jacot-Guillarmod points out that modern facial recognition programs can generate a "biometric template" from ordinary photos that can be used to recognize the person depicted. She raises the question of whether it makes sense to protect such a biometric template as sensitive data without at the

same time extending the protection to the photos from which the template was obtained.

VII. DATA ON ADMINISTRATIVE AND CRIMINAL PROCEEDINGS OR SANCTIONS (NO. 5)

Data on administrative and criminal proceedings or sanctions also remain classified as particularly sensitive personal data under Art. 5 lit. c no. 5 FADP. In addition to the proceedings and sanctions expressly mentioned in the text of the law, disciplinary proceedings, driving license revocations, and penal measures also fall under this provision. However, information about the initiation, implementation, and conclusion of prosecutions and revocations of permits, etc., as well as the corresponding enforcement measures, also fall under Art. 5 lit. c. No. 5 FADP. 29

In order for data to be considered particularly sensitive personal data, it must relate to **sovereign prosecutions or sanctions**. It is irrelevant whether the sanctions or prosecutions are carried out by Swiss or foreign authorities. 30

VIII. DATA ON SOCIAL ASSISTANCE MEASURES (NO. 6)

Particularly sensitive personal data pursuant to Art. 5 lit. c no. 6 FADP includes **data on social assistance measures**. According to the message on Art. 3 lit. c aDSG, this includes "social insurance benefits in connection with illness and accident, as well as guardianship and welfare measures." Primarily, social insurance benefits are covered insofar as they allow conclusions to be drawn about the state of health (cf. Art. 5 lit. c no. 2 FADP). Social assistance measures pursuant to Art. 5 lit. c no. 6 FADP also include, among other things, information on the use of social services, unemployment insurance, and information on individual social assistance benefits, welfare measures or child and adult protection measures, protective custody, and other means-tested social benefits (health insurance premium reductions, rent subsidies, supplementary benefits to AHV/IV, etc.). 31

A majority of the National Council's Political Institutions Committee wanted to remove social assistance measures from the list of particularly sensitive personal data, which would have weakened data protection in this area, but without creating a difference to ER-Konv-108+ or Directive (EU) 2016/680. The motion was rejected by a two-thirds majority in the National Council. 32

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 5 lit. d FADP

A commentary by Hannes Meyle

SUGGESTED CITATION

Hannes Meyle, Commentary to art. 5 lit. d FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Meyle, art. 5 lit. d FADP N. XXX.

Chapter 2 General Provisions

Section 1 Definitions and Principles

Art. 5 Definitions

In this Act:

d. *processing* means any handling of personal data, irrespective of the means and procedures used, in particular the collection, storage, keeping, use, modification, disclosure, archiving, deletion or destruction of data;

CONTENT

I. GENERAL

The term "processing" is to be understood very broadly and encompasses **all handling** of personal data – "roughly speaking: everything that is done with personal data". For example, Art. 5 let. d mentions the forms of processing "obtaining, storing, keeping, using, modifying, disclosing, archiving, deleting or destroying". The terms "storing" and "deleting" were added to bring the wording of Art. 5 let. d FADP closer to that of Art. 4 no. 2 DSGVO. In terms of content, however, the concept of processing remains unchanged by the revision of the law. The old legal concept of data collection was subsumed under the concept of processing. 1

A complete terminological alignment with the DSGVO did not take place for "practical reasons". The FADP speaks of *the act of* processing or *the act of* processing, whereas the DSGVO speaks of *the act of* processing | *the act of* processing. In addition, the examples in Art. 5 lit. d FADP differ significantly from those mentioned in Art. 4 No. 2 DSGVO. However, despite the editorial differences, "*the* processing" within the meaning of the FADP and "processing" within the meaning of the DSGVO are to be understood **as congruent**. When interpreting the term "processing" in accordance with Art. 5 let. d FADP, case law regarding Art. 4 no. 2 DSGVO can therefore be used for orientation purposes. 2

A central principle of the FADP is its technology-neutral character. Therefore, the question of whether processing is taking place is **irrelevant to the means and procedures** used. Processing within the meaning of the FADP can therefore be both manual and automated. It also follows from the technology-neutral character that the FADP also covers or will cover future forms of processing that are not yet known. 3

II. PROCESSING AS A REQUIREMENT FOR THE APPLICATION OF THE FADP

The concept of processing is of central importance, since the FADP is only applicable if personal data is processed by any entity involved in the handling of personal data. The resulting obligations then depend on whether the respective entity is a (jointly) responsible party or a processor. Processing requires an action that has the purpose and effect of doing something with the 4

data, or an action that **objectively relates to the data**. By contrast, actions that merely affect data are not considered processing, such as transporting passengers by bus or train if these passengers are carrying personal data stored on data carriers. It is immaterial whether or not the personal data in question is actually taken note of by a person, which is why processing by means of computer programs is also covered. The purely mental handling of personal data is not considered processing within the meaning of Art. 5 let. d. Accordingly, information that is only present in a person's memory is also not covered by the right of access under data protection law.

5 Sometimes difficulties arise in **defining the term 'processing'** or assigning data processing to specific persons, as the case decided by a German court on the storage of files shows: a real estate company became the owner of a disused hospital property following insolvency proceedings, and patient files were found in the building. The owner objected to the official order to store the files in a specially protected location. The court ruled that the owner was not deemed to be processing the data because she had not stored the files herself and was not handling them in any other way. However, this did not determine whether another entity was processing the data or had it processed as a processor or controller.

6 Questions about the scope of the processing concept have also recently arisen in connection with AI systems. The fact that the handling of information – insofar as it is personal – using AI systems constitutes processing is a consequence of the broad concept of processing and the technology-neutral design of the FADP. However, in individual cases, it may be less clear how to distinguish between different processing operations, such as those that occur when AI systems are used in a collaborative way. This distinction is relevant because it affects who is responsible for compliance with data protection law (in particular, for safeguarding the rights of data subjects) and for any violations that occur during processing. In order to define the obligations, the EU AI ODR differentiates between the different roles of the actors, including between providers and operators of AI systems. Such distinctions are not yet established in data protection law. However, it would be obvious to distinguish here as well between the creation of an AI system (i.e. the associated training, insofar as personal data is involved) and its use.

III. SPECIFIED FORMS OF PROCESSING

The list of specified forms of processing is **merely an example** and the terms overlap to some extent. Only some of the specified forms of processing are subject to specific instructions, such as the collection, disclosure and destruction of data. In all other respects, the data protection principles must be observed for all processing. If an activity cannot be assigned to any of the named forms of processing, it is still possible that it is an unnamed form of processing (see Chapter I above). The named forms of processing are therefore less central to the application of the FADP. 7

A. Collection

Data collection occurs when the collecting body obtains **intentional knowledge of** the data or justifies the disposition of it. It is not procurement if the data is provided by the data subject or by third parties without request and the data recipient does not intend to process it (e.g. when receiving a misdirected e-mail, when listening in on a conversation, etc., although in such a case processing may be involved under certain circumstances). In contrast, personal data is obtained if the relevant body generally wishes to obtain data in general and accepts that personal data may also be obtained in the process. According to Art. 6 para. 3 FADP, data may only be obtained for a specific purpose that is recognizable to the data subject and entails the obligation to provide information in accordance with Art. 19 FADP. Examples of typical procurement actions include collecting data from other sources, recording or logging information. Whether data is protected or freely available is irrelevant. Therefore, for example, a targeted web search on the internet can also constitute the procurement of personal data and lead to the applicability of the FADP. It is not necessary to actually take note of the content of the data; rather, it is sufficient that the data first comes into the possession of a controller. Thus, automated forms of data collection, such as so-called data scraping, also qualify as procurement within the meaning of the FADP. The above principles also apply in the context of generative AI systems: If personal data is collected unintentionally, it is generally not considered to have been obtained, nor is it considered to have been obtained if existing personal data is merely modified (e.g. by generating or editing a text). However, if generative AI systems are used to obtain additional information about a person or to invent such information, 8

this will regularly constitute data collection from a data protection perspective.

B. Storage

9 The term "storing" was introduced in order to align with the wording of the relevant **European legal sources,** including in particular Art. 4 no. 2 DSGVO. According to Art. 4 No. 2 DSGVO, storage is understood to mean the retention of data in embodied form on a data carrier (hard disk, server, USB stick, etc.) with the aim of being able to further process the data at a later point in time. Depending on the purpose, the retention of information in AI systems can also be considered storage (see above n. 6).

10 The **DSV** refers to the term storage in connection with the data security requirements (Art. 3 para. 2 lit. b and e DSV) and the logging requirement (Art. 4 para. 2 and 3 DSV).

C. Retention

11 Retention can be described as the activity by which data is kept available **in the processing context**. In contrast to archiving (see n. 15 below), retained data can therefore still be used. Retention is expressly subject to the FADP as a form of processing, since violations of privacy are still possible even at this stage of processing, for example due to deficiencies in data security. Storage is addressed in Art. 12 para. 2 let. e FADP, according to which the storage period must be indicated in the processing directory, and in the context of the right of access under Art. 25 para. 2 let. d FADP.

D. Use

12 Data use refers to any activity with the aim of using the **information content** of the data (including taking note of the data). The use of the data is mentioned in Art. 5 let. f FADP (profiling), Art. 21 DDO (technical requirements for implementing the release of data) and in Art. 4 para. 5 DDO (logging). However, the FADP and the DSV do not provide specific instructions for the use of data.

E. Modifying

Data modification can be described as an "activity that changes the information content of personal data (**rearranges the content**)." The FADP does not provide for any special instructions for action – apart from compliance with the processing principles – or legal consequences; the alteration of data is mentioned in Art. 3 para. 3 let. a DSV (input control), as well as Art. 4 para. 2 and 3 DSV (logging). 13

F. Disclosure

Disclosure of data is a particularly **sensitive form of processing** and is therefore the subject of a separate provision in OC-NN, Art. 5 let. e FADP. [Comment forthcoming] 14

G. Archiving

Archiving means the **keeping available** of data detached from the processing context. In contrast to storage (see N. 11 above), archiving involves removing data from the previous processing context. It follows that the intensity of the impairment of the privacy of the data subjects is typically reduced. This is expressed in Art. 32 para. 1 let. b and Art. 41 para. 5 FADP, which restrict the rights of data subjects in the case of processing for archiving purposes. In addition, Art. 38 FADP (Special regulation for federal bodies for the provision of certain personal data for the federal archives) refers to archiving purposes and archiving. 15

H. Erasure or destruction

The term **destruction** implies that data is destroyed irretrievably. If the data is physically stored on paper, the paper should be burned or shredded. For electronically stored data, the corresponding storage medium must be rendered unusable and all copies must be treated in such a way that the data can no longer be read. 16

The term "**deletion**" is typically used for electronic data processing and is less far-reaching in comparison: for deletion, it is generally sufficient to use the deletion commands of the respective program so that the data can no longer be recognized in the course of normal program operations and can only be restored with disproportionate means. In other words, personal data is delet- 17

ed when it can no longer be linked to a specific person. Effective anonymization is therefore equivalent to deletion and is one method of deleting personal data. In this context, the so-called relative approach must be applied, which means that the perspective of the persons or units that have access to the data is decisive. However, this also means that it can be difficult to assess in individual cases whether personal data has been effectively deleted because data remains in systems after deletion commands have been executed and can potentially be restored. In such cases, the question arises as to whether the restoration of the data or access to the data requires a disproportionate effort. This can only be assessed on a case-by-case basis, depending on the technical circumstances, but also depending on the interest that third parties might have in restoring the personal reference.

18 The distinction between the concepts of deletion and destruction, which is clearly laid out in the legislative materials, is **not consistently implemented** in the FADP. For example, Art. 6 para. 4 FADP requires that data be "*destroyed* or anonymized as soon as they are no longer required for the purpose of processing" – deletion would also be correctly mentioned here. Even if the law does not use the terms consistently, for the sake of clarity, care should be taken when drafting contracts, for example in the context of order processing contracts, to ensure that the terms of deletion and destruction are not inadvertently reversed. In particular, care should be taken to avoid inadvertently agreeing to the destruction of data instead of an obligation to delete, because destruction may be difficult to carry out or undesirable in the case of electronic data processing (see above, n. 16).

BIBLIOGRAPHY

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).

COMMENTARY ON

Art. 5 lit. f und g FADP

A commentary by Matthias Glatthaar / Annika Schröder

SUGGESTED CITATION

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

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

Chapter 2 General Provisions

Section 1 Definitions and Principles

Art. 5 Definitions

In this Act:

f. *profiling* means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person`s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
g. *high-risk profiling* means profiling that poses a high risk to the data subject`s personality or fundamental rights by matching data that allow

an assessment to be made of essential aspects of the personality of a natural person;

CONTENT

IN A NUTSHELL

The profiling term in the new FADP replaces the previous term personality profile. The provisions on profiling were extensively discussed in the parliamentary deliberations and were one of the reasons for the long legislative process. Profiling is defined as automated data processing for the purpose of evaluating personal aspects. Such profiling is very common in practice, especially in the area of offer personalization, and has no special legal consequences for private data controllers. In addition to normal profiling, the new FADP also recognizes a qualified form of "high risk" profiling. The FADP thus deviates from the DSGVO, which only recognizes qualified profiling in connection with automated individual decisions. High-risk profiling exists if an assessment of essential aspects of the personality is possible by linking data. The classification as high-risk profiling is highly case-dependent and triggers primarily the obligation to conduct a data protection impact assessment, but does not lead to a general consent requirement.

I. GENERAL

A. Preliminary Remark

1 Profiling as an automated assessment of personal aspects is a widely used procedure today, which is of great practical importance especially as a basis for the very widespread offer personalization in the end customer business. Digital services such as streaming services, online stores and social media platforms in particular usually have so much "content" that they could not be used meaningfully without personalization. Today, customers take it for granted that such digital offerings will provide targeted guidance, e.g., on the basis of previous usage behavior.

2 Profiling is thus an everyday process that is often in the interest of customers. However, since profiling involves an evaluation that is usually automated on the basis of correlations and probabilities, the process is considered to be risky and therefore in need of regulation. Profiling always means a generalized personality assessment based on certain characteristics, which may not do justice to the specific person concerned ("pigeonholing"). The heightened sensitivity of profiling is particularly evident when it comes to applications

outside of the end-customer business, e.g., use by authorities in the security and law enforcement sectors.

B. History of origins

The new term "profiling" introduced by the revision replaces the "personality profile" of the previous FADP. While personality profile describes a static state, the new term profiling refers to the assessment process as such. The concept of personality profile was a Swiss peculiarity and with its replacement by the term profiling, there is an alignment with European law (although personality profile has been reborn mutatis mutandis in the form of "high-risk profiling"). The new terminology is also intended to reflect technological progress, e.g., in the areas of Big Data and artificial intelligence, and the associated expanded possibilities for data processing. 3

Profiling was one of the main points of discussion in the legislative process. Differences on profiling were a major factor in the delayed passage of the revised law. There was particularly extensive debate about whether and to what extent profiling should require consent. In the preliminary draft of the FADP, profiling without the explicit consent of the data subject was still listed among personality violations. However, this consent requirement was dropped in the further legislative process. The right to object to profiling, which was put up for discussion, also failed to gain acceptance in parliament. Details of the definition and, in particular, the concept of "high-risk profiling," which was only created during the parliamentary deliberations and remained controversial until the end, were also the subject of discussion. 4

C. Systematics and Delimitation

Art. 5 FADP distinguishes between two forms of profiling: on the one hand, in lit. f, "normal" profiling as automated data processing for the purpose of evaluating personal aspects, and on the other hand, in lit. g, qualified "high-risk" profiling based on normal profiling. While the definition of normal profiling was adopted unchanged from the DSGVO into Swiss law, qualified profiling with high risk is an original creation of the Swiss legislator. With the gradation, the legislator wanted to take into account the fact that the various applications of profiling differ, sometimes considerably, in terms of scope and effects. 5

6 Profiling must be distinguished from automated individual decision-making pursuant to Art. 21 FADP. Profiling is the evaluation process that may underlie an automated individual decision, but is logically upstream of it. Profiling only leads to an automated individual decision if the evaluation manifests itself in a concrete external effect and this external effect is in the form of a legal consequence or a similarly drastic impairment.

II. PROFILING (LIT. F)

A. General

7 The change in terminology from personality profiling to profiling was intended to bring about an alignment with European law, and the legislator has consequently adopted the legal definition of Art. 4 No. 4 DSGVO almost verbatim into Swiss law. Essentially, it comprises four elements: firstly, an evaluation process which, secondly, is automated and, thirdly, produces statements about personal aspects which, fourthly, relate to a natural person. These elements are illustrated below using the example of personalized reading recommendations in bookstores.

B. Assessment Process

8 The focus of the concept of profiling is on the element of assessment. At its core, profiling is an evaluation process in which new knowledge about a person is derived through analysis or prediction. "Prediction" in this context expresses the fact that profiling usually aims at a future-oriented consideration, e.g., in order to make a prediction about which books customers might put in their shopping carts in the case of the book trade. "Analysis," the second form of evaluation mentioned in the legal definition, in contrast, represents an assessment of past or present aspects, although analysis does not usually stand alone, but in turn forms the basis for forward-looking statements.

9 A valuation always involves a normative classification and is therefore subjective to a certain extent. If there is no subjective scope for judgment and it is only a question of the objective determination of a fact, there is no valuation. The mere calculation of the location by a navigation system, for example, contains no more an element of evaluation than the mere retrieval, filtering or sorting of data in a database. If a bookseller sorts her customers on the basis of characteristics such as age or place of residence and forms corresponding

customer groups, this is therefore not profiling. Even if she extracts buyers of a certain author from her customer database in order to draw their attention to a new publication by the same author, the bookseller is merely filtering and not profiling. If, on the other hand, the bookseller assigns e.g. buyers of George Orwell's "1984" to the customer segment "dystopian literature", this is a valuation and thus profiling.

C. Automation

Profiling pursuant to Art. 5 lit. f FADP only covers the automated processing of personal data. Processing is automated if it is carried out with the aid of computer-assisted techniques. There is no automation if the assessment is based exclusively on a human train of thought, i.e. only takes place "in the mind of a human being". 10

If, for example, a bookseller knows the preferences of her customers and makes individual recommendations to them based on these preferences (e.g., if she recommends Margaret Atwood's "The Handsmaid's Tale" to a reader of "1984"), this is not profiling within the meaning of the law because there is no automation. The fact that the bookseller makes notes on each customer in an electronic database does not change this. If, on the other hand, the bookseller has the recommendations calculated by an algorithm, this is an automated process and therefore constitutes profiling. In this case, the automation is not already cancelled out by the fact that the bookseller defines the criteria herself to a certain extent (e.g. assigns authors or books to certain genres), as long as the evaluation is computer-aided and is not limited to simple "if-then" queries. 11

The concrete technical design of the profiling process is not decisive. The concept of profiling is technology-neutral and the qualification as profiling is independent of the technical processes used. In practice, recommendation systems for digital offerings in particular are often based on so-called "collaborative filtering", in which the preferences and behavior of other users are taken into account in addition to the user's own user history and content information. For example, in an online bookstore, if user A and B like similar books and user A has positively rated a particular book that user B has not yet purchased, then the system could recommend that book to user B. However, the use of such correlation-based methods is not conceptually essential. 12

D. Personal aspects

13 For profiling to exist, the assessment must lead to new knowledge about personal aspects of natural persons. Art. 5 lit. f FADP contains a list of personal aspects, the assessment of which may constitute profiling: Work performance (e.g., compliance with quality standards or achievement of productivity goals), economic situation (e.g., income situation or savings behavior), health (e.g., dietary habits or risk propensity for certain diseases), personal preferences (e.g. investment preferences, favorite genres, or preferred travel destinations), interests (e.g., hobbies or leisure activities), reliability (e.g., creditworthiness or personality types), behavior (e.g., social interactions or purchasing behavior), location or change of location (e.g., movement patterns, walking routes, or mobility behavior).

14 The enumeration in Art. 5 lit. f is very comprehensive, but not exhaustive ("in particular"), and depending on the context, other aspects may also be relevant. The element of the personality aspect therefore has hardly any limiting effect. What is required is that the aspect has a certain complexity and is therefore amenable to evaluation in the sense of a subjective assessment. Aspects which do not allow for discretion and can therefore be determined purely objectively do not fall within the scope of profiling (e.g. the determination of body weight). However, as a future-related datum, the same aspects may require assessment (e.g., predicted future body weight). In addition, purely objectively ascertainable aspects may serve as a data basis for the evaluation of other, discretionary aspects (e.g., body weight as an indicator of certain disease risks).

E. Personal reference

15 Profiling in the legal sense finally requires that the statements made refer to individual persons. If, on the other hand, the statements only refer to groups of persons from which no individual persons can be determined, there is no profiling, even if the processing is based on personal data as "input". If, for example, a bookseller merely analyzes which authors and genres are most popular in the various age groups for the purpose of optimizing the product range, without making any statements about individual customers, she is not conducting profiling. The same applies to the analysis of website usage for the purpose of improving user-friendliness, where no personal evaluation is carried out.

There is also no profiling if the processing is based only on anonymous or aggregated data, i.e. the "input data" itself has no personal reference at all. This is not processing of personal data and data protection law is not applicable (Art. 2 para. 1 FADP). However, if the purpose of the processing is precisely to de-anonymize the data, which are in themselves anonymous, and to (re)allocate them to individual persons, this is again a processing of personal data subject to data protection law. In this case, profiling may be involved, the purpose of which is precisely to de-anonymize data by establishing connections. 16

III. HIGH-RISK PROFILING (LIT. G)

A. General

With "high-risk profiling", Art. 5 lit. g FADP introduces a qualified form of profiling based on normal profiling. The legal concept of "high-risk profiling" was first created in the legislative process and was the subject of intense debate in Parliament. Discussions included formulations that would have been based on whether profiling produces personal data worthy of special protection, or on whether profiling extends to various areas of the data subject's life. Finally, the approach of adopting the previous legal concept of the "personality profile" in terms of content, although not in name, has prevailed. High-risk profiling is essentially profiling that leads to a personality profile in accordance with the previous FADP. The personality profile was only superficially abolished with the new FADP. 17

High-risk profiling is a Swiss peculiarity. The DSGVO does not recognize such a qualified form of profiling and makes special legal consequences in the case of profiling dependent on whether the profiling is carried out in connection with an automated individual decision. Greater alignment with the DSGVO could therefore have been achieved if the criterion for "high-risk profiling" had been defined as whether the profiling has legal effects on the data subject or significantly affects him or her in a similar way. The fact that instead the previous personality profile was revived and a Swiss peculiarity was perpetuated is to be regretted. An opportunity was missed here to create greater convergence with the DSGVO. 18

For there to be "high-risk profiling" pursuant to Art. 5 lit. g FADP, two elements must be present in addition to normal profiling: first, a linkage of data and second, essential aspects of the personality to which the statements gen- 19

erated by profiling potentially relate. The two additional elements are both necessary and sufficient. This means, first, that the eponymous high risk is assumed to exist if the two elements mentioned are present. The high risk is not an additional conceptual element that must be examined separately in each case. Further, it means that profiling that does not meet the legal definition does not become "high risk profiling" because it poses a high risk to data subjects in the specific case for other reasons (and therefore requires, for example, the performance of a data protection impact assessment).

B. Linking of data

20 High-risk profiling first requires data linkage. Data linkage refers to the process of connecting, merging, or matching two or more separate data sets to gain a deeper or broader understanding. Such linkage of data can be accomplished in a variety of ways, such as by merging data from different sources that relate to the same individual or by linking data based on common characteristics, criteria, or variables.

21 Linking of data replaces the former legal expression "compilation of data" and thus expresses that profiling is not about a mere collection of data, but about a targeted linking of different data sets. A mere collection of data, possibly also for the preparation of a profiling, does not yet constitute such a linkage. Unlike the previous personality profile, a static collection of data is not sufficient.

C. Assessment of essential aspects of personality

22 While findings about any aspects of personality are sufficient for normal profiling, they must relate to essential aspects of personality for high-risk profiling. It is not required that such essential personality traits actually be assessed. It is sufficient if statements about essential aspects of the personality are basically possible ("permitted") on the basis of the processed data and the manner of the processing procedure. It is then not relevant that Art. 5 lit. g FADP uses the term "assessment" instead of "evaluate". The two terms are to be understood synonymously.

23 According to the will of the legislator, the "Moneyhouse" case law of the Federal Administrative Court on personality profiles should continue to be the guideline for determining when an evaluation of essential aspects of the personality exists. Thus, the decisive factor is whether the linked information is

condensed into a comprehensive picture of the person concerned. Essential criteria here are the amount and type of data used, the context of their use, and the temporal dimension, i.e. whether personal data are collected over a longer period of time and thus provide a quasi biographical picture by showing a development of the person concerned. In this context, even trivial data taken on its own can, through systematic linking, provide an overall picture of the person, if necessary, and convey potentially sensitive information about his or her identity, activities or preferences.

D. The need for a case-by-case approach

As with personality profiling to date, high-risk profiling remains elusive overall. The two conceptual elements of data linkage and the assessment of essential personality aspects provide a basic framework, but are unable to give the concept clear contours and require classification on a case-by-case basis. The fact that it ultimately comes down to a case-by-case consideration has also been recognized by the Federal Administrative Court in its case law on personality profiles. In a sense, "you know it when you see it." 24

High-risk profiling would be assumed in the example of the book trade, for example, if data on reading behavior were combined with food purchasing behavior and possibly other transaction data, as well as with data from fitness tracking apps, for example, in order to draw conclusions about health status and to provide data subjects with advertising for corresponding health offers or even to calculate individual insurance premiums. It would also qualify as high-risk profiling if reading behavior were linked with data on surfing behavior and geolocation data in order to obtain information on ideological views or religious beliefs. High-risk profiling would also be assumed if reading behavior were linked with credit card data and information from professional networking platforms in order to derive findings on assets and the ability to pay and, based on this, to decide which products and services are offered to the data subjects, how and at what prices. 25

IV. LEGAL CONSEQUENCES

A. Normal Profiling

Normal profiling, i.e., profiling without "high risk," is generally relevant under the FADP only for federal bodies (although private parties entrusted with pub- 26

lic duties are also considered federal bodies). First, there is only a sufficient legal basis for profiling by a federal body if the profiling is provided for in a law in the formal sense (Art. 34 para. 2 lit. b FADP). If there is no such basis in a law in the formal sense and the profiling is based on consent, this consent is, on the other hand, only valid if it is explicit, i.e. if it refers to the profiling as such (Art. 6 para. 7 lit. c FADP).

27 In contrast, normal profiling has no special legal consequences for private data controllers and the usual rules apply. In particular, profiling must be made sufficiently transparent and data subjects must be informed about the categories of data created by means of profiling (e.g., preference data) (Art. 19 para. 3 FADP). However, profiling itself does not have to be specifically mentioned or described in the privacy statement. Only if essential decisions are fully automated on the basis of profiling are there special information and disclosure obligations for this (Art. 21 and Art. 25 para. 2 lit. f FADP).

28 Like any other data processing, profiling may also require the performance of a data protection impact assessment if it is associated with high risks for the data subjects. Whether there are high risks must be determined in each individual case on the basis of the specific circumstances and may also be the case if profiling does not qualify as "high risk" profiling pursuant to Art. 5 lit. g FADP due to the lack of existing conceptual elements.

29 Also in the case of profiling, consent is only required if there is a violation of the processing principles and there is no other justification for the data processing. Profiling is no different from "normal" data processing in this respect. The much-discussed consent requirement for profiling, which was still included in the preliminary draft, did not survive the legislative process.

30 The DSGVO also hardly provides for specific legal consequences in the case of profiling, or only if profiling is carried out in connection with an automated individual decision. Without reference to automated decision-making, profiling is only mentioned in Art. 21 para. 1 and 2 DSGVO, but only by way of example, since profiling would be covered by the right of objection like any other type of processing even without specific mention. It should also be noted that within the scope of application of the DSGVO, any data processing and thus also any profiling must be based on a legal basis. However, the available legal bases are not limited and all possible legal bases of Art. 6 para. 1 DSGVO are also available for profiling.

B. High-risk profiling

The intensity with which debates on high-risk profiling have been conducted contrasts with the low legal relevance of this legal figure. The new FADP provides for only three legal consequences attached to high-risk profiling. 31

First, any high-risk profiling must be subject to a mandatory data protection impact assessment, which systematically evaluates the risks to data subjects and, if necessary, defines remedial measures. It is true that Art. 22 para. 2 FADP does not explicitly mention high-risk profiling as a trigger for the obligation to conduct a data protection impact assessment. However, high-risk profiling is by definition a high risk for data subjects, and according to Art. 22 para. 1 FADP, a data protection impact assessment is mandatory for any processing with such a high risk. However, the "high risk" refers only to the initial risk that triggers the performance of a data protection impact assessment. As part of this assessment, the controller may conclude that the actual risk in the specific case is either not high or, after taking planned remedial measures into account, is no longer to be classified as high. In such a constellation, profiling remains "high-risk profiling" according to the legal definition, but must subsequently be treated as data processing without high risk. 32

Second, consent granted in connection with profiling must be explicit pursuant to Art. 6 para. 7 lit. b FADP if private controllers carry out high-risk profiling and they base this profiling on consent in the first place. Art. 6 para. 7 lit. b FADP sets forth requirements for the granting of valid consent, but does not establish a general consent requirement for high-risk profiling. Like normal profiling, high-risk profiling requires consent only if a processing principle is violated and no other justification exists. 33

Third, and finally, the overriding interest in credit checks falls out of consideration if the check is based on high-risk profiling (Art. 31 para. 2 lit. c no. 1 FADP). 34

As explained, the DSGVO does not recognize high-risk profiling, but provides for some specific legal consequences if the profiling is related to a fully automated decision that has legal effects on the data subject or similarly significantly affects him or her. Among other things, in such qualified constellations, the DSGVO also requires that a data protection impact assessment is mandatory (Art. 35 para. 3 lit. a DSGVO). Since decisions of such great significance are rarely made in corporate practice, the threshold for the mandatory perfor- 35

mance of a data protection impact assessment in the case of profiling is rather higher under the DSGVO than under the Swiss FADP. The DSGVO contains sporadic additional legal consequences for profiling that is carried out in combination with an automated individual decision, including an extended obligation to provide information and disclosure, which also includes information on the logic involved and the effects for the data subjects.

V. PRACTICE NOTES

36 In corporate practice, the identification of high-risk profiling is particularly significant, since in the case of private controllers, special legal consequences are only attached to such profiling operations, first and foremost the obligation to conduct a data protection impact assessment. However, as seen, whether or not the threshold for high-risk profiling has been reached is highly dependent on the specific circumstances of the profiling in the individual case. It is therefore not easy to operationalize the concept of high-risk profiling and to define general criteria. In addition, profiling activities that do not qualify as "high-risk profiling" according to the legal definition may also entail a high risk in individual cases and may therefore require a data protection impact assessment.

37 There is much to be said for not applying too detailed criteria when checking whether a data protection impact assessment must be carried out (so-called threshold analysis). It is more effective to generally integrate the assessment of personal aspects as a risk factor in the review and project approval processes and, in a second step, to check on the basis of the specific circumstances whether there is either high-risk profiling according to the legal definition or profiling that entails a high risk for data subjects for other reasons. From a practical point of view, it is always advisable to conduct a data protection impact assessment if profiling reaches a certain intensity or if data from different sources are linked for this purpose.

38 Profiling also has implications for the design and implementation of data protection control processes. Profiling is particularly relevant for the implementation of information processes: both the personal data used in profiling ("input") and the new data and findings created with the help of profiling ("output") should be part of the information provided to data subjects in a suitable and comprehensible manner. The categories of data processed or newly created in connection with profiling, as well as the processing purposes pursued

with profiling, must then be described in the privacy statement. Profiling itself, on the other hand, does not have to be specifically mentioned in the privacy statement. However, an explanation of profiling may be advisable as a confidence-building measure in the interest of transparency. Data processing in connection with profiling must be documented with the required information in the processing directory pursuant to Art. 12 FADP.

Finally, it is good practice to provide possibilities for data subjects to object to profiling. In practice, such opt-out options can be implemented, for example, through technical functionalities with which data subjects can independently switch off or prevent data processing or services that are connected with profiling - e.g., the receipt of personalized direct marketing measures. Such opt-out options operationalize the general right of objection of Art. 30 para. 2 lit. b FADP and also take into account the idea of "privacy by design". Such opt-out options also increasingly meet the expectations of customers to be able to influence the processing of their data in a relevant way. 39

BIBLIOGRAPHY

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).

MATERIALS

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).

COMMENTARY ON

Art. 6 para. 3-5 FADP

A commentary by Caroline Gaul

SUGGESTED CITATION

Caroline Gaul, Commentary of art. 6 para. 3-5 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Gaul, Art. 6 para. 3-5 FADP N. XXX.

Art. 6 Principles

[...]

[3] Personal data may only be collected for a specific purpose that the data subject can recognise; personal data may only be further processed in a manner that is compatible with this purpose.

[4] They shall be destroyed or anonymised as soon as they are no longer required for the purpose of processing.

[5] Any person who processes personal data must satisfy themselves that the data are accurate. They must take all appropriate measures to correct, delete or destroy data that are incorrect or incomplete insofar as the purpose for which they are collected or processed is concerned. The appropriateness of the measures depends in particular on the form

and the extent of the processing and on the risk that the processing poses to the data subject's personality or fundamental rights.

CONTENT

IN A NUTSHELL

The provisions of Art. 6 para. 3 FADP (**purpose limitation and transparency**), Art. 6 para. 4 FADP (**time limitation of data processing**) and Art. 6 para. 5 FADP (**accuracy**) are among the so-called **processing principles**, the most important substantive principles of data protection law. They are essential for the specific design of data processing.

A violation of the processing principles constitutes an infringement of the personal rights of the data subjects. However, the infringement of privacy can be justified by consent, an overriding private or public interest or by law in the case of private data processors. This significant difference to the EU DSGVO, in which every data processing requires a specific legal basis, was also maintained in the new FADP.

Unlike under the EU's DSGVO, a violation of the processing principles discussed here is not subject to a fine under the FADP, but it can have far-reaching consequences, especially in view of the expanded powers of the Federal Data Protection Commissioner (FDPIC) under the new FADP. The Federal Data Protection and Information Commissioner can order that data processing be partially or completely adjusted, interrupted or even terminated, and that personal data be partially or completely destroyed. In addition, possible (civil) legal claims by the persons concerned and, in particular, the consequences of a **loss of trust** and **reputational damage** should be taken into account.

I. GENERAL

A. Preliminary remarks

1 The provisions of Art. 6 para. 3 FADP (**purpose limitation and transparency**), Art. 6 para. 4 FADP (**temporal limitation of data processing**) and Art. 6 para. 5 FADP (**accuracy**) belong together with Art. 6 As. 1 FADP (lawfulness), Art. 6 para. 2 (proportionality and good faith), and Art. 8 FADP (data security) are among the so-called **processing principles**, the most important substantive principles of data protection and the actual guiding principles of the law. Articles 6 para. 6 and para. 7 FADP (consent) are not processing principles, but merely explain the conditions for consent.

The processing principles of the FADP apply to private data processors as well as to federal bodies. A violation of the processing principles constitutes a **violation of privacy**. However, not every violation of privacy is unlawful in the case of private data processors. Rather, it may be justified by the consent of the data subject, by an overriding private or public interest or by law (Art. 31 para. 1 FADP). This significant difference to the EU DSGVO, in which every data processing requires a justification (prohibition with permission reservation), was maintained in the course of the revision of the FADP. Thus, according to Swiss data protection law, a legal basis for private data processing is only required if an infringement of privacy has occurred. In contrast to data processing by private individuals, Swiss data protection law still requires a legal basis for data processing by federal authorities (prohibition with reservation of permission). Even if and to the extent that such a basis exists, the processing principles also apply. They constitute directly applicable behavioral rules, and the data subject can take legal action against any violation of them. Whether and to what extent federal authorities are exceptionally exempt from compliance with the processing principles must be determined on the basis of the legal basis. 2

The data processing principles apply to the entire life cycle of data processing, regardless of the means and procedures applied, and are therefore **technology-neutral**, i.e. designed without reference to specific technical or commercial applications. 3

B. Background and purpose of the standard

The Swiss legislature has always emphasized that Swiss data protection law is not intended to prevent or restrict the possibilities for development in the field of information technology. Rather, the aim is to develop a coherent and **forward-looking data policy** in Switzerland. In this context, the FDPIC has expressly stated that, even under the new data protection law, potentially high processing risks do not represent a deal-breaker for digital transformation projects. However, certain **guard rails** must be observed. In addition to the other processing principles, these include the principle of purpose limitation (Art. 6 para. 3 FADP), the provisions on the duration of data processing (Art. 6 para. 4 FADP) and the requirements for the accuracy of data (Art. 6 para. 5 FADP). In particular, in view of the rapid and dynamic development of infor- 4

mation technology, compliance with these processing principles is intended to prevent excessive, improper or inaccurate data processing.

C. Addressee of the duties

5 The obligations arising from the processing principles apply primarily to the **data controller** (Art. 5 let. j FADP). The processor processes personal data only on behalf of the controller (Art. 5 let. k FADP) and can rely on the same grounds for justification as the controller (Art. 9 para. 4 FADP).

6 The processor is not expressly listed as such as the addressee of the processing principles of Art. 6 FADP; this is otherwise the case with the (punishable) data security processing principle (Art. 8 FADP, Art. 61 let. c FADP) and with further obligations under the FADP, e.g. Art. 12 para. 1 FADP, Art. 17 para. 2 FADP and Chapter 3 of the FADP, which explicitly place the controller and/or the processor under an obligation.

D. Legal and economic consequences of a breach

7 The provisions of Art. 6 para. 3 FADP (purpose limitation and transparency), Art. 6 para. 4 FADP (time limitation on data processing) and Art. 6 para. 5 FADP (accuracy) are not listed in the exhaustive catalog of criminal offenses (Art. 60 ff. FADP). A violation of these processing principles is not punishable under the FADP even if it is not justified. Despite a comprehensive revision of the penal provisions in the course of the revision of the FADP, nothing has been changed. However, there is a risk of criminal liability for violating other obligations that are related to these processing principles, for example the obligation to provide information, Art. 19, 21 in conjunction with Art. 60 para. 1 let. b FADP. Offenses outside the FADP may also come into consideration.

8 The further **powers of the FDPIC** under the new Data Protection Act are of considerable importance. These may, for example, lead to a **ban on processing activities** or an order to **destroy data** in the event of a violation of data protection regulations. In this context, the FDPIC has already announced in his 2022/2023 activity report that he will intensify his supervisory activities and increase the number of investigations.

9 In addition, a violation can trigger legal claims under the FADP (in particular under Art. 32 FADP and Art. 41 FADP) as well as civil claims for violation of personality rights (Art. 32 para. 2 FADP).

Apart from the potential legal consequences of violating the processing principles, in practice particular consideration must be given to the possible **loss of trust** and **reputational damage** that can result from violating the processing principles and can have a long-term negative impact on business development. 10

E. History of the individual processing principles

1. Principle of purpose limitation and transparency, Art. 6 para. 3 FADP

Article 6 paragraph 3 FADP combines the principles of purpose limitation and transparency, which were contained in two separate paragraphs in the aDSG (Article 4 paragraph 3 aDSG and Article 4 paragraph 4 aDSG). The new wording is intended to bring the text closer to Art. 5 para. 4 let. b of Convention 108 plus, in that personal data may only be processed for a "specific" and "recognizable" purpose for the data subjects. The wording that the data may only be processed in a manner that is "compatible" with this purpose is also new. In terms of terminology, the provision is thus closer to Art. 5 para. 1 let. b DSGVO. In terms of content, however, this does not result in any substantive changes compared to the aDSG. 11

2. Time limitation for data processing, Art. 6 para. 4 FADP

Art. 6 para. 4 FADP has introduced a new and explicit obligation to destroy or anonymize personal data as soon as it is no longer required for the purpose of processing. This corresponds to the requirements of Convention 108 plus and Article 4 para. 1 let. e of Directive (EU) 2016/680 and Article 5 para. 1 let. e DSGVO ("storage limitation"). This obligation is also not new. It was previously based on the general principle of proportionality (Art. 4 para. 2 aFADP, Art. 6 para. 2 FADP). By explicitly including it in the law, the legislator wanted to emphasize the particular importance of limiting the processing of personal data over time, which is becoming increasingly important in the context of technological development and almost unlimited storage options. 12

3. Principle of accuracy, Art. 6 para. 5 FADP

While the principle of data accuracy was previously emphasized in a separate article (Art. 5 aDSG), it has now been integrated into Article 6 FADP as paragraph 5 in order to combine the most important data protection principles in 13

a single article. The model for this structure was Article 5 of Convention 108 plus, Article 4 of Directive (EU) 2016/680 and Article 5 of the DSGVO. The right of rectification previously contained in Article 5, para. 2 aDSG is now regulated in Article 32 FADP.

II. SUBJECT MATTER OF THE PROVISIONS

A. Principle of purpose limitation and transparency, Art. 6 para. 3 FADP

1. Requirements

14 According to the principle of purpose limitation and transparency, personal data may only be collected for a specific purpose that is recognizable to the data subject. They may only be processed in a manner that is compatible with this purpose, Art. 6 para. 3 FADP.

15 According to the new wording of the law, identity of purpose is explicitly no longer required. The processing must merely be *consistent* with the initial purpose. Further processing for other purposes is only permitted if it is not unexpected and cannot be considered inappropriate or objectionable.

16 In a judgment of March 18, 2021, the Federal Supreme Court had already qualified the principle of purpose limitation in a case concerning the disclosure of personal data by a federal body, and held that absolute purpose identity cannot be required, as otherwise the administrative assistance provided for in Art. 19 para. 1 aFADP would be too restricted. In any case, however, the purpose of the administrative assistance must at least be *compatible with* the purpose of the original collection of personal data. Under the aDSG, the Federal Supreme Court had already ruled that "compatibility" of the processing with the original purpose was sufficient.

17 The further requirement of recognizability must be met with regard to both the collection of the personal data and the purpose of its processing. It can be considered to have been fulfilled if the circumstances clearly show that the data has been obtained and that the purpose of its processing is clear or if the processing is provided for by law. This possibility still exists even if the terms "evident from the circumstances" and "or provided for by law" from Art. 4 para. 3 aDSG were not adopted in the wording of Art. 6 para. 3 FADP.

The requirements for recognizability are to be determined in the individual case, taking into account the principles of proportionality and in good faith, Art. 6 para. 2 FADP. Vague, undefined or imprecise processing purposes are generally insufficient, although this characteristic must in turn be assessed according to the circumstances and a balance must be struck between the interests of the data subjects and those of the controller or processor and society. In the "Google Street View" case, for example, the Federal Supreme Court ruled that the principle of purpose limitation and transparency is not satisfied simply because Google's vehicles, on which cameras are installed, are visible to passers-by and residents. The purpose of these vehicles, to systematically drive along streets (etc.) and to publish the images on the internet without the consent of those affected, is not readily apparent, even though Google Street View enjoys a high level of awareness among the Swiss population. 18

The requirement of recognizability is closely related to the information requirement under Art. 19 et seq. FADP. However, it should not be confused with it. While the requirement of recognizability is a processing principle, the violation of which may be justified (Art. 31 FADP), this is not the case for the violation of the duty to provide information. Rather, a violation of the duty to provide information is punishable under Art. 60 para. 1 let. b FADP. 19

2. Examples

Further processing of addresses for **mailing advertising** violates the principle of purpose limitation and transparency if the addresses were originally collected in a completely different context, e.g. as part of a political campaign. It is also not permitted to analyze personal data relating to **consumption habits** (for purposes other than combating fraud) on the basis of payments made by credit or customer card without the consent of the data subject. The sending of unsolicited e-mail advertising to unknown and randomly composed addresses collected on the internet or the procurement by a private company of IP addresses of subscribers offering pirated copies for download also constitutes a violation of the principle of purpose limitation and transparency. 20

On the other hand, the use of an address for advertising purposes is permissible under data protection law if the data subject has provided their address with a view to obtaining a **loyalty card** or for an order (online or not) within the scope of an initially recognizable purpose. 21

22 When sending advertising newsletters, the conditions arising from the law against unfair competition must also be met, namely Art. 3 para. 1 let. o UWG ("**spam article**"). A violation of this can lead to criminal sanctions. When sending newsletters abroad, the respective **national laws** and practices must also be observed, which may result in even stricter requirements.

23 Data processing "for **future use**" in the sense of data processing without a specific purpose violates both the principles of proportionality and purpose limitation and transparency and is therefore illegal. However, the storage and retention of **peripheral data of telecommunications** without cause is still permitted in Switzerland. The police retention of recordings from the **surveillance of public places**, in which the data is collected and processed for possible criminal investigations, is also permitted, at least for a certain period of time. The Federal Supreme Court has, however, ruled differently on the (excessive) use of **radio water meters**. In this case, the purpose of storing certain data and the necessity of sending it was lacking.

24 When **disclosing data to third parties**, particular attention must be paid to whether this disclosure is still covered by the original purpose. This also applies to the exchange of data within **group companies**. In the absence of a comprehensive group privilege, companies within the same group are also considered third parties, provided that they do not merely process the data as processors. In practice, it is often difficult to distinguish between a processor and a (joint) controller. As a result, it is crucial to set up the system consistently and make it transparent. For example, in the **area of HR**, it is advisable to make the group context clear in the employment contract. When data is passed on to third parties, it must also be taken into account that (not only but also) the principle of purpose limitation must be observed by the recipient in the further processing of the data.

25 **Big data applications** such as **data warehousing** and **data mining** pose particular challenges in terms of purpose limitation and transparency because it is in the nature of big data analyses that their specific purpose only arises when the data is merged on the basis of the newly acquired findings.

26 Big data is also the most important basis for **artificial intelligence (AI)**, which thus also comes into conflict with the principle of purpose limitation and transparency. The permissibility of such applications must be examined on a case-by-case basis. Often, the subsequent processing purpose cannot yet

be defined when developing AI systems and entering training data, e.g. if the algorithm can perform a variety of tasks. In addition, training data is usually used that was originally collected for completely different purposes (e.g. when data that is freely available on the internet is used as training data). It can therefore often be questionable whether their processing is still "compatible" with the original purpose. Particular importance will be attached here to a differentiated consideration of the various data processing steps in the **AI lifecycle** (development, input of **training data**, use of the AI system's results "**output**", etc.) and to the justifications of consent, performance of a contract and legitimate interest. According to the FDPIC, manufacturers, providers and users of AI systems must also make transparent the purposes, functioning and data sources of the processing based on AI. The French supervisory authority CNIL provides specific examples of purposes according to the DSGVO by developers of AI systems:

Examples of purposes considered to be explicit and specified:

- Development of a large language model (LLM) able to answer questions, generate text according to context (emails, letters, reports, including computer code), perform translations, summaries and corrections of text, perform text classification, analysis of feelings, etc.;
- Development of a voice recognition model capable of identifying a speaker, his or her language, age, gender, etc.;
- Development of a computer vision model capable of detecting different objects such as vehicles (cars, trucks, scooters, etc.), pedestrians, street furniture (dumpsters, public benches, bicycle shelters, etc.), road signs, tricolor lights, road signs, etc.
- Conversely, the purpose would not be considered as specified enough if it only referred to the type of AI system, without mentioning the technically feasible functionalities and capabilities.

Examples of purposes that are not considered explicit and specified:

- Development of a generative AI model (possible capabilities are not defined);
- Development and improvement of an AI system (neither the type of model nor the possible capabilities are defined);
- Development of a model to identify a person's age (the type is not defined).

In this case, the CNIL also recommends, for reasons of transparency, that the controller should be able to determine in advance the foreseeable capabilities of the AI system that pose the greatest risks, that the purpose relates to the functionalities that are excluded from the outset and that the purpose defines the conditions for the use of the AI system as far as possible.

In addition, the EU's AI Act, which may also apply to Swiss companies, must be taken into account, particularly with regard to transparency requirements.

27 The potential for reusing data for **secondary uses** has also been recognized by Swiss lawmakers. On June 12, 2023, the National Council, as the second council, adopted a motion to create a **framework law for the secondary use** of data. This instructs the Federal Council to draft a law that resolves the tension between data protection and data use and is intended to create trustworthy data spaces.

28 At the European level, the Data Governance Act, the Data Act, the regulation on the European Health Data Space and, as already mentioned, the AI Act are also to be taken into account. These may also apply to Swiss companies.

3. Implementation recommendations

29 The purposes of data processing must be defined, permanently adhered to and made transparent. In practice, the latter can usually be achieved as part of the data protection declaration that is required in any case, or at least in part via general terms and conditions or by means of individual communication/notes, depending on the case. Care must be taken to ensure that vague, undefined or imprecise processing purposes are not sufficient. The degree of precision required must be determined in each individual case, taking into account the principles of proportionality and good faith. When data is passed on to third parties, a contractual agreement is often recommended that the data will only be processed for specific and lawful purposes, including an obligation to indemnify. At the very least, however, there should be a reference to the purpose limitation.

B. Time limitation for data processing, Art. 6 para. 4 FADP

1. Requirements

According to the principle of time limitation for data processing, personal data must be **destroyed or anonymized** as soon as they are no longer required for the purpose of processing. 30

Nevertheless, further data processing may be justified, Art. 31 para. 1 FADP. This is particularly the case when **retention obligations** must be fulfilled, for example the ten-year retention obligation for account books, accounting vouchers, the annual and audit reports or retention obligations under tax law. A legitimate interest in retention may also arise from potential future legal disputes and from statutes of limitation. 31

In the strictest sense, '**destroying**' means the irretrievable destruction or removal of data. In the case of data on paper, this means shredding or incinerating it and ensuring that third parties do not gain access to the 'relics'. In the case of electronic data, not only how it is stored is relevant, but also how it was obtained. If they were transmitted via a USB stick, the USB stick must be rendered unusable and all copies must be treated in such a way that the data can no longer be read. If they were transmitted by e-mail, any intermediate storage of this e-mail must also be destroyed. In addition, high demands are placed on destruction. According to the message on the FADP, standard deletion commands or simple reformatting do not constitute destruction in the sense of data protection law. 32

Destroying requires more than **deleting**. Nevertheless, the view is expressed in the literature that Art. 6 para. 4 FADP is an editorial mistake and that the principle of time limitation can also be satisfied by deletion. This is justified by an ill-considered adoption of the term “destruction” from the previous provision in Art. 5 aDSG. In addition, the terms “destruction” and “erasure” are used synonymously in the FADP. In our opinion, this can certainly be agreed to if the term “deletion”, which, incidentally, is not defined in either the FADP or the DSGVO, is understood to mean that no personal reference can be established, because then the FADP is not (no longer) applicable anyway due to the lack of personal data, Art. 5 lit. a. FADP. According to the FADP's risk-based approach, this is already the case if the personal reference could only be established with a great deal of effort that no interested party 33

would undertake. Whether this can also be affirmed in the context of **archiving**, for example, must be examined on a case-by-case basis. Organizational measures, such as access blocks and the four-eyes principle, can also be considered sufficient measures.

34 The principle of time limitation can also be satisfied by means of **anonymization**. Anonymization refers to any measure that ensures that the identity of the data subjects can no longer be determined or can only be determined with extraordinary effort. Anonymization should not be confused with **pseudonymization**. Pseudonymization is the replacement of names and other identifying features with another identifier, such as a placeholder, with the aim of preventing or hindering the identification of the data subject. In other words, pseudonymization can be used to restore the personal reference with the associated key. However, this only applies to the person who holds the key. This **relative approach** means that personal data is also not available to anyone who does not hold the key and for whom obtaining the key is practically impossible. This relative approach has a significant impact in practice because it removes the data from the scope of data protection law for anyone who does not have the key.

2. Implementation recommendations

35 The obligation to destroy or anonymize data can pose major challenges for data controllers in practice. As a first step, it is recommended to gain an overview of the usual data processing in the respective business areas. The respective retention and deletion periods should then be defined. In practice, this is done in clear lists, which are also designed as internal guidelines ("Retention Policy"/"Data Retention Policy").

36 It is helpful for implementation if the software used for data processing already offers corresponding functionalities for automated deletion. In this case, it should be ensured that these functionalities meet the requirements of data protection law from a technical point of view and that the obligation to delete data is also sufficiently covered by contract in the context of data processing agreements with the IT/cloud provider.

C. Principle of accuracy, Art. 6 para. 5 FADP

1. Accuracy of data

a. Requirements

Personal data is accurate if it properly reflects the circumstances and facts re- 37
lated to the data subject. It must be accurate in the overall context, taking into account the purpose and the type of processing. It follows that the concept of accuracy in data protection law is not to be understood in absolute terms, but that the specific application is of considerable importance.

Even correct personal data may be incorrect in the overall context and in 38
consideration of the purpose of the processing in the sense of data protection law, for example if a person is stored in a data collection on creditworthiness as a "person subject to debt enforcement proceedings" although they have paid their bills correctly and on time for years and debt enforcement proceedings have only been initiated because the bill was sent to the wrong address. On the other hand, incorrect statements do not necessarily have to be inaccurate in the sense of data protection law. According to a judgment of the Federal Supreme Court, individual pieces of information cannot be considered incorrect if the totality of the information correctly reflects the actual circumstances. Also, information in the sense of "snapshots" may well have been correct even if it subsequently becomes inaccurate, for example if a judgment still lists a name that has since been changed. In this case, the purpose for which the data is still being used is crucial. In this context, the principle of accuracy must be considered in a differentiated way, especially in the work of archives, museums, libraries and other cultural heritage institutions. Since the task of such institutions is to collect, make accessible, preserve and communicate documents of all kinds, these must not be changed, as this would run counter to the purpose of archiving. Archives allow a snapshot of the past with the help of documents, the "correctness" of which refers solely to the fact that the documents in question are reproduced accurately, regardless of whether this is still considered accurate from a current perspective. Similarly, the claim to correctness in the case of police checks does not refer to the objectively ascertainable information about the persons concerned, but to the authenticity of the protocol. What matters is whether the data available reflects the sub-

jective observation of the authorized person at the time the assessment is made.

39 In principle, the accuracy of data can only relate to **factual information** that can also be determined objectively. **Value judgments** are subjective and can hardly be classified as right or wrong. It is difficult to draw the line when value judgments and facts are mixed up. This has gained particular relevance in the context of 'fake news'. However, the information that a value judgment was expressed by a certain person or documented in a file, for example, can be correct or false. Similarly, the information as to whom the value judgment refers can also be correct or false. The further use of the fact of the value judgment is also governed by the general processing principles.

40 Adhering to the principle of data accuracy in relation to **AI systems** presents particular challenges. Especially in the case of AI systems where the **training data** is obtained from publicly accessible sources, in particular the internet, it is often impossible to effectively verify the accuracy of the data. The results of AI systems' data processing ('**output**') may also be inaccurate. On the one hand, it cannot be assumed that 'statistical accuracy' is generally sufficient for data processing in connection with AI systems. On the other hand, however, data processing in relation to AI systems must not be subject to higher requirements than other data processing, since the FADP is designed to be fundamentally technology-neutral. This means that the question of data accuracy must also be assessed on a case-by-case basis and taking into account the overall context when data is processed using AI systems. The purpose of the data processing, the significance of the output and the expectations of the users are particularly relevant in this context. In practice, it will be crucial here to provide users with appropriate information. The associated requirement to check the output should also be reflected in companies' "**AI guidelines**".

41 In general, processing inaccurate data is not per se a violation of privacy. Only if the incorrect data processed in this way results in a violation of privacy must it be corrected or destroyed. The principle of accuracy is not absolute either. A violation may be justified in the case of private data processors under Art. 31 FADP. In the case of federal bodies, the right to erasure may also be restricted (see Art. 41 paras. 3-5 FADP).

b. Examples

When processing **suspicious information** about the commission of possible criminal offenses, Art. 6 para. 5 FADP does not preclude such processing as long as the significance of the corresponding information is known and the suspicion does not appear as certain knowledge. **Archived e-mails** that, according to current knowledge, contain false information are nevertheless correct in terms of data protection law, provided that they are not processed on the assumption that they are still current. Similarly, the storage of **business correspondence** is permissible within the scope of the storage obligation, even if it contains false information. If a house number is incorrectly recorded in an association's address database, but the address database is not used for postal delivery and only to check the membership list, the information does not need to be corrected. In any case, however, compliance with the other general processing principles must also be checked for such data processing, in particular the principles of proportionality and purpose limitation. 42

2. Duty to verify, correct and delete

a. Requirements

According to the principle of accuracy, every person who processes personal data must ensure its accuracy, Art. 6 para. 5 p. 1 FADP. Art. 6 para. 5 p. 2 FADP also now explicitly states that all appropriate measures must be taken to correct, delete or destroy inaccurate data. This obligation supplements the duty of verification, which would otherwise make no sense. The extent of the duty of verification depends on the individual case. In particular, the purpose and extent of the processing, the type of data being processed, the extent of the data disclosure and the sensitivity of the data must be taken into account. The data processor's duty of verification must also be within this framework. The higher the risk of a violation of privacy, the higher the requirements for the duty of verification. The duty of verification can thus also lead to an **updating obligation**. However, it does not include a general duty to carry out regular checks without cause. 43

The implementation of measures to ensure accuracy can also be **delegated**, for example to the data source or a processor. If the duty to ensure accuracy is violated, this constitutes a violation of the processing principles and thus a violation of privacy by law, Art. 30 para. 2 let. a FADP. However, according to 44

the spirit and purpose of the law, such a breach of duty can only trigger claims for correction and damages if the data is actually inaccurate. The measures to be taken depend, among other things, on the type, scope and purpose of the data processing, the sensitivity of the data and the risk to the data subject's privacy rights. This in turn must be determined on a case-by-case basis. In addition, legal obligations may preclude the measures of correction, deletion or updating.

b. Examples

45 If the data processing for marketing purposes is based on **information provided by the data subject**, the controller does not have to ensure the accuracy of the data. Similarly, there is no general obligation to continuously check a customer file for marketing purposes for outdated addresses. However, if a policyholder notifies the insurer of a change of address that also indicates a change of marital status, the insurer is obliged to update the marital status if this has an impact on the payment of insurance benefits. On the other hand, once information has been provided in an insurance policy, it is no longer necessary to check it, provided it has no influence on the premium or the insurance benefit. When it comes to checking the data held by credit reference agencies, particular consideration should be given to the scope of the data, the existence of personality profiles and consent, and the number of searches carried out. If an insurance company wants to use **artificial intelligence** (**AI**) to create a profile of customers who take out insurance and use this profile as a basis for their decisions when calculating the insurance risk, not only should data from existing customers from data sources with correct and up-to-date information be used as training data, but a pool of customers that is representative of the population should also be used to avoid bias.

3. Implementation recommendations

46 The requirements for the measures required under Art. 6 para. 5 FADP should be proportionate to the risks and consequences of the specific use. Examples of measures to be taken, which at the same time represent key aspects in the context of technology design according to the principles of **privacy by design** and **privacy by default**, may include:

- Checking the reliability of the data source

- Determining the degree of accuracy based on the overall circumstances of the individual case
- If necessary, re-examining the data depending on the overall circumstances and the various phases of data processing
- Reducing false positives / false negatives, e.g. to reduce errors in automated decision-making and in the use of artificial intelligence
- Updating data if it is necessary for the purpose of processing
- Implementation of "self-service" solutions where the data subjects can check their data themselves and correct it if necessary
- Introduction of plausibility checks and quality checks
- Implementation of automatic input checks, e.g. to avoid incorrect input of postcodes
- Drop-down menus instead of free text input

From the point of view of the controllers, it is also advisable to impose a contractual obligation on the data subjects to provide their data correctly and to keep it up to date, and to exclude any liability in this regard as far as possible. In principle, an obligation of indemnity should also be considered for external data sources. Depending on the case, this can be taken into account as part of an overall concept that includes the assignment of data and responsibilities, as well as other related rights and obligations.

BIBLIOGRAPHY

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).

MATERIALS

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).

COMMENTARY ON

Art. 6 Abs. 6 and 7 FADP

A commentary by Gaspare T. Loderer

SUGGESTED CITATION

Gaspare T. Loderer, Commentary of art. 6 para. 6 and 7 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Loderer, Art. 6 FADP N. XXX.

Art. 6 Principles

[...]

[6] If the consent of the data subject is required, such consent is only valid if given voluntarily for one or more specific instances of processing based on appropriate information.

[7] The consent must be explicitly given for:

a. processing sensitive personal data;

b. high-risk profiling by a private person; or

c. profiling by a federal body.

CONTENT

IN A NUTSHELL

Art. 6 para. 6 and 7 FADP stipulate the validity requirements for consent under data protection law. However, the cases in which consent is required are regulated in other provisions. The content of the new provisions on consent is essentially the same as that of Art. 4 para. 5 aDSG. It has merely been specified that consent must be given for one or more specific processing operations, which already applied previously. In the case of explicit consent, the newly introduced profiling has replaced the old legal personality profile. Otherwise, however, there should be no change to the legal situation. If consent is required, it must therefore still be given voluntarily for one or more specific processing operations after appropriate information has been provided. If consent is required for the processing of particularly sensitive personal data, for high-risk profiling by a private individual or for profiling by a federal body, this must also be explicit. However, even in these cases, there is no general requirement for consent, although some argue otherwise. Within the scope of application of the FADP, consent is used more frequently as the legal basis for processing due to the different concept (principle of prohibition with reservation of permission) and the requirements for valid consent are higher overall than under the FADP.

I. GENERAL INFORMATION

A. History of origin

The content of Art. 6 para. 6 and para. 7 FADP essentially corresponds to Art. 4 para. 5 aDSG, although some editorial changes were made as part of the total revision. Explicit consent has been separated from "ordinary" consent and regulated in a separate paragraph. It was also clarified that consent must relate to one or more specific processing operations. This clarification was made with a view to aligning with the revised ETS 108 Convention, but does not result in any change to the legal situation. As the term "personality profile" was also replaced by "profiling" as part of the total revision, consent for high-risk profiling by private individuals and profiling by federal bodies must now be given explicitly. 1

2 The new criterion of unambiguous consent introduced in the draft was dropped during parliamentary deliberations. This had also originally been added with a view to approximating the revised ETS 108 Convention.

B. System and delimitation

3 The Swiss Data Protection Act is based on the principle of permission with reservation of prohibition. Accordingly, processing is generally permitted provided that the processing principles of Art. 6 and data security pursuant to Art. 8 FADP are complied with, personal data is not processed contrary to the express consent of the data subject or personal data requiring special protection is disclosed to third parties (Art. 30 para. 2 FADP). Otherwise, there is a violation of personality rights, which can be justified, among other things, by the consent of the data subject (Art. 31 para. 1 FADP).

4 Art. 6 para. 6 and 7 FADP therefore do not stipulate a general requirement for consent, but only define the conditions under which consent is valid. Whether and for which cases consent is required, however, is regulated elsewhere. Accordingly, consent is not required per se for the cases set out in Art. 6 para. 7 FADP (processing of particularly sensitive personal data, high-risk profiling by a private individual and profiling by a federal body), even if some argue otherwise.

5 Despite the systematic position of the provisions on consent under Art. 6 FADP with the title "Principles", the validity requirements for consent are not a processing principle under data protection law. In particular, there is no violation of personality rights if the requirements for consent are not met, although Art. 30 para. 2 lit. a FADP refers to the "principles" of Art. 6 FADP. For this reason, it would have been better to move the provisions on consent to the definitions in Art. 5 FADP.

C. Scope of application

6 For private individuals, consent may in particular justify a violation of personality rights (Art. 31 para. 1 FADP). In addition, consent may be relevant for private individuals in the following cases: For the disclosure of personal data abroad in derogation of Art. 16 para. 1 and 2 FADP (Art. 17 para. 1 lit. a FADP); for automated individual decisions without having to comply with the requirements of Art. 21 para. 1 and 2 FADP (Art. 21 para. 3 lit. b FADP); in the

context of the right to information for the communication of health data by a health professional (Art. 25 para. 3 FADP).

For federal bodies, consent may replace the general requirement of a legal basis in individual cases (Art. 34 para. 4 lit. b FADP), including for the disclosure of personal data abroad (Art. 36 para. 2 lit. b FADP). 7

In addition, consent is also mentioned elsewhere in the FADP and may also be provided for in special legislation. Whether and to what extent the requirements of the FADP apply here has not been fully clarified, particularly in the intersection with the ban on spam pursuant to Art. 3 para. 1 lit. o UCA. However, this is at least implicitly assumed. 8

D. Comparison with the DSGVO

The Swiss concept differs fundamentally from the reverse concept of the DSGVO. There, the principle of prohibition with reservation of permission applies, according to which any processing of personal data is prohibited unless there is a legal basis for the processing (Art. 6 DSGVO). One of these possible legal bases is consent (Art. 6 para. 1 lit. a DSGVO). Its requirements are generally described in more detail in Art. 4 No. 11 and Art. 7 DSGVO, with regard to the consent of children in Art. 8 DSGVO and for the processing of special categories of personal data, consent must be given expressly (Art. 9 para. 2 lit. a DSGVO). 9

The requirements for valid consent under the DSGVO are stricter than those under the FADP. Consent that is valid under the FADP therefore generally meets the requirements of the FADP, while consent that is valid under the FADP does not necessarily meet the stricter requirements of the GDPR. 10

II. REQUIREMENTS FOR CONSENT (ART. 6 PARA. 6 FADP)

A. General information

Consent is subject to the general "limits" of personal rights, which include the provisions of Art. 16 et seq. CC (capacity of judgment) and Art. 27 CC (excessive commitment). Consent is to be qualified as a unilateral legal transaction, which is why the CO applies in particular to the interpretation of consent (principle of trust), the limitations of Art. 19 and 20 CO and defects of will (Art. 23 et seq. CO). 11

B. Capacity of judgment

12 The granting of consent under data protection law constitutes the exercise of a highly personal right and can therefore be exercised independently by persons lacking capacity (Art. 19c para. 1 CC). However, persons lacking capacity are generally represented by their legal representative (Art. 19c para. 2 CC). Parents can give consent for children lacking capacity within the scope of their legal representation and to the extent of the parental care to which they are entitled (Art. 304 CC).

13 A person is capable of judgment if they do not lack the capacity to act rationally due to certain conditions (infancy, mental disability, mental disorder, intoxication or similar) (Art. 16 CC). As a rule of thumb, the capacity of minors aged 13 and over is to be assumed. Due to the relative nature of the capacity of judgment, the requirements are to be set higher, for example, in the case of complex processing, sensitive personal data and serious interventions in the personality.

C. Timing

14 Consent must generally be given prior to data processing, which may, for example, be prior to data collection or disclosure (see Art. 5 lit. d FADP). If consent is required and has not been given, the corresponding data processing is unlawful.

15 Subsequent consent in the strict sense is excluded. However, subsequent consent can be considered, which is to be interpreted as a waiver of the assertion of claims. However, data processing is unlawful until the time of subsequent consent. In addition, subsequent authorization only extends to data processing about which appropriate information was initially or subsequently provided.

D. One or more specific processing operations

16 The criterion that consent must relate to one or more specific processing operations was added with the total revision. This brings the wording into line with Art. 5 para. 2 of the revised ETS 108, but without changing the legal situation.

As under the old law, it is necessary that the processing is sufficiently defined, in particular with regard to scope and purpose. The data subject should be able to understand for which processing they are giving their consent. The specific scope of the consent results from the declaration of consent and the appropriate information. Without further information, general descriptions of purposes such as "improving the user's experience", "advertising purposes", "IT security purposes" or "future research" are inadequate. The processing can be limited or unlimited in time. In some cases, however, consent is required on a case-by-case basis. 17

Consent to several processing operations does not require that they all have the same purpose; consent can also be given for different processing operations. In addition, a processing purpose such as medical treatment by a doctor may require different processing operations, e.g. the exchange of particularly sensitive personal data with other specialists or insurance companies and processing for billing purposes. 18

The extent to which general consent is permissible is controversial. In any case, the limits of consent must be clear and, based on the principle of proportionality, the more sensitive the nature and scope of the processing, the clearer it must be. Unlimited declarations of consent for any purpose, for any processing or for all categories of personal data by unlimited processors are therefore inadmissible. On the other hand, it is permissible, for example, to authorize the previous employer to generally provide information to potential employers, which requires express consent in the case of the disclosure of particularly sensitive personal data (such as information on absences due to illness). 19

E. Adequate information

Consent under data protection law is based on the "informed patient's consent", meaning that all information must be provided in the specific case so that the data subject can make a free decision. In other words, it is important that the data subject is clear about what they are consenting to, i.e. that they know the scope of their consent. The specific information to be provided was already not uniformly assessed under the old law, nor will it be under the new law. 20

21 According to the view expressed here, the requirements for appropriate information can be based on the duty to provide information pursuant to Art. 19 FADP. This is because the appropriate information required for consent can lead to an exemption from the duty to provide information pursuant to Art. 19 FADP, as the data subject already has the relevant information (Art. 20 para. 1 lit. a FADP).

22 However, this does not mean that all information under Art. 19 FADP must be provided in every case as the basis for the appropriate information under Art. 6 para. 6 FADP, even if such an integrative approach may be required in practice. According to the view expressed here, at least the following information is required for appropriate information in the context of consent:

- Identity of the controller;
- Purpose of processing;
- (categories of) personal data processed.

23 Which of this information is required and to what level of detail, and whether additional information is required, depends on the circumstances of the individual case. In application of the principle of proportionality, the more sensitive the personal data concerned, the clearer the appropriate information must be. For example, Art. 16 para. 2 HRA specifies for consent to research projects, among other things, that information must also be provided on the foreseeable risks and burdens as well as measures to protect the personal data collected. According to Art. 8 para. 1 HRA, information must also be provided on the right of refusal or withdrawal and the consequences of withdrawal, as well as in general on other content required for the decision.

24 Unlike Art. 7 para. 3 DSGVO, however, the FADP does not generally require information about the right of withdrawal and the fact that the withdrawal does not affect the lawfulness of the processing based on the consent until the withdrawal. A lack of information in this regard therefore does not invalidate any consent given.

25 The DSGVO also requires that consent can be withdrawn as easily as it was given. Based on the principle of good faith, the FDPIC has also demanded this for the aDSG. However, there is no support for this in the law and this view should therefore be rejected. On the other hand, the voluntary nature of consent may be questionable if it cannot be revoked in a reasonable manner.

26 In line with the explanations in the 2003 Dispatch, some take the view that information must be provided about the negative consequences or disadvantages of refusing consent. According to the view expressed here, this is not a necessary part of appropriate information, but depending on the adverse consequences, it may call into question the validity of consent due to the lack of voluntariness. On the other hand, information must be provided about any existing risks of data processing.

Appropriate information must always be provided by the controller. However, it is possible to obtain consent for processing by a third party. This regularly requires the third party to be named, unless this information is sufficiently clear from the circumstances, as may be the case, for example, in the case of group companies. 27

The information provided must be interpreted in accordance with the principle of trust, i.e. as the person concerned could and should have understood it. This must be based on the assumption of a person of average understanding of the group of addressees addressed. The doctrine that would like to focus instead on the abilities of the individual person concerned must therefore be rejected. 28

The appropriate information must be precise, transparent and comprehensible. It should be written in the language in which the controller provides the services on which the processing is based. The information may be provided orally or in writing; however, for reasons of proof, it is advisable to provide evidence in text form. If the information about the processing to which consent is given has to be fragmented and compiled from several places in one document, this may be an argument against the provision of adequate information. 29

It must be possible to take note of the information before consent is given. A reflection period may be appropriate depending on the sensitivity of the processing. For example, Art. 16 para. 3 HRA requires that a reasonable period of reflection be granted before the data subject consents to a research project. 30

Whether the information is actually taken note of is irrelevant. The only decisive factor is whether there was a reasonable opportunity to take note of the information. In the case of a global acceptance, i.e. the granting of consent without taking note of the information (e.g. because it can only be found in linked general terms and conditions or a privacy policy), unusual clauses do 31

not apply (unusualness rule). It may therefore be appropriate to highlight unusual aspects separately.

F. Voluntariness

32 Consent must be given voluntarily, i.e. it must be an expression of the data subject's free will. There is an interaction with the need for appropriate information. If the appropriate information is not provided, consent cannot be assumed to be voluntary. Consent is also not voluntary if it was obtained through deception, threats or coercion.

33 The FADP does not have a prohibition of linking based on Art. 7 para. 4 DSGVO, although its existence and scope under the DSGVO is disputed. Nevertheless, there are also forms of inadmissible tying of consent under Swiss law, but the hurdles are higher than under the DSGVO. In particular, consent should not be voluntary if a refusal of consent results in a disadvantage that is unrelated to the purpose of processing or is disproportionate to it. However, any other disadvantage resulting from the refusal of consent does not affect the validity of the consent.

34 Examples: Consent to a credit check for the purpose of obtaining a credit card is given voluntarily and is permissible, as without consent the disadvantage of not receiving the credit card is proportionate. The impossibility of participating in an insurance program is directly related to the data processing for which consent is obtained; and the fact that monetary benefits and cash bonuses in the maximum amount of CHF 75.00 per year are advertised for persons with basic insurance only does not call into question the voluntary nature of the consent. However, the threat of dismissal in the event of non-consent to data processing not provided for in the employment contract is deemed to be involuntary because it is disproportionate.

35 In some cases, voluntariness is only assumed if there is a reasonable alternative course of action. According to the view expressed here, apart from exceptional situations (in particular dominant market position, social or de facto dependencies), no alternative is required for the affirmation of voluntariness. Therefore, if consent is not given, the person concerned can generally be denied the use of a service.

36 The question of whether consent is voluntary is particularly controversial in the employment relationship. Some argue that the necessary voluntariness is

lacking in this context or that any data processing that goes beyond Art. 328b CO is inadmissible. Other authors merely see the scope of voluntariness as being narrower, for example in that a reasonable alternative course of action must be available to employees. The prevailing doctrine and the FDPIC consider data processing that goes beyond Art. 328b para. 1 CO to be permissible only if it is advantageous for the employees or in their interest (Art. 362 CO). Other authors also consider consent that deviates from Art. 328b CO to the detriment of employees to be valid under certain circumstances. According to the Federal Supreme Court, although data processing contrary to Art. 328b CO is unlawful, it can be based on a justification pursuant to Art. 13 aDSG. According to this view, Art. 328b CO is therefore a processing principle and not a prohibition provision. However, the brief explanations on this are criticized in the doctrine. The Federal Supreme Court has subsequently confirmed its view, but without referring to its earlier decision.

According to the view expressed here, consent in the employment relationship is not excluded per se and consent can also be given to processing that goes beyond Art. 328b para. 1 CO. The decisive factor here is whether or not appropriate information was provided and whether or not it can be assumed that consent is actually voluntary in the form of an option to refuse without adverse consequences. For example, consent can be given to the publication of photos of employees without customer contact on the Internet or even for advertising purposes, provided that information has been provided about the corresponding processing and the employee has effective freedom of choice. The position of the employee and the employee's life cycle (application, current employment relationship, termination) may be decisive for this assessment. On the other hand, a lack of voluntariness would have to be assumed in the last example mentioned in n. 34. 37

In the European context, the issue of so-called dark patterns or nudging must be considered for the question of voluntariness, especially in the area of cookie banners. According to case law and the opinion of supervisory authorities, enticing users to give their consent, e.g. through unequal color design and size of the "Accept" and "Decline" buttons or additional effort for declining (e.g. by only offering a "Decline all" button on the second display level, after clicking on "Continue"), calls voluntariness into question. Whether this development will also gain significance in Switzerland is questionable. This is because Swiss law does not generally require consent for cookies. The rele- 38

vant Art. 45c lit. b TCA only requires that users "are informed about the processing and its purpose and that they can refuse the processing." However, further developments in this regard will have to be monitored, as the FDPIC and others generally assume that tracking constitutes a justifiable violation of privacy.

39 The DSGVO requires that granular consent can be given for various processing operations. This is one reason why cookie banners that comply with European law often offer the option of consenting to each individual cookie separately. Of course, the usefulness of such granularity for cookies is debatable. After all, it is rather unlikely that a person would want to give their consent to certain individual cookies and not to others. Since such a requirement of granularity cannot be inferred from the FADP, this can only be demanded in exceptional cases.

G. Unambiguousness

40 The draft FADP still stipulated that consent must be given "unambiguously". In this regard, the dispatch states that the data subject's declaration must unequivocally indicate their will, which depends on the circumstances of the individual case, and that the more sensitive the personal data in question, the clearer the consent must be, based on the principle of proportionality.

41 However, the requirement of unambiguousness was dropped by Parliament and was therefore not included in the wording of Art. 6 para. 6 FADP. However, the fact that the dispatch refers to this criterion has apparently caused confusion among scholars.

42 The 2003 dispatch had already stated that, based on the principle of proportionality, the more sensitive the personal data in question, the clearer the consent must be. This affects the clarity of the declaration of intent, which means that there are parallels with the criterion of the "unambiguous affirmative act" found in the DSGVO. As an alternative to the "declaration", this represents the second application case of the "unequivocal expression of will" pursuant to Art. 4 No. 11 DSGVO. However, in the absence of a corresponding criterion in the FADP, unlike the DSGVO, it cannot be inferred from this that consent is inadmissible, for example by means of pre-ticked boxes. This also does not necessarily contradict the requirement of "privacy by default" pursuant to Art. 7 para. 3 FADP.

However, an interpretation of the criterion of unambiguousness in accordance with the revised ETS 108 would require consent to be "unambiguous". This requirement can relate to both the form and the content of the declaration. The message suggests that the element relates to the form. If this is the case, the legislator has taken this formal requirement into account by stating that consent by silence is generally not sufficient. Insofar as the content is to be affected, the principle that the requirements vary based on the principle of proportionality applies in any case. Thus, under Swiss law, the criterion of unambiguousness would have no independent significance. 43

H. Form

Consent can be given without form. Apart from statutory exceptions, verbal consent is therefore also possible. However, since the data processor bears the burden of proof for consent, documentable consent is the obvious choice. This relativizes, at least de facto, the fundamental freedom of form. 44

In principle, consent can also be obtained within the framework of general terms and conditions. However, if a global assumption is made in this case, the unusualness rule applies, according to which unusual consents are ineffective to the detriment of the data subject. In addition, the ambiguity rule comes into play, according to which unclear formulations are at the expense of the author in case of doubt. 45

Except in the case of the required expressiveness of Art. 6 para. 7 FADP, consent can also be given implicitly. In this case, the declaration of intent does not result from the declaration itself, but from behavior that can be understood as a clear expression of intent based on the circumstances. This is the case, for example, if the data subject makes their data accessible themselves. 46

Implied consent is often used as a synonym for tacit consent, but this should be avoided. Silence or inactivity does not generally lead to valid consent (see Art. 6 CO), unless the parties have agreed to silence as consent. 47

In exceptional cases of urgency, presumed consent is conceivable, e.g. in the case of unconscious patients. However, the significance of such consent is negligible, as in these cases a justification based on the overriding interest of the person concerned would probably apply anyway. In some cases, a distinction is made between presumed consent and hypothetical consent. According to this, consent should be valid despite the lack of adequate information, as 48

the data subject would have consented even if they had been fully informed. However, there is hardly any room for this unless the data subject subsequently consents to this in the form of a waiver of the assertion of claims.

III. EXPLICIT CONSENT (ART. 6 PARA. 7 FADP)

49 If consent is required for the processing of particularly sensitive personal data, high-risk profiling by a private individual or profiling by a federal body, this must be given expressly. This means that consent is not generally required for these processing operations either. Although statements in the parliamentary debate sometimes suggested the opposite, the wording of Art. 6 para. 7 FADP does not anticipate this in the introduction, unlike that of Art. 6 para. 6 FADP, and the FDPIC and the doctrine sometimes argue the opposite, this results from the clarification in the parliamentary consultation and the fact that no change to the legal situation should be made.

50 The criterion of expressiveness must be observed in addition to the requirements of Art. 6 para. 6 FADP. This was better expressed in Art. 4 para. 5 aDSG and in the preliminary draft of the FADP, as "normal" and explicit consent were regulated in the same paragraph and the addition "in addition" made this clear.

51 It is disputed whether the more stringent element of expressness relates only to the form or also to the content of the consent. With regard to form, express is understood to be the opposite of implied. However, written consent is not required. Based on Art. 1 CO, the question of expressiveness is determined by whether the expressed will is directly evident from the declaration of intent in the form of written or spoken words or a sign. In other words, the manner in which the will is expressed must already provide clarity about the will. Examples of explicit signs include actively ticking a box, actively selecting certain technical parameters for IT services, nodding one's head in agreement during medical treatment or opening one's mouth to remove mucous membrane from the cheek after being informed accordingly. For reasons of the burden of proof, however, documentable consent is again required.

52 According to some scholars and the FDPIC, expressiveness also refers to the content. In the case of express consent, the affirmative behavior should refer to the data processing in question and not merely to the action that only results in this data processing. Consent to receive personalized advertising

would therefore not include explicit consent to the high-risk profiling on which the advertising is based.

According to the view expressed here, the requirement of expressness refers to the form of consent and not its content. The 2003 Dispatch states: "Consent is not bound to a specific form and can be given tacitly or by implication, unless it concerns the processing of particularly sensitive data or personality profiles. In accordance with the principle of proportionality, it is already assumed that the more sensitive the personal data in question, the clearer the consent must be." For the second sentence, the dispatch refers to a literature reference that expressly understands consent as the opposite of implied consent. The historical interpretation element confirms this finding, especially as the 2017 dispatch states that there should be no deviation from the current legal situation. 53

IV. Revocation

Consent can be withdrawn at any time and without justification. However, revocation at an inopportune time may trigger liability for damages. A revocation then only has effect for the future, which means that the legality of processing that has already taken place is not affected by the revocation. However, previous data processing can be contested on the basis of a lack of consent. Data processed on the basis of consent may have to be deleted if there is no other justification for further processing in the form of continued storage. 54

According to the Federal Supreme Court, personal data that does not form part of the core area of human existence, such as name, voice or image, can be irrevocably shaped if the contractual obligation is based on economic interests. However, the extent to which these considerations of the right to one's own image can be generalized is not entirely clear. In the case under review, one of the decisive factors was that revocation was possible against payment of a moderate compensation for rescission in the form of a contractual penalty. 55

V. LEGAL CONSEQUENCES OF MISSING, INVALID OR REVOKED CONSENT

If a certain processing requires consent and this is not given (in good time) or does not meet the validity requirements, the corresponding processing is un- 56

lawful or constitutes a violation of personality rights. If processing is continued despite the withdrawal of consent, this also constitutes a violation of personality rights (Art. 30 para. 2 lit. b FADP).

57 In these cases, a controller may invoke other justifications (Art. 31 FADP) as a subsidiary basis. If, on the other hand, no other justification applies, there are claims against private controllers (Art. 32 para. 2 FADP) or federal bodies (Art. 41 FADP) and, if necessary, investigative and administrative measures are taken by the FDPIC (Art. 49 et seq. FADP).

58 A violation of Art. 6 para. 6 and 7 FADP is not directly punishable. However, indirect punishment is possible, particularly in the case of the disclosure of personal data abroad based on invalid or revoked consent, provided that the disclosure was continued based on this consent (Art. 61 lit. a in conjunction with Art. 17 para. 1 lit. a FADP). In addition, in the area of electronic mass advertising in particular, a lack of consent pursuant to Art. 3 para. 1 lit. o UCA may result in a penalty pursuant to Art. 23 UCA.

VI. PRACTICAL TIPS

59 In practice, consent is sometimes obtained for processing that does not require it. It is occasionally argued that the transparency requirement or the principle of good faith speak against obtaining consent that is not necessary. As a rule, such strictness is not appropriate because the question of the necessity of consent is often associated with legal uncertainty. However, since consent can be withdrawn at any time, alternative justifications should be examined first.

60 Formulations such as "I agree to the privacy policy", "I accept the privacy policy" or similar are often found on the internet. However, a privacy policy should only provide information unilaterally and not constitute a bilateral contract. In the case of a global takeover, the unusualness rule also has a restrictive effect. The privacy policy should therefore only be linked and consent should be obtained separately and cautiously.

VII. CRITICISM OF THE STANDARD

61 According to the dispatch on the new Data Protection Act, one of the guiding principles of the revision was to strengthen the rights of data subjects, which

was also to be achieved by more precisely defining the requirements for valid consent from the data subject. It cannot be assumed that this goal will be achieved by the clarification of the requirements for consent. On the one hand, there has been no change to the legal situation. On the other hand, declarations of consent, just like data protection declarations, are hardly ever read. This can result in "information overload" and click fatigue, especially if, in addition to a declaration of consent under data protection law, consent to general terms and conditions is obtained and the data protection declaration is brought to the user's attention.

BIBLIOGRAPHY

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).

MATERIALS

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).

COMMENTARY ON

Art. 7 FADP

A commentary by Samuel Klaus

SUGGESTED CITATION

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

Short citation: OK-Klaus, N. XXX zu Art. 7 DSG.

Art. 7 Data protection by design and data protection by default

[1] The controller is obliged to arrange the data processing in technical and organisational terms so that the data protection regulations, and in particular the principles under Article 6, are respected. It shall take account of this from the planning stage.

[2] The technical and organisational measures must in particular be appropriate with regard to the state of the art, the nature and the extent of the data processing and the risk that the processing poses to the data subject‘s personality or fundamental rights.

[3] The controller is obliged to ensure by means of suitable default settings that the processing of personal data is limited to the minimum

required for the purpose intended, unless the data subject specifies otherwise.

CONTENT

IN A NUTSHELL

Privacy by Design and Privacy by Default serve as guiding principles for the implementation of data protection. According to the principle of Privacy by Design, appropriate measures should be taken in advance, as early as the planning stage of data processing, to ensure systemic data protection. If the data subjects or users have several setting/choice options, the principle of Privacy by Default should ensure that the default setting represents the most data protection-friendly combination of setting options.

I. GENERAL

A. Preliminary remarks and background

1 The premise that data protection requirements must be implemented by means of appropriate technical measures already applied under the previous law, since the requirements of Art. 4 aDSG (principles) and Art. 7 aDSG (data security) could not otherwise be achieved. The revised Data Protection Act now explicitly expresses this in Art. 7 FADP with the two principles "Privacy by Design" (data protection by technology, Art. 7 para. 1-2 FADP) and "Privacy by Default" (data protection-friendly default settings, Art. 7 para. 3 FADP). In terms of content, Art. 7 FADP should be read in conjunction with Art. 6 FADP (principles) and Art. 8 FADP (data security): The technical and organizational measures used by Privacy by Design ("PbDesign") shall in particular enable the implementation of the principles according to Art. 6 FADP, and the guarantee of data security (Art. 8 FADP) represents - among others - one of the relevant focal points. An important sub-aspect of PbDesign is also specifically mentioned in Art. 7 para. 3 FADP with the principle of "Privacy by Default ("PbDefault").

2 The normative purpose of Art. 7 FADP is strongly programmatic and thus difficult to grasp in concrete implementation: The intention behind PbDesign is to create the systemic conditions for fulfilling and (permanently) guaranteeing data protection. It remains to be seen whether this is expedient in view of the limited circle of addressees (cf. Section B below).

3 In terms of legal dogma, the introduction of PbDesign and PbDefault goes back to Art. 10 para. 2-4 of ER-Conv 108+, which will be ratified when the re-

vised FADP enters into force. For federal bodies, PbDesign and PbDefault have already been prescribed in the scope of the SDSG since March 1, 2019 (Art. 5 SDSG). The SDSG will be repealed when the revised FADP enters into force, and the obligation to PbDesign and PbDefault will then be regulated for all addressees in the FADP. Art. 7 FADP implements the requirements of Art. 10 para. 2-4 of ER-Conv 108+ (cf. Art. 4 para. 1 of ER-Conv 108+), in a similar but not identical manner as is done in Art. 25 DSGVO for EU Member States.

Art. 25 DSGVO (data protection through technological design and through data protection-friendly default settings) thus implements the same general requirements, using the same terms and with the same thrust - but against the slightly different background of the DSGVO systematics. When applying, interpreting and implementing Art. 7 FADP, the literature and case law on Art. 25 FADP can thus be helpful, although certain differences must be taken into account: In particular, the different starting position with regard to data processing (prohibition principle with reservation of permission under the DSGVO versus basically permitted data processing with restrictions and possibility of justification under the FADP) must be taken into account in the analogous application of guidelines developed for the implementation of Art. 25 FADP. It remains to be seen whether, over time, the implementation of the principles of PbDesign and PbDefault under the FADP will differ significantly from those under the DSGVO. From a pragmatic point of view, this would be avoided in favor of applying these fundamental principles as uniformly as possible. 4

B. Addressee

The addressees of the requirements of Art. 7 FADP are the data controllers, whereby both private individuals and federal bodies are addressed. However, contract processors, upstream service providers or manufacturers are not covered: The basic idea and purpose of PbDesign should also cover in particular the planners, manufacturers and distributors of systems, applications and other tools used for data processing. However, these are not covered by the scope of application of Art. 7 FADP or are only indirectly covered by the obligation of data controllers. 5

While data controllers are thus directly obligated to implement the requirements of Art. 7 FADP, the basic idea of "systemic data protection" is implemented only indirectly with respect to the actors upstream in the value chain: According to Art. 7 FADP, data controllers are obliged to take appropriate 6

measures to ensure that upstream services and products are designed in such a way that they (data controllers) can fulfill their obligation to PbDesign and PbDefault according to Art. 7 FADP. This must be taken into account by the responsible parties, e.g., by means of contractual requirements vis-à-vis service providers or suppliers, appropriate design of procurement requirements, etc.

II. DATA PROTECTION BY TECHNOLOGY / PRIVACY BY DESIGN (PARA. 1-2)

A. Concept and Background

7 The concept of PbDesign is based on the idea that technical means should not hinder the implementation of data protection requirements, but rather enable and even promote it. Originally discussed under the rubric of specific "Privacy Enhancing Technologies (PET)," PbDesign evolved over time into a broader concept. There is no generally binding definition; rather, the term is used depending on the context in each case.

8 The content of the concept of PbDesign was significantly shaped by Ann Cavoukian (Privacy Commissioner of Ontario, Canada, from 1997-2014), with a concept of PbDesign based on 7 principles (principles in italics, emphasis in bold according to Cavoukian implementation):

1. *Proactive* not *Reactive*; **Preventative** not *Remedial*: PbDesign is to be understood as a proactive, anticipatory concept and is designed to prevent privacy breaches (rather than to remedy breaches that have occurred).

2. *Privacy as the Default Setting*: Even if the data subject does not take any specific actions, data protection should be ensured as comprehensively as possible, cf. below III - Data Protection Friendly Default Settings / Privacy by Default (para. 3).

3. *Privacy Embedded into Design*: Data privacy must be taken into account as an integral part of the design and implementation of systems and processes.

4. *Full Functionality - Positive Sum, not Zero-Sum*: Data privacy should not be prevented or lead to functional restrictions, but should create added value through its integral consideration.

5. *End-to -end security - Full lifecycle protection*: Data security must be ensured throughout the entire lifecycle of the data concerned.

6. *Visibility and Transparency - Keep it Open*: Transparency and verifiability must be guaranteed.

7. *Respect for User Privacy - Keep it User-Centric*: The interests of the data subjects must be taken into account.

These basic principles can serve as guidelines and aids to understanding. Due to their rather programmatic orientation, they are hardly suitable as concrete implementation aids. In the text of the law, references can at least be found to Principle 1 - Proactive/Preventative (in Art. 7 para. 1 FADP with the preventive approach and the reference to consideration from the planning stage), to Principle 2 - Default Setting (in Art. 7 para. 3 FADP regarding data protection-friendly default settings), and to Principle 3 - Embedded (in Art. 7 para. 1 FADP with the obligation to design data processing with regard to data protection requirements and consideration from the planning stage). Principle 5 - Full Lifecycle Protection is then addressed in Art. 8 para. 2 FADP and Principle 1 - Proactive/Preventative in Art. 8 para. 1 FADP. 9

For practical implementation, existing guidelines of a general nature (such as EDSA Guidelines 4/2019 on Article 25 DSGVO or ISO Standard 31700 on Privacy by Design) as well as sector- or application-specific guidelines can be helpful (see Section D - Implementation in Practice below). When implementing these, any differences arising from the fact that many such guidelines are geared towards the DSGVO must be taken into account. 10

B. Content and Scope (para. 1).

PbDesign aims to eliminate or at least reduce the risk of breaches of data protection rules through technical precautions, but without targeting a specific technology. Rather, appropriate technical and organizational measures ("TOM") are to be implemented in the design of the systems, applications and processes used. In this context, not only a specific system, an individual application or a specific technical aspect is to be considered, but in the sense of a "holistic approach" the entire data processing, with a focus on the implementation of the principles according to Art. 6 FADP. 11

12 From a temporal point of view, PbDesign must already be taken into account from the time of planning the data processing (Art. 7 para. 1 sentence 2 FADP). If a data protection impact assessment ("FADP") is to be carried out pursuant to Art. 22 FADP, the TOMs provided for the implementation of PbDesign may be included in the FADP process and listed there as measures within the meaning of Art. 22 para. 3 FADP. However, the obligation to PbDesign and the obligation to perform a FADP are independent of each other, i.e., the obligation to PbDesign exists even if there is no "high risk" within the meaning of the pick-up criterion of Art. 22 para. 1 FADP to perform a FADP.

C. Adequacy (para. 2).

13 The TOM to be implemented under PbDesign must be "adequate," which expresses the risk-based approach of this provision. Article 7 para. 2 FADP mentions "in particular" (a) the state of the art, (b) the type and scope of data processing, and (c) the risk to the personality or fundamental rights of the data subjects as relevant criteria for assessing adequacy. This list is not exhaustive; the overall view is decisive, taking into account the specific circumstances.

14 The state of the art refers to an advanced level of technical development that has proven itself in practical application or has become established in the market. This also includes the economic feasibility from a general, objective point of view (not that of the person responsible in each case). Since the state of the art is constantly evolving, particularly in the digital area, the implementation of PbDesign also includes an obligation to regularly check whether the implemented TOM still correspond to the current state of the art or need to be adapted if necessary: In this regard, Art. 7 para. 1 FADP stipulates that PbDesign must be taken into account "from" (and not merely "during") the planning stage.

15 The type and scope of data processing refer to the content-related and quantitative components of the processing: From a content-related perspective, it is in particular decisive which data (categories) are processed in which way and for which purpose. From a quantitative perspective, both the scope of data subjects (i.e., the number of data subjects) and the scope of the data categories processed (i.e., the number of data records affected) must be taken into account.

The risk to data subjects is the general benchmark for assessing the adequacy of TOM. The higher the risk, i.e., the greater the probability of occurrence and the potential consequences, the higher the requirements for the technical arrangements to be considered adequate. Clearly structured and mathematically probabilistic tools can serve as aids in risk assessment. However, they should only serve as a starting point, since the risk assessment must be carried out from a holistic, content-related perspective and take into account all (not just probabilistic) aspects. 16

In assessing appropriateness, a risk-based rather than an absolute standard should generally be applied. In this context, the risk associated with a processing operation must be set in relation to the technical possibilities for reducing it. The principle of PbDesign aims to strike an appropriate balance between the conflicting goals of data processing and data protection. In the sense of Principle 4 - Positive Sum, not Zero-Sum, formulated by Cavoukian (cf. n. 8 above), data processing should not be prevented, but rather made possible with due regard for data protection requirements, in order to create added value for data controllers and data subjects. 17

D. Implementation in Practice

There is no simple recipe for success on how to implement PbDesign universally. PbDesign must be understood as a project-specific process. Accordingly, there is no universal procedure that can cover all use cases. Rather, the TOM to be implemented must be geared (1.) to the specifics of the data processing in question, (2.) to the sector-specific environment in which it takes place, and (3.) to the pre-existing systems and processes in which it is embedded (whereby these must also be adapted if necessary). Successful implementation of PbDesign thus requires that the project- or processing-specific risks and requirements are identified and addressed with concrete measures tailored to them. In this context, the measures for implementing data security (Art. 8 FADP, Art. 1-6 FADP) cover only one (albeit extremely relevant) subarea (cf. n. 30 below). 18

A clearly structured procedure based on the relevant guidance for the application case is recommended, supplemented with further clarifications and specifications of one's own based on the project-specific particularities. This procedure should be sufficiently documented to allow for later review and updat- 19

ing (e.g., due to technical changes, further development of the state of the art, adjustments to the business case, etc.).

20 Various aids can be consulted for guidance, such as international standards, best practices from industry associations, guidance documents from data protection authorities, etc. During implementation, it should be noted that such guidance can be useful as a starting point, but must in any case be supplemented by the requirements of the specific use case and with respect to the current state of the art. It must also be taken into account that many of these guidelines were formulated with a view to Art. 25 DSGVO. When using them any differences under the FADP must therefore be taken into account, such as in particular the different starting position with regard to data processing (principle of prohibition with reservation of permission under the FADP versus fundamentally permitted data processing with restrictions and possibility of justification under the FADP).

1. International standards

21 The International Organization for Standardization (ISO) published the ISO 31700 standard on Privacy by Design in February 2023. This is divided into two parts: ISO 31700-1:2023 (https://www.iso.org/standard/84977.html) and ISO/TR 31700-2:2023 (https://www.iso.org/standard/84978.html).

22 The first part (ISO 31700-1:2023 - Consumer protection - Privacy by design for consumer goods and services - Part 1: High-level requirements) contains, in addition to general guidance and definitions of terms (clauses 1-3), in clauses 4-8 an overview of general requirements and procedures for the design of a product/service throughout its life cycle (such as. For example, Section 4.4 - Designing human computer interface (HCI) for privacy, Section 7.2 - Integrating the design and operation of privacy controls into the product development and management lifecycles, or Section 8.2 - Designing privacy controls for retirement and end of use). Since the ISO standard is not based on a specific data protection law foundation, it also contains, in addition to these design-specific requirements, specifications on aspects strongly influenced by the applicable (local) data protection law (such as Section 5.2 - Provision of privacy information, Section 5.4 - Responding to consumer inquiries and complaints, or Section 6.2 - Conducting a privacy risk assessment). Such requirements must therefore always be read in conjunction with the relevant legal provisions, such as Art. 19 et seq. FADP regarding the duty to inform, Art.

22 f. FADP regarding the data protection impact assessment, etc. However, they can also serve as a basis for a structured procedure in this regard.

The second part (ISO/TR 31700-2:2023 - Consumer protection - Privacy by design for consumer goods and services - Part 2: Use cases) contains three illustrative use cases that demonstrate the implementation of the requirements of the first part: (1) On line retailing (eCommerce online store); (2) Fitness company (fitness center with devices connected by sensors to a fitness app of the user); and (3) Smart locks (product line of electronic IoT door locks with online connection and associated control app). The use cases cover many practical aspects. The clearly structured implementation of the specifications of the first part in the use cases can therefore not only serve to familiarize the user with the topic, but also directly as a checklist when implementing individual relevant aspects. 23

In conclusion, it can be said that the ISO standards 31700-1/2 are kept at a high level of abstraction due to their general orientation. Nevertheless, they can serve as a good basis thanks to their clear structuring. The practice-oriented use cases can also be helpful in the sense of checklists for comparable aspects in different use cases. 24

2. Guides and orientation aids

There are many general guides and orientation aids. The following list can serve as a starting point for your own research. For a conceptual overview, for example, EDSA Guideline 4/2910 on Article 25 [DSGVO] of the European Data Protection Board (EDSA) is suitable, while for a more pragmatic start, for example, the Privacy Patterns can serve: 25

- **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).

26 In the area of software and application development in particular, various questions arise regarding the implementation of PbDesign and PbDefault. Guidance can be provided here by data protection authorities as well as industry-specific guidance, such as:

- **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. Examples of possible measures

27 The specific measures must be determined in each case depending on the specific use case and the associated risk profile. The following list can serve as an exemplary overview of possible measures and show initial starting points. Orientation to concrete use cases can also be helpful, cf. e.g. Tamò-Larrieux, p. 203 ff. and the use cases in ISO/TR 31700-2:2023 (cf. n. 23).

28 Possible measures can be grouped into aspects from a systemic perspective, more technical aspects, and those of an organizational nature. The systemic aspects relate (like the processing principles according to Art. 6 para. 1-5 FADP) in a holistic view to the entire business case. The technical and organizational aspects intersect with the data security requirements (Art. 8 FADP). The systemic, technical and organizational aspects overlap in many areas and can hardly be clearly distinguished from each other. However, by using the systemic aspects to pull certain higher-level topics "in front of the bracket" of technical/organizational implementation, so to speak, a structured approach can be facilitated, in particular by allowing general, higher-level aspects to flow into all considerations at an early stage and to be taken into account in all project phases.

29 From a general, higher-level systemic perspective, the following aspects should be examined, for example:

- **Data minimization (FADP 6 para. 2)**: The personal data collected must be limited in terms of content (which data (categories)) and scope (how much data, e.g., in terms of time) to what is necessary for processing the respective business case; there should be no "data collection for stock".
- **Data segregation**: Restraint in linking or pooling data, centralizing data holdings and aggregating data sets, etc.
- **Pseudonymization**: Pseudonymization can create additional protection (in the sense of segregating identification information from other data categories), especially if the linking of certain data to a specific person is only necessary for certain processing steps.

- **Data declaration**: marking of the data records (e.g. by means of metadata or descriptors) e.g. concerning origin, protection level, storage period ("expiration date"), etc.
- **Anonymization and/or deletion (Art. 6 para. 4 FADP)**: To implement the principle of data minimization (e.g. by means of "expiration dates" for certain data sets, by regular anonymization/deletion cycles, etc.).

From a technical point of view, reference can be made first and foremost to the technical measures required to implement data security (cf. Art. 8 FADP and the explanations on this in Art. 1-6 FADP). However, other technical measures are also conceivable which do not (only) serve data security, but the general data protection objectives in general. For example, technical measures to implement the general processing principles (Art. 6 para. 1-5 FADP) and the principle of data minimization (Art. 6 para. 2 FADP) may be particularly relevant. One might think, for example, of the technical implementation of deletion concepts (see above) or the automatic pixelation of faces/identifying features in the case of non-personal images/videos, etc. 30

From an organizational perspective, the internal prerequisites must be created to implement the systemic and technical requirements. This may include the following aspects, for example: 31

- **Corporate culture and holistic view**: The corporate culture must understand data privacy as part of corporate activity (and not, as is often still the case, as an externally imposed restriction). A "data protection-friendly mentality" is therefore necessary. In addition, data protection must be viewed as a whole, i.e., not only in terms of specific processing, but also, for example, as part of contract/vendor management.
- **Processes, responsibilities and documentation**: The implementation of procedures and processes relevant to data protection must be defined and adequately documented. Clear responsibilities and sufficient documentation are particularly important. Even if there is no general principle of accountability under the FADP, and there may be no legal obligation to create a specific document (e.g., a processing directory, cf. Art. 12 in conjunction with Art. 24 FADP), its creation (at least in a simplified form) may nevertheless be necessary or at least helpful in order to be able to implement the principles of PbDesign, review them over time and adapt them if necessary.

- **Training and sensitization**: To ensure that the planned TOM are actually implemented, employees must be trained accordingly and sensitized to data protection issues, e.g., through data protection training, internal directives and regulations, etc.
- **Technical implementation**: The technical measures (N. 30) must be supplemented by appropriate organizational measures to ensure their implementation. For example, effective access restriction also requires a process for granting access authorizations, regularly checking that they are up to date, and ensuring that they are deleted (e.g., when employees change jobs or duties). Likewise, the specification of a restriction on the storage period of certain data requires an associated process for the regular performance of a corresponding check and possible deletion.

III. DATA PROTECTION-FRIENDLY DEFAULT SETTINGS / PRIVACY BY DEFAULT (PARA. 3)

A. Term

32 PbDefault is a partial content of PbDesign (cf. n. 8 no. 2 above) and was formulated in Art. 7 para. 3 FADP. The wording is misleading, as there is no obligation to create special setting options (cf. n. 35 below). The obligation under Art. 7 para. 3 FADP only refers to the fact that if there are several setting options, the default settings must be set in such a way that the most "minimally invasive" data processing in terms of data protection is implemented.

33 The Message describes the default settings as "those settings, in particular of software, which are applied by default, i.e. if no deviating input is made by the user". This is to be understood as the basic setting, standard setting or "default configuration" which is applied in each case if the users do not actively select another setting themselves.

B. Content and scope

34 Even though the message specifically mentions software as a use case, the scope of application is not limited to software or system settings, but concerns all data processing. Thus, all setting options that exist during data processing and, in particular, data collection are generally covered. Where various setting

options or choices exist, the most data protection-friendly combination of settings must be provided as the basic setting.

Data protection-friendly default settings can only be made if various setting options are provided at all. Whether such are to be provided must be examined under the aspect of PbDesign (N. 7 ff.). The provisions on PbDefault (Art. 7 para. 3 FADP) in any case do not impose a specific obligation to provide certain setting options in every case in order to differentiate the intensity of the data protection intrusion. 35

In terms of content, the qualitative focus must be on the extent of the intrusion into the personal or fundamental rights of the data subjects, not solely (quantitatively) on the number and scope of the data processed. The reference in the dispatch to the principle of data minimization is to be understood as a reference to the guiding principle of PbDefault, and not as an indication that its implementation should be approached in a purely quantitative-technical manner. 36

The purpose of the processing serves as a yardstick (cf. the wording regarding the limitation "to the minimum necessary for the purpose of use"). In determining this purpose, the controller remains free, i.e. there is no obligation to offer certain services even without data collection or data processing. If, for example, an online service is financed by personalized advertising, there is no obligation to offer an ad-free version of this service. However, when implementing the online service and the associated data processing for personalized advertising, the principles of PbDesign and PbDefault must be observed. 37

Based on the most privacy-friendly default setting, data subjects can make a different choice and thus also allow more extensive data processing. There is no obligation to provide for such further options. However, the controller is likely to provide for this as a rule out of its own interest, in order to give data subjects the opportunity to consent to more extensive data processing that would not be strictly necessary to achieve the narrowly defined purpose of use. 38

C. Implementation in practice

The starting point is the purpose of use and the "most minimally invasive" data processing necessary to implement or achieve it. Whether different implementation variants or setting/choice options are available must be decided by 39

the responsible party on the basis of the business or use case and by applying the principles of PbDesign (n. 7 ff.). If this is the case, the most data protection-friendly combination of setting/choice options must be provided as the default or basic setting, i.e., the default setting with the least impact on the privacy rights or fundamental rights of the data subjects.

40 If the data subjects are given the option to deviate from these most data protection-friendly settings and to allow further processing, it must be checked whether consent within the meaning of Art. 6 para. 6 FADP is required for such further processing and thus whether the conditions provided for therein (and possibly also those of Art. 6 para. 7 FADP) must be observed.

41 While (under Swiss law, in contrast to the situation under the DSGVO), under the aspect of consent, pre-activated checkboxes ("ticked boxes") can also be considered (explicit) consent, depending on the circumstances, this seems questionable under the aspect of PbDefault: the purpose of PbDefault and its formulation in Art. 7 para. 3 FADP is precisely that data subjects should be able to rely on all setting/choice options implementing the most data protection-friendly variant in the basic setting.

42 This is to be observed under the headings of the trust principle and the unusualness rule by analogy with the rules of interpretation developed for global adoptions of GTCs. The purpose of PbDefault pursuant to Art. 7 para. 3 FADP is precisely that data subjects should not be expected to study each setting option individually, check it for its privacy-friendliness and then have to switch it on or off or select or deselect it individually. Rather, they should be able to rely on the fact that the combination of setting/choice options presented to them at first use represents the most data-saving, data protection-friendly and thus "minimally invasive" combination of setting options.

43 Depending on the specific wording of the individual setting options, this may of course mean that certain selection fields must already be activated in advance: If a selection option consists, for example, of an option such as "I do not wish to receive product information", such a selection field would have to be activated by default in accordance with the principle of PbDefault (even if the delivery of product information would be permissible under Art. 3 para. 1 lit. o UWG on the basis of a pre-existing customer relationship).

44 Depending on the specific wording of the individual setting/choice options, it may therefore be the case that under the aspect of PbDefault certain options

must be activated, while others must be deactivated. The decisive factor is that the combination of enabled/disabled options implements the most data protection-friendly combination of setting/choice options in each individual case. Data subjects should be able to rely on the fact that, provided they do not make any changes to these default settings, they will always enjoy the most data protection-friendly setting.

According to the view expressed here, this must also apply to the default setting in the context of obtaining consent. The requirements for PbDefault are not limited to purely technical parameters, but according to Art. 7 para. 3 FADP are directed at "the processing of personal data" in general. In a holistic view, as the concepts of PbDesign and PbDefault presuppose, any consent obtained must also be understood. The unusualness rule should be applied here: If users confirm GTCs in the context of a global acceptance, they are protected from unexpected consequences by the unusualness rule. The same should apply when adjusting settings and obtaining consent: The principle of PbDefault creates a legitimate expectation among data subjects that they will benefit from the most privacy-friendly setting at all times without having to make their own adjustments. This should not be undermined by allowing pre-activated selection fields for more extensive processing that does not correspond to the most data protection-friendly basic setting. Rather, data subjects should be protected in their trust in the comprehensive implementation of the principle of PbDefault. The concrete circumstances of the respective application case are decisive for the assessment. 45

IV. CONSEQUENCES OF BREACH OF DUTY

Violation of the obligations of Art. 7 FADP has no direct sanctioning consequences (cf. Art. 60 et seq. FADP). Nor does such a breach of the duty to implement PbDesign and PbDefault per se (yet) constitute a personal injury: Art. 30 para. 2 lit. a FADP explicitly refers only to Art. "6 and 8" (and not "6 to 8"): "In particular, a violation of privacy occurs if: (a) personal data are processed contrary to the principles set forth in Articles 6 and 8." 46

On the other hand, a breach of the obligations of Article 7 FADP may have indirect sanctioning consequences if the systems, applications and processes underlying a processing operation make it impossible or restrict compliance with the data protection requirements due to inappropriate planning and/or implementation. If, for example, stored personal data cannot be accessed 47

(and, if necessary, edited, corrected or deleted) in a personalized manner, and the data controller is (or must be) aware of this, it is only a small step to (possibly) intentionally providing false or incomplete information within the meaning of Art. 60 para. 1 lit. a FADP.

48 Inadequate implementation of the principles of PbDesign and PbDefault may also result in the data processing carried out generally violating data protection regulations, in particular the principles of Art. 6 FADP. If there are sufficient indications of such violations, the FDPIC may open an investigation ex officio or upon notification (Art. 49 para. 1 FADP) and issue appropriate orders (Art. 51 FADP), including an order to implement the principles of PbDesign and PbDefault (Art. 51 para. 3 lit. b FADP). If an order of the FDPIC is then not complied with, a sanction under Art. 63 FADP (disregard of orders) may be imposed.

V. TRANSITIONAL PROVISIONS

49 In principle, the FADP is directly applicable to all data processing from the time of its entry into force, unless Art. 69 et seq. FADP do not provide for special transitional provisions. According to Art. 69 FADP (transitional provisions concerning ongoing processing), the requirements of Art. 7 FADP do not apply to existing data processing that continues unchanged: "Articles 7, 22 and 23 do not apply to data processing that was started before the entry into force of this law if the purpose of the processing remains unchanged and no new data are obtained."

50 The exemption provision of Art. 69 FADP thus refers only to data processing with purely static data sets and a constant processing purpose and only to existing data processing, not to the systems, applications, processes or other aspects of data processing used for this purpose as such: As soon as new data is processed with an existing system, application or process, or for new purposes, this system, application or process (or other aspect of data processing) must be measured against the newly applicable specifications of PbDesign and PbDefault. Thus, while legacy systems that continue to operate unchanged (such as a purely static archive application with no new data inflows) are covered by the transitional provisions, existing operational systems, applications and processes must be designed in accordance with the principles of PbDesign and PbDefault and continuously adapted to the relevant state of the art.

BIBLIOGRAPHY

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/7foundational-principles.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.

MATERIALS

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).

COMMENTARY ON

Art. 10 FADP

A commentary by Michèle Balthasar

SUGGESTED CITATION

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

Short citation: OK-Balthasar, N. XXX zu Art. 10 DSG.

Art. 10 Data protection officer

[1] Private controllers may appoint a data protection officer.

[2] The data protection officer is the contact point for the data subjects and for the authorities responsible for data protection in Switzerland. He or she has the following tasks in particular:

a. training and advising the private controller in matters of data protection;

b. providing support on applying the data protection regulations.

[3] Private controllers may invoke the exception in Article 23 paragraph 4 if the following requirements are satisfied:

a. The data protection officer exercises his or her function towards the controller in a professionally independent manner and is not bound by any instructions.

b. He or she does not carry out any activities that are incompatible with his or her tasks as a data protection officer.

c. He or she has the required expertise.

d. The controller publishes the contact details of the data protection officer and notifies the FDPIC thereof.

[4] The Federal Council shall regulate the appointment of data protection officers by federal bodies.

CONTENT

IN A NUTSHELL

Art. 10 FADP regulates the appointment and duties of the data protection advisor as well as the conditions for using the exemption under Art. 23 para. 4 FADP. The institution of the data protection advisor enables private companies to regulate themselves. The appointment of a data protection advisor is voluntary for the private controller, however, if appointed, it may benefit from the exemption whereby consultation of the FDPIC may be waived in the case of a data protection impact assessment (DIA) under certain conditions.

I. GENERAL

A. Introduction

1 Art. 10 FADP governs the appointment and duties of the data protection advisor as well as the conditions for using the exemption under Art. 23 para. 4 FADP. Art. 23 DPA specifies the requirements for a private controller who appoints a data protection advisor. The institution of the data protection advisor also enables private companies to regulate themselves or to appoint a person to manage data protection within the company.

2 With the introduction of the new provision on the data protection advisor in Art. 10 FADP, the consultation of the FDPIC - which is mandatory under certain conditions - in the context of a DIA is now facilitated. Thus, a data processing project of private data controllers that still presents a "high risk" despite a FADP has been performed no longer has to be submitted to the FDPIC if the data protection advisor has already been consulted (Art. 23 para. 4 FADP). A company that has appointed a data protection advisor may therefore rely solely on internal data protection advice without having to consult the FDPIC in addition.

3 The appointment of a data protection advisor is voluntary for the private controller. Under the previous law, the appointment of a "data protection advisor" (comparable in its design) meant that companies were no longer required to notify the FDPIC of their data collections, which would otherwise be subject to registration. With the revision, the obligation to register for private individuals is generally eliminated.

While the appointment of a data protection advisor is voluntary for private data controllers, it is mandatory for federal bodies (Art. 10 para. 4 FADP in conjunction with Art. 25 ff FADP). The Federal Council regulates in Art. 25 DPA the appointment, in Art. 26 DPA the requirements and duties of the data protection advisor of federal bodies. Art. 27 DPA defines the duties of the federal bodies vis-à-vis the data protection advisor, and Art. 28 DPA defines the data protection advisor as the point of contact vis-à-vis the FDPIC. 4

B. Comparative law

1. Obligation to appoint a data protection officer under DSGVO

With the entry into force of the DSGVO, the European Union introduced the obligation to appoint a so-called data protection officer in certain cases. Art. 37 para. 1 DSGVO lists three groups of cases in which a data protection officer must be appointed. 5

First, according to Art. 37 para. 1 lit. a DSGVO, this obligation exists for public authorities and public bodies, with the exception of courts, if they act within the scope of their judicial activities. This includes, for example, building authorities, water and energy suppliers or transport companies. 6

Furthermore, Art. 37 para. 1 DSGVO in lit. b imposes an obligation to designate if the core activity of the controller or processor is to carry out processing operations which, by virtue of their nature, their scope and/or their purposes, require extensive regular and systematic monitoring of individuals. Recital 97 to the DSGVO explains that the core activity of a controller refers to "its main activities and not to the processing of personal data as an ancillary activity." The European Commission's Article 29 Working Party had published guidance on this topic with WP 243 regarding Data Protection Officers ("DPOs"). "Core activities" are thus the main work processes necessary to achieve the controller's or processor's objectives. "Regular" monitoring is when it is ongoing or periodic, and "systematic" when it follows a methodical or organized approach or is part of a broader strategy. Examples include private security companies that monitor private shopping malls and public places, or apps whose core functionality requires the analysis of location data (e.g., sports or navigation apps). 7

8 Finally, according to Art. 37 para. 1 lit. c DSGVO, there is an obligation to designate a data protection officer in cases where the core activity of the controller or processor consists of extensive processing of special categories of personal data pursuant to Art. 9 DSGVO or of personal data relating to criminal convictions and offences pursuant to Art. 10 DSGVO. Whether a processing operation is extensive within the meaning of this provision must be clarified on a case-by-case basis, for example by taking into account the amount of data processed or the number of data subjects. Examples are the processing of patient data in the ordinary course of business of a hospital or the processing of customer data in the ordinary course of business of an insurance company.

2. Obligation to appoint a data protection officer in accordance with country-specific regulations.

9 Country-specific regulations may provide for more extensive provisions under which a data protection officer must be appointed. For example, the German Federal Data Protection Act (BDSG) provides for an obligation to appoint a data protection officer if at least 20 employees are permanently involved in the automated processing of personal data (Section 38 para. 1 sentence 1 BDSG). In addition, Section 38 para. 1 sentence 2 of the BDSG lists two further scenarios in which companies must appoint a data protection officer regardless of the number of persons involved in the processing: On the one hand, in cases where a DSFA is required pursuant to Art. 35 DSGVO, and on the other hand, in constellations in which they process personal data on a businesslike basis for the purpose of anonymized transmission or for the purpose of market or opinion research.

C. Terminology

10 The former FADP used the term "data protection officer" in German and "responsabile per la protezione dei dati" in Italian, while the French version reads "conseiller à la protection des données," i.e., "data protection advisor" (Art. 11a para. 5 lit. e aDSG). In order to avoid confusion with "responsible person" according to Art. 5 lit. i FADP or with "responsabile", the revision of the FADP introduced the term "data protection advisor" in German or "consulente per la protezione dei dati" in Italian. As a result, the terminology of Art. 10 FADP has been standardized in all three languages.

At the same time, it has also been clarified that the responsibility for the processing of personal data in compliance with data protection law does not lie with the data protection advisor, but with the company responsible, the "responsible party". 11

II. DATA PROTECTION ADVISOR TO THE PRIVATE CONTROLLER

A. Appointment of the Data Protection Advisor (Art. 10 para. 1 FADP)

1. Voluntary nature of the appointment of a data protection advisor

Art. 10 para. 1 FADP states that the appointment of a data protection advisor is voluntary for private data controllers. According to the FADP, it is thus up to the private controller whether it appoints a data protection advisor. However, a company that has appointed a data protection advisor in accordance with Art. 10 para. 3 FADP may, even if the risk remains high, rely solely on internal data protection advice after carrying out a DIA without having to consult the FDPIC (Art. 23 para. 4 FADP). 12

However, companies that operate internationally must comply with the requirements of the DSGVO and are therefore often required to appoint a data protection officer pursuant to Art. 37 DSGVO. 13

Furthermore, it is in the interest of every company to ensure efficient and effective data protection within its organization in terms of appropriate compliance. It is therefore often advisable to at least appoint a data protection officer internally and to entrust him or her with data protection tasks. This person does not have to fulfill the requirements under Art. 10 para. 3 FADP. However, if he or she does not meet the requirements under Art. 10 para. 3, the company cannot benefit from the facilitations under Art. 24 para. 3 FADP. 14

In the case of the designation of such a person or body, ambiguities regarding their functional designation, status, position and field of activity should be avoided. It should therefore already be clear from the job title within the company and vis-à-vis the FDPIC and the data subjects that it is not a data protection advisor pursuant to Art. 10 para. 3 FADP. It is advisable to choose a different designation for this function, such as data protection unit, data pro- 15

tection contact person, data protection coordinator or privacy officer. The company responsible is free to assign tasks as it sees fit. Nevertheless, the tasks should be clearly defined in a specification.

2. Appointment of an Internal or External Data Protection Advisor

16 The company responsible may designate an internal person or an external person or body as data protection advisor.

17 The internal data protection advisor is an employee or a department of a company who specifically deals with data protection in the respective company. In larger companies, they are regularly supported at a lower hierarchical level by so-called data protection managers or data owners who are responsible for data protection in their respective area, such as for creating and maintaining the list of processing activities (Art. 12 FADP).

18 External data protection consultants, on the other hand, are natural or legal persons who offer the service of data protection (data protection as a service) and act on the basis of a contractual relationship. As a rule, however, even in these cases a contact person must be appointed within the company to serve as a point of contact for both him or her and the employees on data protection issues within the company.

19 The advantage of an internal data privacy advisor is that he or she is integrated into the company itself and thus has a better overview of the internal processes. Furthermore, the advisor can directly check and influence that data privacy is "lived" in the corporate culture and does not exist only on paper. On the other hand, it can be disadvantageous to be too close to the company and its employees, which can lead to conflicts of interest. Often, there is also a lack of resources and the corresponding know-how, or there are conflicts of interest to ensure that data protection is adequately safeguarded within the company. In such situations, it makes sense to outsource the mandate of the data privacy advisor.

3. Appointment of a joint data protection advisor for a group of companies

20 For a group of companies, it is possible to appoint a joint data protection advisor. However, the joint data protection advisor must be easily accessible to the data subjects and the FDPIC as an internal contact person via suitable

communication channels. He or she must be able to communicate effectively with data subjects and cooperate effectively with the competent supervisory authorities. However, there is no obligation to be based in Switzerland as long as the data protection advisor is able to perform his or her duties effectively. Nevertheless, knowledge of a national language is likely to be required.

B. Tasks of the data protection advisor (Art. 10 para. 2)

1. Contact point for the FDPIC and other authorities responsible for data protection in Switzerland, as well as for data subjects

The data protection advisor is an important point of contact with regard to the data processing activities carried out by the data controller. He or she is involved in the company's data protection compliance processes. A professional contact person can thus be identified directly, which makes it easier for the FDPIC or data subjects to exercise their rights. 21

For questions relating to the processing of personal data in the company, he or she therefore serves as a point of contact for the FDPIC and other authorities responsible for data protection in Switzerland (such as FINMA or the cantonal data protection authorities). He or she also serves as a point of contact for the data subjects, for example in the event of a request for information pursuant to Art. 25ff. FADP. 22

2. Training and advice for the private controller on data protection issues (para. 2 lit. a)

In order to ensure effective data protection in the respective company, the data protection advisor must train, educate and sensitize the private controller or its employees accordingly. At the very least, all employees who come into contact with personal data must be involved. The focus should be on the principles of data protection law (Art. 6 FADP). Other training topics include the requirements for disclosure abroad and the handling of particularly sensitive personal data within the company. In addition, employees must also be trained with regard to data security requirements (Art. 8 FADP). 23

The training of employees in data protection and data security by the data protection advisor should be repeated at regular intervals, preferably annually. Regular awareness-raising ensures that the topic of data privacy remains 24

present in the minds of employees. In addition, current innovations, e.g., with regard to the company's IT landscape, can be passed on to employees in a timely manner.

25 In his or her advisory role, the data privacy advisor has the task of advising on compliance with data privacy regulations in data processing, identifying the relevant facts of the data privacy issue in each case and, on the basis of these facts, identifying alternative decisions.

3. Cooperation in the application of data protection regulations (para. 2 lit. b)

26 A further task of the data protection advisor is his or her involvement in the application of the data protection regulations. This includes, in particular, helping to issue terms of use and data protection regulations. Furthermore, he or she shall review the processing of personal data and recommend corrective measures if a violation of data protection regulations is identified. In addition, she or he shall assist the private controller in the preparation of DSFAs and review their execution. Furthermore, it is important that the data protection advisor is perceived as an interlocutor within the institution and that he or she is a member of the relevant working groups that deal with data processing activities within the company. However, it is not part of the duties of the data protection advisor of the private controller to report data security breaches to the FDPIC or to data subjects. Although it may often make sense to involve the data protection advisor in the case of data security breaches, this is not required by law.

27 The data protection advisor is to be understood as a supporting body, but not as a supervisory body. With regard to the auditing of data processing and the recommendation of corrective measures, it is therefore not a question of introducing an active auditing obligation or prescribing systematic controls of all data processing. Rather, it is sufficient for the data controller to become active if, for example, the data controller requests an audit of data processing or if he or she receives indications that data protection regulations have been violated. Of course, the data controller is free to demand that the data protection advisor proactively check data processing. It is conceivable and common in practice that he or she will conduct a data protection audit once a year.

Other tasks of the data protection advisor that may be considered are: 28

- Developing and reviewing the implementation of data security measures (Art. 8 FADP);
- Examination of processing by the processor (Art. 9 FADP);
- elaboration and audit of the registers of processing activities (Art. 12 FADP);
- Examination of the disclosure of data abroad (Art. 16 ff. FADP);
- Support in the fulfillment of information obligations (Art. 19 ff. FADP);
- Development and implementation of processes for handling requests from data subjects (Art. 25 FADP);
- Developing appropriate processes to safeguard data subjects' rights and comply with data protection regulations (Art. 25 ff. FADP);
- Conducting risk assessments (e.g., risk of unintentional/unauthorized data disclosure, deletion or processing, data loss or technical error, etc.), for example, as part of a DSFA;
- Preparation of annual reports on the activities for the attention of the controller

4. Excursus: No Responsibility of the Data Protection Consultant

It is often assumed that the data protection advisor is responsible for data protection and its compliance within the company. However, the data protection advisor has no authority to act beyond his or her training, advisory and participation functions, which are derived from the FADP itself. The sole decision-making authority - and thus also the sole responsibility for the processing of personal data in compliance with data protection law - lies with the company responsible. The data protection advisor should report to the highest management level of the company concerned. The situation would only be different if the data protection advisor were to act as a de facto body and thus have a decisive influence on the decision-making of the controller by deciding on the means and purpose of the processing. However, this would not be permissible due to the professional independence required under Art. 10 para. 3 FADP and the fact that the data protection advisor is not bound by instructions. If a data protection advisor nevertheless decides on the purpose and 29

means of data processing, liability (of a mandatory and/or criminal nature) would be possible.

30 If the data protection advisor makes recommendations, the company should ensure that the recommendations are implemented. If it does not do so and the recommendation was justified, this can - if such an incident becomes public - lead to not inconsiderable damage to the company's image. This may even lead to sanctions being imposed on an individual employee. However, if the recommendation was wrong or incorrect, the data protection advisor is liable within the scope of his or her existing employment or contractual relationship.

C. Requirements for the data protection advisor (para. 3)

31 In order for a company to be released from consulting the FDPIC if a high risk still exists despite the FADP having been performed (Art. 23 para. 4 FADP), the data protection advisor must meet the requirements of Art. 10 para. 3 FADP.

1. Professionally independent and not bound by instructions (lit. a)

32 The data protection advisor must be independent in his or her activities to the extent that the tasks can be performed independently of instructions and cannot be sanctioned by the company on the basis of his or her activities. This means that he or she may not be given any instructions in the performance of his or her duties as to how he or she should proceed in a given situation, e.g., what result should be achieved, how a complaint should be followed up or whether or not the FDPIC should be consulted. Furthermore, he or she must not be instructed to take a particular position on a question of data protection law (for example, with regard to the interpretation of a law).

33 In addition, it must be ensured that the data protection advisor can freely express his or her recommendations - even if they may be disagreeable in part - without fear of disadvantage. This independence also means that the data protection advisor can refer important matters to the highest management (such as the board of directors of a stock corporation) (Art. 23 lit. c FADP). In principle, he or she should therefore also report directly to the management or even the board of directors of the controller.

2. No incompatibility with other duties (lit. b)

In order for the data protection advisor to be able to perform his or her duties within the company, he or she must not engage in any other activities that are incompatible with his or her duties. Data privacy consulting should be performed separately from the tasks of the company. A conflict of interest must be avoided. This could be the case, for example, if the data privacy consultant is a member of the management, head of the operating division or head of the IT department, or if he or she performs functions in the area of personnel management or information system management (such as IT manager). The data protection advisor may not at the same time hold a position in which he or she himself or herself decides on the means and purpose of the data processing activities of the data controller or has an interest in such activities. It is also advisable not to mix data protection advice with that of other legal advice and representation. 34

A possible conflict of interest must therefore be avoided in advance by the organizational position of the data protection advisor. As a matter of principle, care should be taken to ensure that no line responsibility is associated with the position of data privacy advisor. It is therefore advisable for a company to establish the function of data privacy advisor as a staff position, for example. It is important that this does not involve an executive function in a business area. Another possibility would be to combine the task of the data privacy advisor with that of the information security officer. 35

Because conflicts of interest are otherwise hardly avoidable in practice, the data protection advisor - except in the case of larger companies with their own data protection departments - is likely to be an external service provider as a rule. 36

3. Required Expertise (lit. c)

In order to be able to perform his or her duties independently, the data protection advisor must have the necessary professional qualifications. She or he must have sufficient knowledge in all areas to be able to assess recommendations and proposed measures and evaluate them within the framework of the company's data protection strategy. 37

The requirements include not only knowledge in the area of data privacy and data security, but also expertise specific to the company. If she or he may have 38

less developed knowledge in certain areas, she or he must at least be able to access such knowledge. Interdisciplinary knowledge, especially in the areas of IT and law, is required. Management systems must be understood.

4. Publication of contact data (lit. d)

39 It is the responsibility of the data controller to publish the contact details of the data protection advisor and to notify the FDPIC. The FDPIC has created a reporting portal for this purpose. As with the private controller, it is not necessary for the company to publish the name of the data protection advisor. It is sufficient, for example, if the e-mail address of the technically responsible office is provided. The responsible office can also be an entire team or a company. The data protection advisor is an important contact person with regard to the data processing carried out by the company in question. The publication of contact details ensures that data subjects or the FDPIC can contact the data protection advisor directly.

40 It is not necessary for the company to publish the name of the data protection advisor. It is sufficient, for example, if the e-mail address of the technically competent office is provided.

D. Obligations of the Private Controller (Art. 23 DPA).

41 In order for a company to be exempted from consulting the FDPIC if there is still a high risk despite the FADP having been performed (Art. 23 para. 4 FADP), the private controller must also fulfill certain obligations. The content of these obligations corresponds to the previous provisions of data protection law; they have only been adapted to the new FADP in terms of terminology.

1. Provision of the necessary resources (lit. a)

42 Pursuant to Art. 23 lit. a DPA, the private controller must provide the data protection advisor with the necessary resources - usually in the form of working time - to enable him or her to perform his or her duties. While the requirements vary depending on the size of the company, she or he must always have sufficient resources to adequately perform the function. This means that the more complex and/or sensitive the data processing operations, the more resources must be made available to the data protection advisor.

2. Granting access to all information, documents, lists of processing activities and personal data (lit. b)

In order to be able to perform his or her function, the data protection advisor must be granted access, upon request, to all information, documents, lists of processing activities and personal data that he or she requires to perform his or her duties. In addition to access, this also includes that he or she obtains knowledge of all data processing activities carried out within the company. This requires a comprehensive right to inspect documents, a right to be shown data processing systems and a right to information from all persons responsible for data processing. It would be advisable to introduce a reporting obligation within the company, which means that all data processing must be reported to the data protection advisor. 43

However, access to the information is restricted in that it applies only to those documents which the data protection advisor actually needs to fulfill his or her duties. For example, if the data protection advisor is conducting a general review of internal data protection regulations or data processing processes, he or she will not normally need access to personal data. 44

3. Granting the right to inform the highest management or administrative body in important cases (lit. c)

Art. 23 lit. c DPA introduces the possibility for data protection advisors to inform the highest management or administrative body in important cases, i.e., the body that also bears responsibility for compliance with data protection regulations in the company. This is because the data protection advisor does not have any decision-making power of his or her own, but is subordinate to the highest management level of the company concerned. 45

The provision establishes a right of escalation for the data privacy advisor. This allows the data protection advisor not only to rely on the documents available to him or her during internal audits of compliance with data protection regulations, but also to enforce the procurement of additional information and documents. In addition, this ensures that the data protection advisor can report to the highest bodies of the controller or the commissioned processor in the event of complex circumstances and particularly serious violations and bring about a decision. In practice, information to the highest man- 46

agement or administrative body may also be provided by means of quarterly and annual reports on the activities of the data protection advisor.

III. DATA PROTECTION ADVISOR TO FEDERAL BODIES (ART. 10 PARA. 4 FADP)

A. Appointment (Art. 25 DPA)

47 Federal bodies are required to appoint a data protection advisor in the Schengen area based on Article 32 of Directive (EU) 2016/680. However, the rules governing the appointment of the data protection advisor by the federal bodies are not found in the FADP, but have been left to the Federal Council (Art. 10 para. 4 FADP).

48 According to Art. 25 DPA, several federal bodies may jointly appoint a data protection advisor. This provision is intended primarily to enable smaller federal bodies or departments with a centralized organizational structure to take advantage of sensible and resource-saving synergies. Larger federal agencies, on the other hand, can be expected to appoint a data protection advisor on their own. It is also open to federal bodies to appoint several data protection advisors.

B. Requirements and Tasks (Art. 26 DPA)

49 Art. 26 para. 1 DPA contains the requirements for the data protection advisor: he or she must have the necessary expertise and exercise his or her function vis-à-vis the federal body in a professionally independent manner and subject to instructions. This provision is analogous to the one under Art. 10 para. 3 FADP for private data controllers, which is why reference can be made to it.

50 The role of the data protection advisor in federal bodies, which are usually hierarchical, has been strengthened and institutionalized with the revision so that he or she can perform his or her duties effectively. The independence of the data protection advisor is expressed by the fact that in important cases - as provided for private individuals in Art. 23 lit. c FADP - the data protection advisor can turn to the top management of the federal body. The independence of the data protection advisor must be guaranteed primarily by organizational measures: for example, it is important to prevent the activity as a data protection advisor from having a negative impact on the employee interview.

Art. 26 para. 2 DPA contains the tasks of the data protection advisor of a federal body. They have been terminologically aligned with the provision in the case of private data controllers (Art. 10 para. 2 FADP), which is why reference can also be made to the statements made there. He or she participates in the application of the data protection regulations, in particular by examining the processing of personal data and recommending corrective measures (lit. a). If a violation of the data protection regulations is identified, he or she advises the data controller and reviews its implementation (lit. b). Furthermore, he or she trains and advises the employees of the federal body on data protection issues (lit. c). Finally, he or she serves as a point of contact for data subjects (lit. d). 51

C. Duties of the federal body (Art. 27 FADP)

The federal body shall grant the data protection advisor access to all information, documents, lists of processing activities and personal data that he or she requires to perform his or her duties (Art. 27 para. 1 lit. a FADP) and shall ensure that he or she is informed of any breach of data security (Art. 27 para. 1 lit. b FADP). 52

Art. 27 para. 1 lit. a DPA is thus identical to the regulation for private controllers in Art. 23 lit. b DPA. Reference can be made mutatis mutandis to the explanations there. Moreover, this obligation applies to all breaches of data security, not only to those that must be reported to the FDPIC pursuant to Art. 24 FADP. Information on data security breaches pursuant to Art. 27 para. 1 lit. b FADP can be ensured, for example, by the federal body obliging employees by means of instructions to inform the data protection advisor in the event of a data security breach. The data protection advisor advises the data controller on whether the breach is subject to a notification obligation within the meaning of Art. 24 FADP. The federal body shall ensure that he or she is informed of a data breach. However, the notification itself is the responsibility of the federal body. It decides whether and which breaches are reported to the FDPIC. 53

Finally, the federal body publishes the contact details of the data protection advisor on the Internet and communicates them to the FDPIC (Art. 27 para. 2 FADP). As with the private controller, it is not necessary for the company to publish the name of the data protection advisor. It is sufficient if, for example, 54

the e-mail address of the technically competent body is provided. The competent body can also be an entire team or a company.

D. Contact point of the FDPIC (Art. 28 DPA)

55 The data protection advisor serves as the FDPIC's point of contact for questions relating to the processing of personal data by the federal body concerned. Thus, since he or she has the necessary expertise and internal knowledge, he or she is the direct technical contact person for the FDPIC.

BIBLIOGRAPHY

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).

MATERIALS

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.

COMMENTARY ON

Art. 11 FADP

A commentary by Ursula Sury / Jael Inauen

SUGGESTED CITATION

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

Short citation: OK-Sury/Inauen, N. XXX zu Art. 11 DSG.

Art. 11 Code of conduct

[1] Professional, industry and trade associations that are authorised to safeguard the economic interests of their members in their articles of association and federal bodies may submit codes of conduct to the FDPIC.

[2] The FDPIC shall state and publish his or her opinions on the codes of conduct.

CONTENT

IN BRIEF

Codes of conduct are rules of behavior, from professional, industry and business associations. They have become established in the business world as part of "good corporate governance" as a code of conduct and are now to be extended to data privacy. The requirements and provisions of data protection law are specified in sector-specific terms by codes of conduct. Federal bodies and private associations are free to draw up their own codes of conduct.

The codes of conduct may be submitted to the FDPIC. The FDPIC checks the compatibility of the codes with the FADP. Submission is only mandatory if the code is to be used as justification for a data export under Art. 12 DPA. However, it is generally recommended for reasons of due diligence and liability.

Art. 11 can be compared to Art. 40 GDPR, where the requirements and legal consequences of codes of conduct or "rules of conduct" (Art. 40 GDPR) are similar. The codes established pursuant to Art. 40 GDPR thus provide a good point of reference for a possible implementation in Switzerland. If approval of the code for the European Union is desired, its requirements are authoritative.

Furthermore, the creation of codes of conduct promotes the internationalization of companies and the standardization of data protection within individual industries. Codes of conduct have been introduced on an international economic level for some time and support transnational, uniform and efficient corporate management. A code of conduct may therefore enable a company to meet international, legal and industry-specific requirements.

I. GENERAL

A. History of origins

1. Codes of Conduct in the Company

One of the key objectives of the total revision of the FADP was to expand and promote aspects of self-regulation. While Art. 11 aDSG only provided for a certification procedure (n. 22 f.), this is supplemented in the nDSG by the instrument of codes of conduct. These are intended to enable associations to concretize the data protection legislation, autonomously according to their 1

needs. The code of conduct introduces an economic and corporate concept ("code of conduct") into data protection law. As part of the compliance culture and "corporate governance", codes of conduct have been widespread in companies for some time. Now they are provided for and defined by law to support, concretize and guide data protection management systems.

2. Best practices

2 For the implementation of data protection, the BBl 2017 mentions so-called "Best Practices" for the implementation of data protection within the company. "Best practices" have long been common in the corporate governance environment and describe various models or methods for systematically optimizing procedures, processes or practices within the company itself. A procedure is standardized in order to achieve the optimal business process. The concept of "good practice" is also explicitly mentioned in Art. 5 para. 1 lit. g FADP, according to which the FDPIC itself should develop working tools to ensure compliance.

3 Best practices are also represented internationally; in Art. 4 para. 3 of the Ordinance on Data Protection Certifications (VDSZ), reference is made to existing international standards, which are statued as a benchmark for functioning data protection management systems. Indirectly, reference is also made here to good practice and codes of conduct. New Zealand and Argentina also refer to codes of conduct as best practices.

4 In Switzerland, too, there was a discussion in the consultation as to whether the FDPIC should itself issue data protection best practices, since the FDPIC has the task of advising federal bodies and private individuals and, in this context, also providing them with guidelines and working tools. These guidelines in the sense of best practices would thus also have influenced codes of conduct. Art. 58 para. 1 lit. g FADP can also be understood as a competence to develop guidelines that are similar to codes of conduct.

5 In the consultation, the business community in particular criticized that the FDPIC would exceed its executive powers, since such guidelines indirectly have an effect similar to that of a law. Therefore, it was finally decided not to grant the FDPIC these additional competences. Instead, the self-regulatory, individualized measures of the codes of conduct, which met with broad ap-

proval in the consultation, will be relied upon. "Best practices" can then be recorded in the code of conduct itself.

B. Norm Purpose

The purpose of the norm and the goal of the legislator is to create a framework of orientation and legal certainty for stakeholders and business associations. Through a self-regulatory measure, an association can concretize data protection requirements and flexibly adapt them to new data protection developments. 6

1. Promoting Data Protection Compliance

Codes of conduct are intended to promote data privacy compliance on two levels: on the first level, they provide a framework that creates legal certainty for various groups and trade associations. Data protection measures can now be regulated in a uniform manner. Autonomous concretization also offers opportunities for profession-specific adjustments and flexibility in the face of data protection developments. The latter, in particular, is likely to prove especially important as technological progress takes hold at breakneck speed. Of course, with these freedoms, the requirements of the DPA itself must always be observed and complied with. In this way, the new Data Protection Act can be better implemented in the long term. The addressees are to be encouraged to behave in accordance with the law. 7

On a second level, the law represents a relief for the FDPIC. It is becoming apparent that the adoption of codes by data controllers will lead to a standardization of data protection guidelines in the individual sectors. The FDPIC can base any audit of a controller on the code that has already been approved and only has to check whether it is being complied with. A potentially time-consuming search and compilation of data protection regulations scattered in regulations and statutes is now no longer necessary. The admissibility checks for data privacy compliance are no longer selective and case-by-case, but are based on a uniform set of rules defined by a code of conduct. 8

2. Regulated self-regulation

In the context of digitalization and global networking, intermediary service providers and network operators are gaining ever greater influence over the collection and processing of personal data. In addition, legislators are general- 9

ly only able to react to a particular technology after it has become socially and legally relevant.

10 "Regulated self-regulation" now builds a bridge between state legal norms (so-called "hard law") and private-law, sector-specific guidelines. Codes of conduct offer a prime example here. On the one hand, codes of conduct are provided for by law and their submission has certain legal consequences (n. 30 f.); on the other hand, the legislator gives associations considerable leeway as to how they wish to draw them up, tailored to their own environment. The example of the data protection code of the German Insurance Association, which is based on the analogous regulation of the GDPR, illustrates how this is specifically designed in practice. It sets out rules for handling personal data in typical insurance activities such as statistics, rate calculation and premium calculation. The rules for passing on data to various industry-specific categories of persons, such as reinsurers, intermediaries, competitors, etc., are also defined in more detail. In the case of the processing of creditworthiness data, on the other hand, reference is made to the law without issuing any further regulations.

11 Within the framework provided by law, the associations and federal bodies are free to orient themselves and regulate on an industry-specific basis. Knowledge and awareness of data protection are growing within the company. Contextualized, precise codes of conduct lead to greater legal certainty. Specified standards should also meet with greater understanding and approval in the respective industry. Providing companies with such practice-oriented measures is essential for contemporary, dynamic and, above all, compliant data protection law.

II. CONTENT

A. Code of Conduct

1. A Code of Conduct in General

12 A code of conduct is a formal document containing a set of standards. Its purpose is to define in concrete terms the behavior that is desirable in a company. It is well respected in the corporate culture and is considered an important pillar of good corporate governance and has become an indispensable part of the corporate culture.

However, a code of conduct is not part of a mandatory legal system. Companies decide for themselves whether or not they wish to adhere to a code of conduct. It is a voluntary commitment. Once the company has made a commitment, the code is in principle binding. It is up to the association to decide how and whether to enforce compliance with its code. The purpose of such a code is to guide the behavior of employees and managers, both within the company and toward outside third parties. This is achieved by standardizing and systematizing everyday actions and norms of behavior within and outside the company. 13

In this way, a code of conduct protects the company both internally and externally. Externally, employees are protected in their decisions and the company can better protect itself from external attacks by being able to demonstrate legal conformity, compliance and diligence through the code of conduct. Internally, a code of conduct contributes to a healthy, supportive corporate culture by setting standards, for example in the area of communication, to which employees must adhere. This strengthens trust among employees. 14

For the creation of a code of conduct in general, it is helpful to be guided by guiding questions. In particular, the following points should be clarified: 15

- How must I behave?
- What am I allowed to do and what is prohibited?
- When must I intervene in the behavior of a third party?
- Who is my contact person if I have questions, doubts or uncertainties?
- What happens if I violate the Code of Conduct?

The regulated points provide employees themselves with important information on desired behavior. It is therefore important to formulate a code of conduct clearly and comprehensibly and to adapt it to the company. The focus of the corresponding behavioral requirements is also the company- or industry-specific risks of the individual company. A valid code of conduct is regularly updated and confirmed by the management. 16

2. Codes of conduct in data protection

Data privacy codes of conduct refer to the standards of the FADP, expand on them and adapt them specifically to the industry concerned. These include, for example, sample templates for data protection declarations, high-risk data 17

processing in the company or guidance on the correct anonymization of data. The following is a list of guiding questions on possible areas of regulation. These questions are neither conclusive nor mandatory. However, they provide an overview of what should be included in a data protection-specific code of conduct.

- Is the data I am processing accurate?
- Who is affected in this data processing?
- What personal data is being collected?
- Which data is particularly risky?
- Can data encryption be adequately ensured?
- Do the data subjects have a right to information?
- Does the company have technical and organizational data protection measures in place?
- Requirements for the transfer of personal data abroad and the guarantee of Swiss data protection law safeguards
- Procedural modalities in the event of a conflict between data subjects and data controllers.

18 Such guiding questions can serve as a starting point for associations. However, in order to meet the individual requirements in a particular industry, more detailed explanations and careful documentation and reflection on the data collected on a day-to-day basis in that industry are needed. The needs of the companies belonging to the association, i.e. employees, shareholders, customers, etc., must be taken into consideration.

3. Concretization and self-regulation

19 The code of conduct pursuant to Art. 11 FADP thus applies the norms of the Data Protection Act to a specific situation. General formulations are concretized, made more precise and also made comprehensible to employees.

20 It must be at least as strict as the FADP, with at most stricter, industry-specific requirements. The association itself shall make any clarifications. This is intended to promote self-regulation and personal responsibility. State intervention is to be minimized. Furthermore, self-regulatory autonomy promotes a sense of responsibility on the part of those responsible.

The state should not actively intervene in the activities of individual industries or other associations, but leave it to them to flesh out the general clauses of the DPA according to their needs. This leads to clarity about the legal situation and precise formulations. 21

B. Distinction from certification

Article 13 FADP introduces data protection certifications that demonstrate the data protection compliance of a company's systems, products and services. The certification bodies act independently here within the framework of the instructions of the FDPIC. Thus, in contrast to the codes of conduct, the FDPIC does not monitor itself, but only exerts an indirect influence by issuing regulations on the recognition of a certification (Art. 13 FADP). The VDSZ, which elaborates and specifies the requirements for certification bodies, serves as a guide. 22

Data protection certifications serve to selectively evaluate the data protection conformity of a system or individual processing operations. Codes of conduct, on the other hand, describe all or most of the specifications of a company's processing activities, or how they should be handled on an industry-specific basis. In other words, codes of conduct provide a general framework of guidance, while data protection certifications confirm the compliance of an individual operation. Certifications are critical to implementing data privacy compliance in practice. While codes of conduct define the desired behavior analogous to the law in theory, certification serves as an instrument in the implementation of the rules in everyday life. 23

Certifications and a code of conduct are therefore by no means mutually exclusive. It would therefore seem to be expedient for a company to obtain selective data protection certifications from qualified bodies in addition to a code of conduct. This is especially true if the specific data processing appears to be atypical, new or particularly risky for the company concerned. 24

III. OPINION OF THE FDPIC

Professional, industry and business associations that are authorized by their statutes to protect the economic interests of their members are authorized to draw up a code that can be submitted to the FDPIC for review. 25

26 Individual data controllers or order processors cannot submit their codes of conduct. This is justified by the fact that Art. 11 DPA aims at a certain standardization within individual industries.

27 By contrast, associations and organizations that have a certain national or at least regional significance are probably entitled to submit their codes of conduct, analogously to Art. 89 CCP. A cantonal association will regularly meet this requirement.

28 The legal form of the association is in principle not decisive. However, individual companies, especially stock corporations, are excluded because they lack members. For the same reason, foundations are not eligible to submit applications. Consumer organizations and associations of affected persons lack the prerequisite to represent the economic interests of their members.

29 Federal bodies are always entitled to make submissions. This is justified by the numerous legal requirements and different tasks imposed on the various bodies.

A. Legal scope of a submission

30 According to Art. 11 DPA, the submission of a code of conduct for associations and companies is in principle optional. This principle is relativized by Art. 12 DPA. There, the obligation is provided to submit the code to the FDPIC for approval if a data export is to be justified by the code (Art. 12 FADP). The principle of voluntariness, which applies both to the creation of the codes of conduct and to the submission of these to the FDPIC, is now breached by this constellation of foreign data transfers. This can be justified with a higher security standard, which results almost automatically from the far more risky international data exchange. This is to ensure that the code of conduct guarantees sufficient data protection. This is underlined by a "binding and enforceable" obligation on the controller or the processor in the third country to comply with the Code of Conduct (Art. 12 para. 3 DPA). It becomes binding through measures that comply with the applicable law in the respective third country such as anchoring the codes in the statutes of the controller.

31 A template offers itself as advantageous from the point of view of due diligence and liability within the represented companies. This is because only an official statement can sufficiently prove that the code is compliant with data protection law. A confirmed code of conduct is direct evidence that the com-

pany is following clear regulations that comply with the DPA in terms of data protection law.

Since codes of conduct are self-regulatory measures that have an effect on the respective industries and professions for which they were created, they represent a legal concretization for practice. They therefore also offer the possibility of generally accepted standards of conduct being formed in a particular area. This greatly simplifies compliance with data protection for companies; in this way, they would have a concrete guide and orientation standard for their own area of activity. 32

B. Consequences of the Opinion

The FDPIC is obliged to issue an opinion. The opinion is not an order, but a real act and is therefore in principle not binding. Nevertheless, a confirmation by the FDPIC may have different consequences. 33

A positive opinion can always be expected if the code provides for compliance with all provisions of the DPA. The yardstick for the opinion is therefore the law. The FDPIC may add suggestions for improvement and recommendations to the opinion, especially in the case of a lack of concretization or incorrect application of the law. According to Art. 59 FADP, a fee is charged to private individuals for an opinion. Pursuant to Art. 44 Para. 1 and 2 FADP, the fee is in principle calculated on the basis of the time spent, with the hourly rate being CHF 150 to CHF 250, depending on the function of the executive staff. 34

After a positive opinion, it can be assumed that the conduct in compliance with the Code will not result in any sanctions or administrative measures, i.e. that the data processing activities in compliance with the Code are data protection compliant. 35

Also, a data protection impact assessment (DPA) can be dispensed with if the FDPIC issues a positive opinion and the code of conduct is based on a DPA that is still up to date and protects the personal and fundamental rights of the data subject (Art. 22 para. 5 lit. a and lit. b FADP). An approved code of conduct is an alternative or an exception to the obligation to prepare an impact assessment. For risk analyses of a company, it makes sense to link DSFAs and codes of conduct in order to minimize any risk under data protection law as far as possible. 36

37 The consequences of an incorrect statement are now questionable. In this case, the private individual believes that his or her own code of conduct complies with data protection law. Therefore, processing based on this will not result in any administrative measures or sanctions. If the private individual nevertheless violates data protection on the basis of false information, he or she may still risk sanctions. This is because the requirements for valid protection of legitimate expectations are strict. In particular, sufficient specific wording in the Code is required for its acceptance, and the facts that have occurred must be congruent with what has been provided for.

38 Art. 11 does not provide a rule for the case that different associations establish different rules in their codes for the same or overlapping facts. Provided that the competing drafts meet the above requirements in themselves, the FDPIC will give the codes a favorable opinion.... However, it is free to point out contradictions in its opinion, since the unification of data protection rules is included in the purpose of the norm.

39 Thus, the situation may arise where a controller who is a member of different associations undertakes to comply with conflicting codes of conduct. Since the FDPIC will only issue a positive opinion if the legal requirements of the DPA are met, this will not bring it into conflict with the law. Nevertheless, it is advisable to adhere to only one code of conduct in order to keep the company's internal data protection principles stringent.

IV. SELF-REGULATION UNDER ART. 40 GDPR

40 The GDPR also has a standard for self-regulation and concretization of data protection. Art. 40 GDPR speaks of the "elaboration of rules of conduct" which are drawn up by associations or similar bodies. Here, too, the focus is on self-regulatory measures by companies. The rules are to be considered as a supplement to, and not a substitute for, legal regulations.

41 The requirements for and legal consequences of codes of conduct and those of rules of conduct are similar. Thus, codes of conduct are also submitted to a supervisory authority for an opinion, which is also published. According to the general accountability obligations pursuant to Art. 5 para. 2 GDPR, the controller must comply with the principles of data protection law and must also be able to prove this. The drafting of rules of conduct facilitates this. Art. 40 GDPR specifies the requirements for codes of conduct in more detail

(para. 2 lit. a-k) and provides for various procedures to ensure secure data protection within all Member States, also through implementing acts by the Commission.

The GDPR also promises companies advantages and simplification of proof if they voluntarily comply with approved codes of conduct. 42

In contrast to Switzerland, a code of conduct that has been submitted to the European Data Protection Board by the national supervisory authority (Art. 63 GDPR) and confirmed by them can also have effect at the Union level. Rules of conduct can be declared valid throughout the Union by means of a declaration of general applicability (Art. 40 para. 9 GDPR). A code of conduct that is based only on the DPA and has been submitted only to the FDPIC has no guarantee of transnational data protection compliance. It seems advantageous that (Swiss) associations operating in the Union also submit their codes to the competent bodies in the EU or that controllers adopt already approved codes of conduct. This facilitates market access and at the same time leads to an increase in efficiency, as less time and resources have to be spent on bureaucratic and regulatory processes. In addition, a harmonization of standards is created, which particularly benefits companies that operate both in Switzerland and in the EU. 43

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 12 FADP

A commentary by Ursula Sury / Jael Inauen

SUGGESTED CITATION

Ursula Sury/Jael Inauen, Commentary to art. 12 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Sury/Inauen, art. 12 FADP N. XXX.

Art. 12 Record of processing activities

[1] The controller and the processor shall each maintain a record of their processing activities.

[2] The controller's record shall as a minimum contain:

a. the identity of the controller;

b. the purpose of processing;

c. a description of the categories of data subjects and the categories of processed personal data;

d. the categories of recipients;

e. if possible, the retention period for the personal data or the criteria for determining this period;

f. if possible, a general description of the measures taken to guarantee data security under Article 8;

g. if the data are disclosed abroad, details of the State concerned and the guarantees under Article 16 paragraph 2.

[3] The processor's record shall contain information on identity of the processor and of the controller, the categories of processing carried out on behalf of the controller, and the information mentioned in paragraph 2 letters f and g.

[4] The federal bodies shall notify the FDPIC of their records of processing activities.

[5] The Federal Council shall provide exceptions for legal entities that have fewer than 250 employees and whose data processing poses a negligible risk of harm to the personality of the data subjects.

CONTENT

IN BRIEF

Art. 12 FADP describes the obligation for federal bodies and private data controllers and order processors to keep a register of processing activities. Data should be recorded throughout its life cycle in the company. A directory contains at least:

- the identity of the persons in charge
- the categories of personal data processed
- the purpose of the processing
- if possible, the retention period or at least the criteria for determining this period
- the recipients of the processed data
- measures to be taken in accordance with data protection law
- requirements for the disclosure of data abroad

The directory does not include categories of personal data that the company does not process at all and guarantees for the disclosure of data abroad if no data export is carried out. Also data that would have to be obtained first only with disproportionate effort.

Finally, companies with fewer than 250 employees (SMEs) are legally exempt from the obligation to create and maintain a processing directory due to administrative relief. Since a directory of processing activities serves the purpose of internal clarification of the data processed as well as compliance with liability and due diligence obligations, it is recommended for every company to keep a directory.

The directory of processing activities, which is not bound by any formal requirement, is recorded within the company and offers, among other things, a possibility for regulated self-regulation in addition to codes of conduct and certifications. On the one hand, the company gains clarity about the data it processes; on the other hand, the FDPIC will also be guided by data processing directories from the entry into force of the revised DPA in order to check data protection compliance.

I. GENERAL

A. Overview

According to the provisions of the Data Protection Act (DPA), a directory of processing activities is an important tool for ensuring compliance with data protection regulations. It provides a systematized overview of data processing activities and serves as an obligation for both federal bodies and private individuals. It provides information about the origin and purpose of the data, storage aspects, as well as applied security measures and data transfer, possibly abroad. The standard replaces Art. 11a aDSG i.V.m. Art. 11 VDSG and specifies and extends the obligation to keep a register of data collections. Responsible parties must independently determine and systematically document the data collected internally. In the register, there is thus an increased focus on the documentation obligation and the data processing activities. However, a register of processing activities must be distinguished from a register of data collections and has additional content requirements (cf. n. 6). 1

Thanks to the register of processing activities, organizations have important information of their digital data, they have a clear and up-to-date overview. This benefits both the FDPIC, whose review of a company's data protection compliance is simplified, and the company itself. 2

B. History of origins

Pursuant to Art. 11a aDSG, the "Commissioner", i.e. the FDPIC, kept a publicly accessible register of data collections ("Register"). While federal bodies had to register all data collections with the FDPIC (Art. 11a para. 1 aDSG), private individuals were only required to register if they either regularly passed on personal data to third parties (Art. 11a para. 3 lit. b aDSG) or if they processed personality profiles or data requiring special protection (Art. 11a para. 3 lit. aDSG). Art. 11a para. 5 aDSG exempted several holders of data collections from a notification obligation to the FDPIC, including holders of a data protection certification or companies with a data protection officer. 3

Art. 11a FADP did not itself specify the requirements for a register of data collections, but Art. 11 FADP did. According to this, the register had to contain descriptions of the internal organizational structures and the data processing and control procedures. Evidence about the planning, implementation and 4

operation of the data collection as well as the IT resources used also had to be listed. These clarifications applied only to data processing operations subject to reporting requirements.

5 However, the term "list of processing activities" goes beyond a brief overview of collected data. It additionally includes information on what is done with the data, how it is collected, and where it is transferred. Registers overlap with a directory of processing activities in terms of content, but focus more in-depth on the (company's) internal structure, planning and management. The current FADP no longer includes the term register of data collections, as it has been replaced by directory of processing activities.

6 Art. 12 DPA is more comprehensive and requires additional information such as the identity of the controller, the purpose of processing, a categorization of both the personal data processed and the intended recipients, the retention period and concrete measures to ensure data security. Although much overlaps with Art. 11 VDSG, the requirements are much more detailed, which should also simplify the creation of a directory. The former general documentation obligation, i.e. an obligation to report data collections, is also replaced by the data processing directory.

7 With the entry into force of the new FADP, according to Art. 12 FADP, private individuals and federal bodies must create a directory of processing activities. However, it is exclusively federal bodies that must submit their processing directory to the FDPIC (Art. 12 para. 4 FADP). The obligation to keep a register, however, also applies to private individuals. The directory of processing activities makes it possible to better control one's own data. The directory of processing activities is now classified under the general data protection provisions.

C. Purpose of the norm

8 Art. 12 FADP is an obligation standard for data controllers and processors. The purpose of the norm is to increase transparency in the processing of data. This is ensured by the stricter requirements for the directory (Art. 12 FADP) than for its former counterpart, the register of data collections (Art. 11a aDSG). With precise minimum information, data controllers have a clear orientation framework as to which data belong in a directory. In this way, data processing is recorded in a standardized manner. It becomes easier for the person re-

sponsible to keep track of the collected data within the company. On the one hand, he or she can adequately fulfill the duty to inform and, on the other hand, satisfactorily comply with the right to information.

A systematic collection of data and information is generally beneficial for companies, not only in the area of personal data. A materials directory or a record of information that is subject to a confidentiality obligation enables the company to always have an up-to-date, correct and simplified overview of the internal flow of information. Here, too, the principle applies that the systematic collection and gathering of data represent an important digital asset. 9

The standard also represents a simplification for the FDPIC. It benefits from the standardization of the directory, since all relevant categorizations or edits are now directly available to it. In the future, the FDPIC will ask for the directory first during an investigation. Nevertheless, failure to maintain a directory does not lead to an immediate sanction. However, providing false information or refusing to assist in an investigation by the FDPIC remains punishable, as it already is under current law. 10

II. CONTENT

A. Content of a processing directory

Art. 12 provides for some minimum content requirements for this directory, as follows: 11

- Who is responsible, Art. 12 para. 2 lit. a FADP.
  The person responsible is the person who decides on the purpose and means of data processing. If there are several persons responsible, all of them must be listed.
- What is the purpose of processing?, Art. 12 para. 2 lit. b FADP.
  The purpose can vary; the decisive factor is the goal pursued with data processing. As a rule, the person who initiates the processing also decides on its purpose.
- Which persons and what type of personal data are processed (categorizations), Art. 12 Para. 2 lit. c FADP.

Categories of data subjects are typified groupings such as "consumers" or "employees". Categories of "processed personal data" refer to the types of data processed, such as personal data requiring special protection.

- Who is the recipient of the processed data?, Art. 12 Para. 2 lit. d FADP.
  The recipients of the processed personal data are also categorized, such as supervisory authorities.
- How long is personal data kept or how can this duration be determined?, Art. 12 para. 2 lit. e FADP.
  In particular, it is about the archiving periods of collected data. If there is no legal basis or no longer a defined purpose for storing the collected personal data, it must be deleted or anonymized (Art. 6 para. 4 FADP).
- What measures are taken to ensure data security according to Art. 8, Art. 12 para. 2 lit. f FADP?
  Reference is made to the fundamental principles of data protection and data security. These include, in particular, the integrity of the data collected, appropriate technical and organizational measures and "privacy by default" and "privacy by design".
- What measures must be taken to disclose data abroad?, Art. 12 para. 2 lit. g FADP.
  In addition to the legal measures (cf. Art. 16 ff. FADP), this also includes contractually agreed standard clauses in contracts and internationally defined, sector-specific standards (cf. Art. 11 FADP in conjunction with Art. 12 DPA).

12 Art. 12 is very precise and detailed, but still allows a certain degree of flexibility. For example, the directory should only include information about which there is sufficient certainty in terms of content. A description should only be given if the activities can be described in sufficiently concrete terms. Sometimes, for example, the exact retention period cannot be specified. Thus, only the criteria for the retention period need to be specified. Due to this broad definition, it would be desirable to develop sector-specific guidelines that could be applied uniformly in the respective industries. Both the work of the companies and that of the FDPIC would be facilitated. By developing sector-specific guidelines that could be applied uniformly in the respective industries, this broad design could be made more concrete. This would help both the responsible parties and the FDPIC to facilitate their work. The guides

would provide clear instructions to the officers and help them better understand and implement the data protection requirements in their industry. At the same time, it would allow the FDPIC to conduct more consistent privacy review and enforcement across industries.

B. Form of a Directory

Article 12 DPA does not specify in detail how exactly data processing activities are systematized in the directory of processing activities. There are also no formal requirements. A directory can be a simple Word or Excel document or a complex IT solution. The directory can be kept in a decentralized manner and its maintenance can even be delegated. 13

C. Obligations of private persons

1. Legal requirements

In principle, all companies and other private persons in charge are obliged to keep a register of processing activities. This results from the fact that almost all private individuals collect and also process personal data in their economic or non-profit activities. 14

2. The processor

The register of processing activities must be kept by the controller and the processor (Art. 12 para. 1 FADP). The order processor is a person who processes data on behalf of the controller (Art. 5 lit. k FADP). An example is the IT service provider who hosts a website or an employee who takes contact data from customers. A data controller, on the other hand, is the person who decides on the purpose and means of data processing (Art. 5 lit. j DPA). 15

Each company is exclusively responsible for the data processed internally. An order processor (Processor), is not obliged to maintain a processing directory for the data controllers. Data of the person in charge, also called "controller", does not have to be listed. This is only the responsibility of the controller itself, which is responsible for its collected data - for example, customer data. Otherwise, this would lead to excessive collection of personal data. This requirement would be almost impossible for companies to enforce. One would have to collect the entirety of all personal data of the client for every service. A proliferation of directories and an associated loss of an overview of the data 16

collected would be to be expected. The directory of the order processor therefore contains less information than that of a data controller. On the other hand, this directory creates transparency in the contractual relationship between the data controller and the data processor by stipulating that both parties must be clearly identifiable. The relevant framework conditions are set out in Art. 9 FADP, which clarifies data processing by a processor.

3. Legal exceptions: SME

17 Art. 12 para. 5 provides an exception for companies that employ fewer than 250 people and do not process high-risk data. These are exempt from the obligation to keep a register of processing activities. High-risk data processing activities are those that are more likely to result in a violation of privacy (invasion of privacy, medical data, sexual orientation, religious denomination, etc.). This exception is also mentioned in Art. 24 of the Ordinance on Data Protection (DPA). However, Art. 24 does not contain any more detailed provisions regarding the legal exception. It is merely repeated that SMEs are exempt from a directory obligation unless they process personal data requiring special protection on a large scale (lit. a), or carry out high-risk profiling (lit. b). The concept of high risk is used analogously to that in Art. 22 para. 2 DPA.

18 The aim of this exception is to reduce the administrative burden on smaller companies. Not only the size of a company is taken into account, but also the respective data that is processed and which risks are associated with it. SMEs are also affected by the sanctions provided for in the DPA, and compliance with data protection principles is required of SMEs. This results in an indirect documentation obligation for companies, even though they are not legally obligated to create a processing directory. This is because the FDPIC will deal with the data protection measures within an SME regardless of whether a processing activity directory exists or not. The SME must therefore present the processed data anyway. A directory provides better protection for the company in terms of liability and due diligence.

19 If half of all data processed are high-risk, they fall under the requirements of the enhanced documentation obligations, but may still not be required by law to be listed in a directory of processing activities. Liability and risk for any data protection violations are always borne by the data controller. The creation of a processing directory is therefore recommended if high-risk data processing is carried out, regardless of the scope.

4. Contractual requirements

It is also possible to provide for the maintenance of a directory by contract. Although such an obligation is dispositive, it could develop greater significance depending on the industry. Indeed, by keeping a processing directory, a company can protect itself not only from the FDPIC and the legal requirements, but also from other companies that may be partners as well as customers. If a data controller knows how the data processor processes and stores data and by what means, this promotes trust and cooperation between both parties. Furthermore, enforcing a practice where directories are contractually agreed upon allows for independent elaboration of directories that are adapted to the respective economic sectors and meet the specific data protection challenges in the affected work areas. 20

In contracting directories, certain aspects need to be taken into account and various hurdles may arise. Implementing such a practice allows companies to independently create directories that meet the specific requirements and data privacy challenges of their respective economic sectors. 21

One of the hurdles is drafting contracts to meet the precise requirements of data protection law. Clear agreements must be reached on the type of data collected, the purpose of the data processing, the retention period, security measures and other relevant data protection aspects. It is important to ensure that contractual arrangements comply with the law and that the rights of data subjects are adequately protected. 22

In addition, figuring out sector-specific directories can be challenging. Different economic sectors have different data privacy requirements and specific areas of work that may present specific data privacy challenges. Companies must be able to identify and incorporate these specific requirements into their directories in order to comply with data protection regulations. 23

Collaboration among the parties involved, such as the companies, privacy experts, and regulators, as appropriate, can be helpful in successfully implementing contractual agreements and carving out industry-specific directories. 24

D. Obligations of Federal Bodies (Art. 12 para. 4 FADP)

25 According to Art. 5 lit. i FADP, federal bodies are not only authorities or central administrative bodies, but any authority or service of the federal government, as well as persons who fulfill public tasks of the federal government.

26 According to Art. 12 para. 4 FADP, federal bodies have the obligation to report their directories of processing activities to the FDPIC. The FDPIC himself keeps a register of the processing activities of federal bodies pursuant to Art. 56 FADP, which is published.

27 Even before the revision of the Data Protection Act, federal bodies were obliged to record organizational structures and data processing procedures in a register of data collections. This implicitly included the name and address of the responsible federal body, a designation of the data collection, the body responsible for the right of access, and the legal basis and purpose. Categories of personal data processed, the recipients, as well as the participants in the data collection were recorded (Art. 11a of the old FADP). Registers of data collections also had to be notified to the FDPIC for registration in accordance with Art. 11a aDSG. In general, federal bodies were subject to more stringent requirements. The Federal Council also had the power to determine special regulations for data protection (Art. 16 para. 2 aDSG).

28 There is thus no significant change in the obligations for federal bodies. Rather, Art. 12 DPA acts as an extension to private persons of the obligations that previously applied only to federal bodies. A register of processing activities must therefore be kept for federal bodies without exception. A register that already exists and is kept accurate and up-to-date already meets many of the requirements for a directory, which is why there is often little or no need for changes to implement the current Data Protection Act. The most significant change is that instead of being divided by data collection, it is now divided by data processing.

E. Implementation of Data Protection Compliance

29 In principle, a directory of processing activities is not intended for data subjects, but is mainly used for internal control of a company as well as for investigation by the FDPIC. By creating a directory of processing activities, data controllers gain clarity about their own data processing activities. Keeping a

register simplifies the implementation of certain obligations and fulfillment of data subject rights, such as the right to information (Art. 25 FADP).

1. Information obligations

Art. 19 FADP provides for an information obligation for the controller and the processor when obtaining personal data. At a minimum, the identity and contact details of the data controller, the purpose of processing and, if applicable, the recipients of the personal data procured must be disclosed. With the data protection revision, the duty to provide information was generally expanded. Prior to the revision, it applied only to the acquisition of particularly sensitive data or personality profiles, whereas it now applies to every acquisition of personal data. 30

With a directory of processing activities, the data subject is informed efficiently and uniformly about the collection of his or her own data. Furthermore, the purpose, the means and, under certain circumstances, the retention period can also be communicated precisely, since this information is itself already contained in the directory. In this sense, the directory represents an administrative relief for companies, with which external information processes towards data subjects or also the FDPIC can be designed more simply and efficiently. This more efficient design results in several advantages. First, the data controller reduces the administrative burden, as it no longer has to create and send a separate notification for each individual data processing. Instead, it can refer to the directory, which already contains all the necessary information. Second, communication with data subjects is standardized. Since all information is contained in the directory, all data subjects receive the same information about purpose, means and retention period, resulting in more consistent and transparent communication. Third, the directory also facilitates cooperation with external parties, such as the Federal Data Protection and Information Commissioner (FDPIC). When the FDPIC requests information about data processing, the company can simply provide the directory instead of having to prepare separate reports for each individual data processing operation. 31

2. The Right of Access

The right to information under Art. 25 DPA is a data subject right that an individual can assert under data protection law. With the right to information, the 32

lawfulness of a data processing can be checked and the data subject has the right to demand an authorization or deletion of the data. According to Art. 25 FADP, the data subject shall receive all information about his or her own personal data so that he or she can assert his or her rights, namely the identity of the controller, the purpose of the processing and the processed personal data itself. The rights that may be asserted thereafter are, for example, the right to rectification of the incorrectly collected personal data or the elimination of the latter (Art. 32 FADP).

33 A register of processing activities ensures and supports the right of access, as it fully encompasses the information that must be communicated to the data subject pursuant to Art. 25 FADP. With a properly maintained directory, the data subject receives complete, uniform and correct information about the data collected. Adequate information is guaranteed and security is increased for both parties, since the company has a better overview of the collected data and runs less risk of violating data protection regulations. If the directory is not correct, this can lead to the controller not recording information about the data processing correctly or taking inadequate security precautions. This creates a risk of data breaches and may result in legal consequences.

F. Data held abroad (Art. 12 para. 2 lit. g).

34 According to Art. 12 para. 1 lit. g FADP, when data is disclosed abroad, the respective country must be indicated, as well as the guarantees according to Art. 16 para. 2 FADP. These provisions ensure that the data subject is informed about the transfer of his or her personal data abroad and that appropriate data protection measures are taken. The directory of processing activities can include these requirements by stating the exact purpose of the data transfer abroad and naming the destination country. In addition, the directory should also contain information about the safeguards taken in accordance with Article 16 (2) FADP, in order to reassure the data subject that adequate protective measures are in place. It is important that the data subject is informed in a clear and comprehensible manner that his or her data will be transferred abroad and what protective measures have been taken in the process. This ensures the data subject's right to information and protects his or her privacy. These tighten the data protection requirements in the case of cross-border data processing and disclosure. In principle, personal data may only be disclosed abroad if there is a decision by the Federal Council that this country it-

self guarantees adequate data protection. Which countries have an adequate level of data protection is determined by the Federal Council and published in Annex 1 of the Data Protection Ordinance. Inadequate protection is provided by, among others, Russia, a large part of African and South American countries, and all of Asia (with the exception of Israel).

Article 16 para. 2 FADP requires either an international treaty, contractual data protection clauses, specific guarantees approved by the FDPIC, standard protection clauses, or binding internal company data protection specifications that are also approved by the FDPIC (Art. 16 lit. a-e FADP). These now apply in the case of data disclosure not only if the country itself does not ensure adequate protection, but for any foreign disclosure. 35

III. COMPARISON WITH EU LAW

Article 12 DPA, like several other articles after the total revision, has some parallels to the requirements of the GDPR. For example, Art. 12 was drafted in analogy to Art. 30 GDPR. Both in Art. 30 GDPR and in Art. 12 FADP, public bodies as well as private individuals must keep a register. In it, the identity of the controller and the commissioned processor must be stated. Both provisions require information on the purpose of processing, the categorization of personal data processed and recipients, the guarantees for transfer abroad, the retention period and technical and organizational measures regarding the implementation of data security. The exemption from the creation of a data processing directory is also preserved in both Art. 30 GDPR and Art. 12 DPA. The statement "if possible" (para. 1 lit. f and g) allows for some flexibility, as in the Swiss Data Protection Act. The content of a directory is not defined equally and strictly for every company, but is based on how precisely the processed data can be circumscribed in the first place. Thus, it is not always possible to say with certainty when data will be deleted, nor do all companies follow analogous and generally accepted technical and organizational measures. A data directory should also be able to adapt to the respective activity. 36

Differences between the provisions arise sporadically in the formulations and explanations. Analogous to the FDPIC in Switzerland, the data protection supervisory authority in the EU assumes similar functions such as monitoring compliance with the GDPR or the DPA. Article 30 of the GDPR additionally requires that the identity of the data protection officer be stated in the directory, if one exists in the company. The transfer abroad must be specifically 37

stated according to DSGVO and the form of a directory must be in writing. Public bodies or private individuals also have an obligation under Union law to make the directory of processing activities available to the supervisory authority upon request. Cooperation in good faith with public authorities is generally required.

38 In addition to Art. 30 GDPR, Art. 24 of Directive 2016/680 elaborates on the content of a register of processing activities. It is only worth mentioning here that Art. 24 of the Directive also provides for the use of profiling (Art. 24 para. 1 lit. e) and the indication of the legal basis for the transfers of personal data (Art. 24 para. 1 lit. g) in a processing register. This is not provided for in the Swiss regulation, but can be covered by supplementary information in the purpose of processing or the categorizations of personal data processed.

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 14 FADP

A commentary by Martin Steiger

SUGGESTED CITATION

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

Short citation: OK-Steiger, N. XXX zu Art. 14 DSG.

Section 2
Data Processing by Private Controllers with Registered Office or Domicile Abroad

Art. 14 Representative

[1] Private controllers with registered office or domicile abroad shall appoint a representative in Switzerland if they process the personal data of persons in Switzerland and the data processing meets the following requirements:

a. The processing is connected with the offer of goods or services or the monitoring of the behaviour of persons in Switzerland.

b. The processing is on a large scale.

c. The processing is carried out regularly.

d. The processing poses a high risk to the personality of the data subjects.

[2] The representative shall serve as the contact point for the data subjects and the FDPIC.

[3] The controller shall publish the name and the address of the representative.

CONTENT

IN A NUTSHELL

Art. 14 FADP regulates the obligation to appoint a data protection officer in Switzerland by private controllers based abroad. The obligation exists only under certain cumulative conditions and is likely to apply in practice to only a few controllers. The representation is intended to serve as a point of contact for data subjects and the FDPIC to facilitate enforcement of the FADP against certain controllers abroad. Controllers must publish the name and address of their representation, for example as part of the privacy statement on their website.

I. GENERAL

A. Purpose

1 Controllers without a registered office in Switzerland must designate a representation in Switzerland under certain conditions, which are rarely met. The formulation of these conditions leads to legal uncertainty as to when they are fulfilled at all.

2 The obligation can be justified by the broad territorial scope of the FADP, since the FADP applies to all matters that have an impact in Switzerland, even if they are initiated abroad (Art. 3 para. 1 FADP). The obligation to designate a representative is intended to improve the practical enforceability of the FADP, analogous to the EU data protection representation under Art. 27 FADP.

B. History of origins

3 During the parliamentary debate, the FADP was amended to include data protection representation pursuant to Art. 14 and 15 FADP. The two articles form in the 2nd chapter with the "General Provisions" the 2nd section "Data Processing by Private Holders with Seat or Residence Abroad". The structure is based on the EU data protection representation according to Art. 27 DSGVO. Accordingly, the data protection representative can be a legal entity or a natural person. The Data Protection Regulation (DSGVO) does not mention representation.

The data protection representation touches on political demands for a mandatory jurisdiction for large foreign Internet platforms, such as social media platforms in particular, in criminal and civil law matters, but does not implement them. A possible implementation of these demands for a mandatory domicile of service could be brought by a consultation draft of the Federal Council on the regulation of large communication platforms announced for 2024, according to which such platforms should designate a contact point and a legal representative in Switzerland. 4

II. OBLIGATION TO APPOINT A DATA PROTECTION OFFICER (PARA. 1)

Article 14 para. 1 FADP sets out the conditions under which data controllers must exceptionally designate a data protection officer in Switzerland. Unlike the EU data protection representation under Art. 27 para. 1 and 2 DSGVO, there is no general obligation with exceptions. Accordingly, the number of data controllers concerned is likely to be small. 5

The FDPIC may order or decree the designation of a representative as an administrative measure (Art. 51 para. 4 FADP). 6

Violation of the obligation to designate a representative is not covered by the penal provisions under Art. 60 et seq. FADP. Failure to comply with an order of the FDPIC to designate a representative may be punished by a fine (Art. 63 FADP). 7

A. Personal scope

The obligation to designate a representative applies to private data controllers (Art. 5 lit. j FADP) with their registered office or place of residence abroad if they process data of individuals in Switzerland (Art. 5 lit. a and b FADP) and the processing meets the cumulative requirements under Art. 14 para. 1 lit. a-d FADP. In contrast to the EU data protection representation, the obligation in Switzerland applies only to data controllers and not also to data processors. 8

B. Material scope of application

1. in connection with the offer of goods or services or with the observation of the behavior of persons in Switzerland (lit. a).

9 Art. 14 para. 1 lit. a FADP is based on the alternative requirements for the territorial scope of the FADP by offering or observing conduct (Art. 3 para. 2 FADP), rather than with the active principle under Art. 3 para. 1 FADP. Accordingly, the requirement only applies if an offer or observation of behavior has an effect on a factual situation in Switzerland. A mere connection with an offer or a behavioral observation is not sufficient.

10 The first cumulative requirement under Art. 14 para. 1 lit. a FADP is met, on the one hand, if the processing of personal data is related to the offer of goods and services to persons in Switzerland. According to recital 80 to Art. 27 para. 3 DSGVO, an offer that is free or free of charge is sufficient.

11 The accessibility of offers alone, e.g. in an app on a social media platform or via a website, is not sufficient. Concrete indications are required that an offer is actually directed at persons in Switzerland. Possible indications are, for example, content in Swiss national languages, delivery options to Switzerland, price information in Swiss francs, prices with indication of Swiss VAT, publication of a Swiss telephone number or the use of a Swiss top-level domain (.ch or .swiss).

12 By contrast, the first cumulative requirement under Art. 14 para. 1 lit. a FADP is met if the processing is carried out in connection with the observation of the behavior of persons in Switzerland as an alternative to the offer or simultaneously with the offer. The term "behavioral observation" is defined in terms of Art. 3 para. 2 DSGVO. The mere recording of access to an online service or website is therefore not sufficient. There must be actual targeting of individuals in Switzerland or the observation must lead to profiling with respect to the data subjects in Switzerland. Thus, the provision is likely to apply to providers of internet platforms such as ByteDance, Google and Meta, but not, for example, to operators of online stores, as long as their business model is not data-centric and profiling of users is only carried out to the usual extent for their own marketing purposes.

2. comprehensive processing (lit. b)

The second cumulative requirement under Art. 14 para. 1 lit. b FADP is met if the processing of personal data is extensive. What is meant by "extensive processing" is not explained in the law. 13

Art. 22 para. 2 lit. a FADP cites the extensive processing of personal data requiring special protection as an example of high-risk data processing, but also does not explain what constitutes "extensive". Possible criteria would be a large number of data subjects in Switzerland or a large amount of data about individuals in Switzerland. 14

3. regular processing (lit. c)

The third cumulative requirement under Art. 14 para. 1 lit. c FADP is met if there is regular processing of personal data. What is meant by "regular processing" is not explained in the law. 15

It is obvious that there is no regularity if the controllers process personal data only occasionally or for a limited period of time. On the other hand, regularity is likely to exist if a controller regularly processes personal data in order to carry out its activities (example: offering through online store) or pursuing a data-centric business model (example: monitoring through social media platform). 16

4. high risk for the personality of the data subjects (lit. d).

The fourth cumulative requirement under Art. 14 para. 1 lit. d FADP is met if the processing involves a high risk to the personality of the data subjects. This requirement corresponds to the risk-based approach in the FADP, but without mention of the fundamental rights of data subjects (see also, for example, Art. 5 lit. g FADP: high-risk profiling; Art. 22 para. 1 and para. 2 FADP: data protection impact assessment; Art. 24 para. 1 FADP: notification of data security breaches). The lack of mention of the fundamental rights of data subjects is likely a legislative oversight given the other mentions in the FADP. 17

Processing of data that poses a high risk to the privacy of data subjects is likely to be rare in practice. Data protection impact assessments therefore rarely reveal a high risk or such a risk is eliminated by appropriate measures. 18

III. FUNCTION OF THE DATA PROTECTION OFFICER (PARA. 2).

19 The Data Protection Officer serves as a point of contact for data subjects and the FDPIC. Data subjects and the FDPIC may contact the representative, but are not required to do so. The representation is legally considered to be authorized to serve notifications.

20 The representation is thus an alternative point of contact for data subjects and the FDPIC as a special authority in addition to the controller. If the controller has appointed a data protection officer, there are a total of three different alternative points of contact (Art. 10 para. 1 and 2 FADP).

21 The data protection officer of a data controller cannot simultaneously act as the data protection officer of the same data controller. Such representation would be incompatible with the independence of the data protection advisor (Art. 10 para. 3 lit. a and b FADP).

22 For data subjects, representation as a point of contact has the particular advantage that they can address data protection concerns directly to the data controller in Switzerland, especially within the framework of their rights under Art. 25 et seq. FADP. In the case of data file owners without representation in Switzerland, data subjects must, for example, address requests for information to the respective data file owners or their data protection officers at their registered office or place of residence abroad.

23 For the FDPIC, representation as a point of contact has the particular advantage that it does not have to reach data controllers abroad by way of international mutual legal assistance.

24 The law does not specify the languages in which data subjects can contact the representation. In the case of an offer-related representation, data subjects should be able to contact the representation at least in the language of the offer or in one of the languages of the offer. The restriction to national languages does not seem appropriate. The FDPIC should be able to contact the representation in one of the four official Swiss languages (Art. 33a APG by analogy).

IV. VOLUNTARY APPOINTMENT OF A DATA PROTECTION OFFICER

The data controller may appoint a data protection officer in Switzerland even without an obligation under Article 14 para. 1 FADP. The data controller may also entrust the voluntary and the mandatory representative with tasks that go beyond the obligations under Art. 14 f. FADP. 25

V. DISCLOSURE OF NAME AND ADDRESS (PARA. 3)

The data controller must disclose the name and address of its data protection officer. In the case of a legal entity as data controller, the company name corresponds to the name. The publication of an e-mail address or telephone number is not explicitly required. However, in the case of publication in the digital space, it is obvious to offer a digital contact option such as, in particular, an e-mail address. In comparison, Art. 13 para. 1 lit. a DSGVO is not only the "address" but the "contact details" before. 26

In order to fulfill its function as a contact point (Art. 14 para. 2 DSGVO), the name and address of the representative must be published in an easily findable and accessible form. It is obvious to publish the information as part of the general privacy statement on the website of the controller or, if necessary, also in the imprint. 27

In contrast to the information requirements under Art. 13 f. DSGVO, the name and address of the representation in Switzerland are not covered by the information obligation under Art. 19 f. FADP. 28

In contrast to the data protection officer (Art. 10 para. 3 lit. d FADP), there is no obligation to notify the FDPIC of the representation. The FDPIC must find out from the published information whether a data controller has designated a representative or inquire directly with the representative. 29

BIBLIOGRAPHY

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).

COMMENTARY ON

Art. 15 FADP

A commentary by Martin Steiger

SUGGESTED CITATION

Martin Steiger, Kommentierung zu Art. 15 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Steiger, N. XXX zu Art. 15 DSG.

Art. 15 Duties of the representative

[1] The representative shall maintain a record of controller`s processing activities that contains the information set out in Article 12 paragraph 2.

[2] On request, he or she shall provide the FDPIC with the information contained in the record.

[3] On request, the representative shall provide data subjects with information on how they can exercise their rights.

CONTENT

IN A NUTSHELL

Art. 15 FADP lists certain further obligations for a data protection representative pursuant to Art. 14 FADP. The representative must keep a record of the processing activities for the controller(s) and provide the FDPIC with the relevant information upon request. Furthermore, the representative must provide data subjects with information on the exercise of their rights upon request.

I. GENERAL

Art. 15 FADP enumerates certain further obligations of the data protection representative in addition to the obligations under Art. 14 para. 2 and 3 FADP (function as contact point, Art. 14 para. 2 FADP, and publication of contact details, Art. 14 para. 3 FADP). The enumeration in Art. 15 FADP is to be understood as non-exhaustive due to the broad role of the representation as a contact point. 1

II. DUTIES OF THE DATA PROTECTION REPRESENTATIVE

A. list of processing activities (para. 1)

According to the wording, the data protection representative must keep a register of the processing activities of the data controller (para. 1). This obligation goes further than the obligation under Art. 30 para. 1 DSGVO, according to which the EU data protection representation must keep a register only for processing activities that are subject to its competence. This excessive obligation, which in any case goes significantly further than the DSGVO, is likely to be a legislative oversight. 2

The exemption for companies with fewer than 250 employees pursuant to Art. 12 para. 5 FADP in connection with Art. 24 DPA does not apply. Art. 24 DPA does not apply to the data protection representation. According to Art. 14 para. 1 lit. a FADP, the data protection representative must only be designated if the processing by the data controller poses a high risk to the personality of the data subjects, among other things. This corresponds to the general risk-based approach of the FADP, as expressed in particular in Art. 24 FADP. 3

4 The information in the directory must comply with Art. 12 para. 2 FADP. In practice, the controller will keep a partial directory of processing activities that have an impact on Switzerland and provide a copy to the representation.

B. obligation to notify the FDPIC (para. 2)

5 The representation must communicate the information contained in the directory to the FDPIC upon request (para. 2), even without an administrative procedure. In practice, the representation is likely to communicate the directory to the FDPIC instead of providing only the information contained therein.

6 The obligation thus applies independently of the duty of the data controller to provide the FADP with all necessary documents in the context of an investigation (Art. 49 para. 3 FADP) and also independently of the power of the FADP to order access to all necessary lists of processing activities in the context of an investigation (Art. 50 para. 1 lit. a FADP).

7 The FDPIC does not have to take the route of international mutual legal assistance with the representation as a contact point in order to obtain the information in the directory. The representation in Switzerland may only communicate information that is already available.

8 A voluntarily designated representation does not have to maintain a directory as such.

C. information to data subjects (para. 3)

9 As a contact point (Art. 14 para. 2 FADP), the data protection representation must provide information to data subjects on request about the exercise of their rights under Art. 25 et seq. FADP upon request.

10 The representation must enable requesting data subjects to exercise their rights. The representation must inform data subjects, for example, at which contact details and by which means they can exercise their right to information (Art. 25 ff. FADP) vis-à-vis the controller and whether the controller has appointed a data protection advisor (Art. 10 FADP) who can be consulted (Art. 10 para. 2 FADP).

11 The duty of the data controller to provide information (Art. 19 ff. FADP) remains unaffected by the duty of the representation to provide information.

The data controller may also instruct the representative to provide other information to the data subjects.

BIBLIOGRAPHY

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).

COMMENTARY ON

Art. 18 FADP

A commentary by Apollo Dauag

SUGGESTED CITATION

Apollo Dauag, Commentary of art. 18 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Dauag, art. 18 FADP N. XXX.

Art. 18 Publication of personal data in electronic form

If personal data are made generally accessible by means of automated information and communications services in order to provide information to the general public, this is not deemed to be disclosure abroad, even if the data are accessible from abroad.

CONTENT

IN BRIEF

Anyone who lawfully makes personal data available on the internet for the purpose of informing the public (and thus an indefinite group of people) does not have to meet the requirements for disclosure abroad.

I. DEFINITION AND CLASSIFICATION

Art. 18 specifies the conditions under which the **general disclosure** of personal data on the internet is not considered disclosure abroad. 1

The publication of personal data in electronic form in accordance with Art. 18 concludes the third section, "Disclosure of personal data abroad." In addition to the principle in Art. 16 and the exceptions in Art. 17, Art. 18 describes the conditions under which the aforementioned provisions on disclosure abroad no longer apply. If the conditions are met, the **non-applicability of Art. 16 and 17 becomes the legal consequence**. 2

This is a **legal presumption** and is irrefutable: if the disclosure meets the conditions set out in Art. 18 (fictional basis), it is deemed not to constitute disclosure abroad in accordance with Art. 16 and 17 (fictional consequence). 3

This presumption does not affect the fact that it is a disclosure. This therefore constitutes a processing operation. The general **(processing) principles** of Art. 6 ff. must be fulfilled at all times. 4

As part of the **total revision** of the DSG, the provision on "cross-border disclosure" (Art. 6 aDSG) was transferred to a separate section entitled "Disclosure of personal data abroad." The permissibility of disclosure under the conditions set out there (formerly Art. 6 para. 1 and para. 2 lit. a aDSG) is now regulated as a principle in Art. 16, and the exceptions (formerly Art. 6 para. 2 lit. b–g aDSG) are now listed in Art. 17. 5

"Publication in electronic form" (formerly Art. 5 VDSG) has been transferred to Art. 18 with three editorial clarifications. In the draft and in the message, it was referenced as Art. 15; it was not yet included in the preliminary draft. Furthermore, this provision was inconspicuous in the **legislative process**. 6

7 The legal consequence of Art. 18 is exclusive, which is why publication on the internet does not constitute an exception within the meaning of Art. 17 para. 1 lit. a–f and is therefore not listed there.

II. INTENT OF THE LEGISLATOR

8 The internet knows no national borders. The publication of personal data on the internet inevitably results in its **global accessibility**—even in countries without adequate data protection. Because the audience is global and undefined, the responsible person in Switzerland cannot fulfill the requirements for permissible disclosure abroad. The legislator presumably accepts the associated risk of violations of privacy as a "concession to increasing digitalization."

9 Accessibility in countries without adequate data protection can be made more difficult by **country blocks** (IP blocks, known as "geoblocking"), but cannot be prevented entirely.

III. REQUIREMENTS

10 Two requirements must be met **cumulatively**, otherwise general accessibility is considered disclosure abroad.

A. Objective: informing the public through general access

11 The **publication** must (by definition) aim to inform the public by creating general access.

12 No additional requirements may be imposed on the **need for information**: it is covered if the processing of personal data for publication on the internet is lawful, in particular proportionate and fit for purpose.

13 Only a group of recipients whose location cannot be determined can be considered the **public**: if the location abroad can be determined or access can be controlled (e.g. through country blocking, see N. 9 above), it would be reasonable for the responsible person to fulfill the requirements for permissible disclosure abroad. However, a geographical restriction contradicts general access.

General access means that the information is made available without restriction. However, access does not have to be granted free of charge or without registration. Registration does not change the risk: as a result of global accessibility, even registered recipients from a country with adequate data protection can move to a country without adequate data protection and access the published personal data from there. 14

B. Means: automated information and communication services

Art. 18 refers to "automated information and communication services" in a technology-neutral formulation. The comments refer to "the Internet or Internet-based services" and "websites, blogs, or even news services such as Twitter, etc." This also includes "publication via apps, streaming services, video-on-demand portals, and comparable services." This covers **any form of publication in electronic form** that allows global access. This also applies to email newsletters. 15

In our opinion, the **server location** is irrelevant: firstly, there is a risk of accessibility from countries without adequate data protection (without country restrictions, see above N. 9) regardless of the server location. Secondly, even if the data is initially stored in Switzerland, it cannot be prevented from being copied to servers located abroad. Thirdly, the DSG also applies to circumstances that have an impact in Switzerland, even if they originate abroad. The distinction between servers located in Switzerland and servers located abroad does not appear to be relevant here. 16

IV. LEGAL CONSEQUENCES

If the **requirements are met**, publication in electronic form is not considered disclosure abroad under Art. 16 DSG. Exceptions under Art. 17 DSG do not need to be examined. 17

If the **requirements are not met**, publication in electronic form is considered disclosure abroad under Art. 16 DSG. Exceptions under Art. 17 DSG may apply. A violation of Art. 16 DSG (disclosure without adequate protection) is considered a breach of duty of care and may result in criminal liability under Art. 61 lit. a DSG. 18

V. SIGNIFICANCE IN PRACTICE

19 In fact, the legal presumption in Art. 18 forms the basis for the publication of personal data on the Internet and thus enables participation in modern media traffic: the hurdles applicable to disclosure abroad cannot be overcome by the responsible persons with reasonable effort.

20 Legally, the removal of the requirements for permissible disclosure abroad merely represents a **specific privilege for the responsible person in Switzerland**: the publication of personal data on the internet must always meet the requirements for processing and disclosure. Publications that are inappropriate or otherwise violate the principles of processing cannot be privileged.

21 According to Art. 3, the provisions of the DSG also apply in principle to processing initiated abroad (of personal data published on the internet). Even if the legislator accepts the risk of personal rights violations associated with global accessibility, the wording of Art. 18 does not contain any general privilege for the responsible person abroad. Consequently, further disclosures (following publication on the internet) are not subject to the requirements for disclosure abroad, but must also meet the requirements for processing and disclosure.

22 **Additional requirements** apply to federal authorities: in addition to the requirement for a legal basis for the publication of this data (e.g., the Freedom of Information Act), Art. 36 para. 5 stipulates the obligation to delete the data in question from "the automated information and communication service" as soon as there is no longer any public interest in public access.

23 As far as can be ascertained, this provision (neither as Art. 5a VDSG nor as Art. 18) has not yet been incorporated into a published court ruling.

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 19 FADP

A commentary by Matthias Glatthaar / Annika Schröder

SUGGESTED CITATION

Matthias Glatthaar/Annika Schröder, Kommentierung zu Art. 19 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Glatthaar/Schröder, N. XXX zu Art. 19 DSG.

Chapter 3 Duties of the Controller and of the Processor

Art. 19 Duty to provide information when collecting personal data

[1] The controller shall inform the data subject in an appropriate manner when collecting personal data; this duty to provide information also applies if the data is not collected from the data subject.

[2] It shall provide the data subject on collecting the data with the information required for the data subject to exercise their rights under this Act and to guarantee transparent data processing; it shall provide the following information as a minimum:

a. the controller`s identity and contact details;

b. the purpose of processing;

c. if applicable, the recipients or the categories of recipients to which personal data is disclosed.

[3] If the data is not collected from the data subject, the controller shall also inform the data subject of the categories of processed personal data.

[4] If the personal data are disclosed abroad, the controller shall also inform the data subject of the State or the international body to which such data are disclosed and if applicable of the guarantees under Article 16 paragraph 2 or the application of an exception under Article 17.

[5] If the data is not collected from the data subject, the controller shall also inform the data subject of the information specified in paragraphs 2–4 at the latest one month after receiving the data. If the controller discloses the personal data before the expiry of this deadline, it shall inform the data subject at the time of disclosure at the latest.

CONTENT

IN A NUTSHELL

The obligation to provide information pursuant to Art. 19 FADP concerns the data protection declarations that are important in practice and is specifically intended to increase the transparency of data processing. It supplements the general principle of transparency and requires that data subjects be informed of the key points of data processing whenever personal data is collected. The list of minimum information to be provided is shorter than that of the DSGVO and includes contact information, purposes of processing, categories of data processed, categories of data recipients, information on transfers abroad and information on automated individual decisions. However, Art. 19 FADP goes beyond the DSGVO in one respect and also requires the specification of recipient countries, whereby the specification of country groups or regions is sufficient. In most cases, the information does not have to be actively communicated to data subjects and it is sufficient if it is made readily available on the Internet. The obligation to provide information is one of the criminal offenses under the revised Data Protection Act: Anyone who intentionally fails to provide the information or intentionally provides false or incomplete information can be fined. In view of the fact that data protection declarations are hardly ever read or understood in detail in practice, it seems questionable overall whether the information obligation actually achieves the objective pursued of increasing transparency with regard to data processing.

I. GENERAL

A. Purpose of the Norm

1 Art. 19 FADP standardizes the duty of the controller to provide information when obtaining personal data. This concerns the data protection notices, which are significant in practice, or the data protection declarations, which are very common in business life. The duty to inform is one of the core provisions of data protection law, which is sometimes reflected in the fact that it is one of the provisions of the new Data Protection Act that is subject to penalties.

2 The aim of the duty to inform is to increase the transparency of data processing. Transparent processing of personal data is a fundamental principle of data

protection law and increasing transparency was a stated goal of the FADP revision. Data subjects should know that data about them is being processed, and they should have the opportunity to find out the key points of the data processing.

Transparency of data processing should enable data subjects to make an informed decision about the use of offers and services and enable them to exercise their rights granted by data protection law. The duty to provide information thus also indirectly serves to strengthen the rights of data subjects, which corresponds to another objective of the revision. 3

Finally, according to the dispatch, the duty to provide information is intended to increase the public's awareness of data protection and thus also to promote data protection concerns in general. 4

B. History

Art. 19 FADP expands the obligation to provide information already contained in the previous FADP when obtaining personal data. Under the old law, data subjects only had to be informed in the event of the acquisition of particularly sensitive personal data or personality profiles. Now, data controllers must inform the data subject whenever they obtain personal data. The catalog of mandatory disclosures is also moderately expanded by the new FADP. The revised FADP also combines the provisions that were previously spread across several articles and creates a uniform regulation for processing by private data controllers and by federal bodies. 5

Increasing the transparency of data processing was one of the main objectives of the revision of the FADP. In addition, the Data Protection Convention 108, which is binding on Switzerland, imposes a general obligation to provide information when obtaining personal data, which must be implemented in national law. Directive (EU) 2016/680, which is relevant for the Schengen area, also has an information obligation. The extension of the information obligation was therefore undisputed in principle in the legislative process. With few changes, the text that has become law corresponds to the version of the draft. 6

C. Classification and delimitation

Art. 19 FADP supplements the general transparency requirement of Art. 6 FADP. While the transparency requirement creates basic transparency, the in- 7

formation requirement builds on it to serve a more extensive need for information. The controller should not only ensure that the data collection is recognizable as such, but also provide the data subjects with certain information on the processing purposes and the manner of processing. Illustrative is David Rosenthal's food comparison: it must be immediately recognizable to consumers that the product in question is a strawberry jam (transparency requirement), while the list of ingredients and other details can be found on the food label, which can be consulted if interested (information requirement).

8 Unlike the transparency requirement, the duty to inform is not a concretization of the right of personality under Art. 28 of the Civil Code, but is of a public law nature. Violation of the duty to inform therefore does not constitute a violation of personality rights. Accordingly, a violation cannot be justified under Art. 31 FADP. The exceptions and limitations to the duty to inform are exhaustively standardized in Art. 20 FADP.

9 Art. 19 FADP is in turn supplemented by Art. 21 FADP, which provides for a special duty to inform in the case of full automation of important decisions, as well as concretized by Art. 13 FADP, which sets out requirements for the type and manner of information.

10 The duty to inform must be distinguished from the concept of consent. A data protection declaration ensures transparency as required by law, but does not constitute consent under data protection law and does not legitimize an act of data processing that is subject to justification under Art. 30 f. DPA. FADP that requires justification. However, there is a connection between the duty to inform and consent insofar as, on the one hand, the information basis required for valid consent can be created by means of a data protection declaration and, on the other hand, the fulfillment of the duty to inform and the obtaining of consent can coincide in individual cases (e.g. if a declaration of consent contains all the mandatory information required by Art. 19 FADP).

D. Interpretative Notes

11 The duty to provide information under the revised DPA is modeled on the duty to provide information contained in the DSGVO. However, Art. 19 FADP does not simply reproduce the obligation to provide information contained in the GDPR, but sets out a provision that deliberately deviates from parts of the GDPR. For example, the FADP prescribes fewer minimum disclosures than

the GDPR and grants more extensive exemptions from the information obligation. As shown by Thomas Steiner, Art. 19 FADP is therefore to be interpreted autonomously and the DSGVO practice is only to be consulted for confirmation and plausibility checks of the Swiss interpretation result.

With David Vasella, a cautious interpretation of the duty to inform must also be advocated: On the one hand, Art. 19 FADP is also a penal norm and the principle of legality under criminal law therefore requires a restrictive interpretation. On the other hand, the fulfillment of the duty to provide information involves considerable effort for companies, which affects economic freedom under Article 27 FC and is only permissible if the interference is proportionate and limited to the necessary extent. Finally, a certain restraint in the interpretation is also required because a basic transparency is already guaranteed by the transparency requirement of Art. 6 FADP and the information obligation only protects a need for information that goes beyond this. 12

II. OBLIGATED PERSON AND CONNECTING FACTOR (PARA. 1)

A. Obligated person

The duty to inform is directed at the controller, i.e. the private person or federal body that decides on the purpose and means of processing. Order processors bound by instructions are not subject to any duty to provide information for processing carried out on behalf of the controller. 13

The person responsible does not have to carry out the duty to provide information himself. He may also delegate the provision of information to a processor or another third party (e.g. to a web agency when operating a website). Even in such cases, however, the responsible party remains responsible for the proper fulfillment of the duty to inform. 14

B. Connecting factor

The duty to inform is triggered by any acquisition of personal data, regardless of whether the data controller acquires the data directly from the data subject or indirectly. The type of data procurement is only relevant for the time of information. It is also not decisive whether it is a permanent or repeated procurement or, as in the case of an isolated lottery, only a one-time data collec- 15

tion. In both cases, information must be provided. A (renewed) collection that triggers the duty to inform also occurs if already existing personal data is used for a new or additional purpose.

16 Information does not have to be provided if the data controller receives personal data by chance or otherwise without any action on his part. Examples are inquiries from journalists, blind applications, employee recommendations or unsolicited e-mail inquiries. However, information must be provided if such unintentionally obtained personal data is to be used for new or additional purposes.

17 The linking of the duty to inform to the event of data acquisition means, in terms of transitional law, that data subjects do not have to be informed about data processing already in progress when the new FADP comes into force (unless the information has already been provided at an earlier point in time anyway). However, data subjects, e.g., existing customers, must be informed at the latest when new data is obtained, e.g., subscribers to an online service when they next log in or participants in a customer loyalty program when they next make a purchase.

III. CONTENT OF THE INFORMATION (PARA. 2-4)

A. Mandatory information

1. General

18 Art. 19 FADP contains in para. 2-4 a catalog of mandatory information that must be provided to data subjects: Contact details of the data controller, purposes of processing, data recipients or categories thereof, categories of data processed, as well as recipient states in the case of transfers abroad and their safeguarding. Few additional mandatory disclosures can be found in other provisions of the FADP, such as in Art. 21 FADP regarding automated individual decisions and in Art. 14 para. 3 FADP regarding representation in Switzerland.

19 Compared to the FADP, the catalog of the FADP is short. This is to be welcomed and at least leaves room outside the scope of the DSGVO to inform with a sense of proportion and to counteract the "information overload" that

is rampant today. The flexible regulation of the FADP allows the information to be limited to relevant details based on risk and to omit unnecessary details.

2. Contact details

First, the name and contact details of the data controller must be provided. 20
The law does not specify which contact details must be disclosed. However, it is obvious to provide at least a postal address and an e-mail address. It is also conceivable to provide a telephone number, but in view of the possibility of intrusive contact by troublemakers, this is unusual and not recommended.

Controllers domiciled abroad must also publish the name and contact details 21
of any representation in Switzerland appointed in accordance with Art. 14 FADP (Art. 14 para. 3 FADP).

The disclosure of the contact details of any appointed data protection advisor 22
is voluntary. This is in contrast to the DSGVO, where it is mandatory to provide the contact details of the data protection officer. However, the FADP provides a (small) incentive to publish the contact details of the data protection advisor, in that private data controllers can only claim the exemption from notifying the FDPIC in the case of high residual risks after a data protection impact assessment has been carried out. For this purpose, it is sufficient to publish a functional mailbox (e.g., datenschutz@unternehmen.ch); it is not necessary to mention the data protection advisor by name.

3. Processing purposes

The data controller must indicate the purposes for which personal data are 23
processed. Data subjects should therefore be able to find out what their data is being processed for.

The level of detail with which the processing purposes are described is left to 24
the controller. Short descriptions such as "communication", "contract processing", "product development" or "marketing" are generally permissible. However, more detailed descriptions or explanatory examples are more helpful, which is also recommended in view of the purpose limitation principle because unclear formulations would be interpreted narrowly in accordance with the principle of trust, in case of doubt to the disadvantage of the data controller.

25 In addition to current processing purposes, possible future processing purposes can also be listed. This is permissible even if the processing in question is not yet specifically planned, but is merely a possibility. In view of the purpose limitation principle of Art. 6 para. 3 FADP, many companies will be inclined to draft such excessive data protection notices in order to keep new data uses open as far as possible, although this is not conducive to the clarity of data protection notices.

4. Data Recipients

26 The categories of recipients to whom personal data are disclosed must then be specified. The insertion of "if applicable" in the legal text has little practical relevance, since the recipients also include the commissioned processors used by the controller, and nowadays hardly any controller can manage entirely without commissioned processors. Jointly responsible parties are also considered recipients, as are, of course, actual "third parties". Group companies belonging to the same group are also recipients, but not entities belonging to the same legal entity such as individual departments or branches.

27 The categories can be defined by the responsible party at its own discretion; the law does not make any specifications in this regard. Conceivable, for example, would be somewhat narrowly defined categories such as "IT service provider", "logistics company" or "collection service provider", but broad categories such as "order processor" are also permissible.

28 Instead of categories of recipients, individual recipients may also be named. However, the naming of individual recipients is voluntary; the naming of categories is sufficient. In practice, it is usually not necessary to specify individual recipients, since the majority of companies have quite a large number of recipients (especially order processors) and maintaining a corresponding list would be time-consuming. The specification of specific recipients has become somewhat widespread in the online sector, where the third-party tools used are sometimes listed individually in connection with cookies and similar technologies.

5. Personal data processed

29 The categories of personal data processed must then be specified. Here, too, the controller is free to define the categories at its own discretion and to choose a level of detail that it deems reasonable and suitable for providing

sufficient information to the data subjects. Categories such as "master data", "behavioral data" or "preference data" would be conceivable. Personal data requiring special protection" or more narrowly "health data" would also be possible categories. It is usually also helpful to specify the categories, which are sometimes rather elusive, with examples of data types (e.g. "name", "e-mail address", "place of residence") and to make them more tangible. Also helpful, but not required, is the assignment of the individual data categories to concrete processing purposes.

According to Art. 19 para. 3 FADP, the categories of data processed need only be specified if the data are not obtained directly from the data subject. This is based on the idea that the data subject only has a need for information in this case. If, on the other hand, the data subject discloses his or her personal data himself or herself (e.g. by filling out an online form or a lottery ticket or by submitting a job application), he or she already knows the data processed by the data controller. 30

Following this idea, the restriction must be interpreted narrowly and limited to cases in which the data subject knowingly discloses data. On the other hand, the categories of data processed must also be indicated, for example, if the data are collected directly from the data subject, but without his or her active involvement and he or she may therefore not be aware that data about him or her are being processed. This is the case, for example, with automated collection of transaction data when shopping in stores or in online commerce, or with web tracking on the Internet. For the same considerations, the categories of data processed must also be indicated if the controller derives new data from the data received from the data subject, e.g. information about personal interests and affinities. 31

6. Recipient states

If personal data is disclosed abroad, the recipient states must be indicated. According to Art. 5 lit. e FADP, disclosure includes not only the transfer but also any access to personal data from abroad. Such transfers abroad are very common in the corporate world, e.g. when using cloud-based services. 32

With the obligation to disclose the recipient states, the FADP is unnecessarily stricter than the DSGVO, where information only has to be provided about the foreign disclosure itself, but not about the recipient states. The FADP 33

overlooks how international data traffic has become. After all, even under the FADP, individual countries do not have to be listed, which would hardly be practical in practice. The specification of country groups or regions is sufficient, e.g. "EU/EEA" or "Europe". The specification of "worldwide" is also permissible. For data subjects, it is evident that their data can in principle be processed in any country in the world.

34 If the recipient countries include countries without an adequate level of data protection, additional information must be provided: In such constellations, the guarantees made pursuant to Art. 16 para. 2 FADP to ensure an appropriate level of data protection or the exemption claimed pursuant to Art. 17 FADP must be disclosed. Here, for example, it is sufficient to refer to the conclusion of the standard contractual clauses recognized by the European Commission and the FDPIC, which are by far the most common instrument for safeguarding foreign transfers.

7. Automated Individual Decisions

35 If the controller uses automated individual decisions, it must inform data subjects about this and about the possibility of having the decision subjected to human review at the request of the data subject (Art. 21 FADP). Automated individual decisions are decisions that are fully automated and that have legal consequences for the data subjects or affect them significantly in some other way. The obligation to provide information therefore only applies to fully automated decisions; information does not have to be provided about decisions that are only partially automated or computer-aided.

B. Further information

36 In corporate practice, many companies will go beyond the mandatory disclosures outlined above, usually taking their cue from the DSGVO's more comprehensive catalog. Especially (but not only) larger and internationally oriented companies aim for "DSGVO-compliant" privacy notices, be it on a voluntary basis or because their data processing operations fall within the (extraterritorial) scope of the DSGVO. The DSGVO catalog also provides, in particular, for information on the storage period, the applicable legal basis, the legitimate interests pursued, if any, the rights of data subjects and the right of appeal.

However, the inclusion of such additional information under the FADP is usually not required by law. Information that goes beyond the minimum catalog must only be provided if it is necessary in a specific case to ensure reasonably transparent data processing (Art. 19 para. 2 FADP). This will rarely be the case and is more likely to be the case the more sensitive the data processed, the more extensive the processing, the more critical the modalities of the processing, the greater the criticality of the purpose of the processing and the more novel the technologies used for the processing. According to Art. 19 para. 2 FADP, the guiding principle is what data subjects need to know in order to be able to exercise their rights. 37

The DSGVO catalog probably represents a kind of upper limit. It is hard to imagine cases in which it might be necessary under the FADP to go even further than the information required by the DSGVO. 38

The regulation of the FADP theoretically also leaves room for specifying the handling of the information obligation for a specific industry in a code of conduct pursuant to Art. 11 FADP. However, such industry-specific codes of conduct have not yet been able to establish themselves in practice and will probably play only a minor role in the future. 39

IV. MODALITIES OF INFORMATION (PARA. 5; ART. 13 DPA)

A. Time

Depending on whether the personal data are obtained directly from the data subject or indirectly, information must be provided at different times. Direct procurement occurs when the data subject discloses his or her data to the data controller on his or her own initiative (e.g., by filling out a form or creating a user account) or the data controller collects the data by observation itself or by automated means (e.g., by recording purchase transactions or collecting movement data through a fitness tracker). In contrast, indirect procurement occurs when the responsible party collects data from public sources (e.g., media reports or public registers), obtains data from third parties (e.g., an address trader or a credit agency), or derives new data from existing databases (e.g., deriving preferences by analyzing transaction data). 40

In the case of direct procurement, the information must be provided at the same time as it is procured. In practice, this means that the required informa- 41

tion must be easily accessible at the time of procurement, e.g., on the website of the responsible party. The provision of information immediately after the first data acquisition, which was still permitted under the old law, is no longer permitted under the new law. In contrast, information may be provided in advance of the acquisition, provided that the connection between the information and the acquisition is sufficiently clear to the data subjects.

42 In the case of indirect procurement, information must be provided not immediately but within one month of receipt of the data (Art. 19 para. 5 FADP). However, the one-month grace period requires that the personal data are not disclosed by the controller to any other recipient. If, on the other hand, the controller discloses the personal data before the deadline expires, the grace period does not apply and the information must be provided at the latest at the time of disclosure. Since disclosures to order processors also fall under this (e.g., storage in the cloud), the information deferral has little practical significance and information must usually be provided immediately even in the case of indirect procurements, which often requires active communication. If this proves impossible to implement, the only recourse available to the data controller is to make use of an exception under Art. 20 FADP.

B. Form

43 The FADP does not contain any formal requirements for the communication of information. Oral information is also sufficient, e.g. in the form of tape announcements. In practice, however, text form is usually recommended, if only for reasons of proof.

44 In practice, the most widespread way of fulfilling the information obligation is by means of data protection declarations ("privacy notice" or "privacy policy"). A common approach is to describe a broad range of data processing activities in a general privacy notice (from customer business to personnel recruitment to cooperation with business partners) and to supplement this in a targeted manner with special product- or service-specific privacy notices. Special online data protection declarations ("cookie notice" or "cookie policy") for data processing in connection with a visit to a website or an app are also common in practice.

45 Data protection declarations represent one-sided information for the data controller and as such can be flexibly adapted to take into account, in particu-

lar, the dynamic nature of many data processing operations. From a practical point of view, the one-sided information also means that no active confirmation or acceptance of the privacy statement by the data subjects is required and therefore, in most cases, the checkboxes frequently found in online forms or ordering processes can be dispensed with.

It is also conceivable to include data privacy notices in general terms and conditions (GTC). Unlike data privacy statements, however, data privacy notices contained in GTCs become part of the contract and can therefore only be changed by amending the contract, which often proves too cumbersome in practice. In addition, the duty to inform can only be fulfilled vis-à-vis contractual partners (but not vis-à-vis other data subjects) by means of GTCs. It is therefore not recommended to integrate data protection notices in GTC and only a reference to the data protection declaration should be included in GTC. Additional data protection provisions in GTCs are at most justified if data protection consent is to be obtained, although consent obtained via GTCs is sometimes viewed critically. 46

Data protection notices are interpreted according to the unusualness and ambiguity rule, i.e., special reference must be made to unusual points and unclear formulations are interpreted to the disadvantage of the author. This also applies if data protection notices are designed as data protection statements or otherwise as unilateral information, at least insofar as they are not purely informative and can also have a legal effect, e.g., via the definition of the processing purposes or as an information basis for possible consents. Data protection notices integrated into GTC are additionally subject to abuse control pursuant to Art. 8 UWG. 47

C. Provision

The mandatory disclosures must be easily accessible to data subjects (Art. 13 DPA). It is not required that data subjects actually take note of the information. The access principle does not apply, but it is sufficient if data subjects have the possibility to access the information without great effort. Access to information may therefore require the cooperation of the person concerned, also because basic transparency is already guaranteed by the transparency requirement and the duty to provide information only serves a more extensive need for information. 48

49 However, the steps to be taken by the data subject in order to obtain knowledge must be reasonable. No longer easily accessible and therefore insufficient would be, for example, the mere designation of a contact person or the sending of the data protection statement only upon request. In contrast, the provision of data protection notices on a website is widespread. The information on the Internet is sufficient as long as it is ensured that the data protection information on the website can be easily found and accessed with a few clicks. In practice, a separate subpage for the data privacy statement and its permanent link in the footer, i.e., in the area at the bottom of a web page, has proven effective.

50 Information on the Internet is generally sufficient even if the data is processed offline. Data subjects are now accustomed to finding data privacy notices on the company's website, and they even take this for granted. Data privacy notices provided on the Internet also offer various advantages, such as simplified navigation and expanded possibilities for user-friendly design. The change of media to the Internet is therefore reasonable in most cases. Only in special cases, e.g., when sensitive processing of particularly sensitive personal data is involved, older groups of persons are targeted, or calling up an Internet page is not reasonable in terms of time due to the situation, may it be necessary in exceptional cases for data subjects to be able to access all mandatory information pursuant to Art. 19 FADP without having to change the medium.

51 One useful means of facilitating the change of medium is the display of QR codes that can be scanned with a cell phone and lead to the data protection statement on the internet. Such QR codes are increasingly common in practice (e.g., in signage for video surveillance), but they are not legally required.

52 Not only permissible, but also generally geared to the needs of data subjects, is multi-level information, in which only an initial overview of data processing is provided at the first level and the full information is only provided at a further level. In principle, the person responsible can define at his or her own discretion which information is provided at which level. There is no "basic information" that must be provided at the first level.

53 Versioning or dating of the privacy statement can be useful, but is not required by law, nor is the archiving and making available of earlier versions, which is sometimes found in practice.

D. Communication

The provision of the required information is usually sufficient and no active communication to data subjects is necessary. The references to the data protection statement in forms, in e-mail signatures, on letterhead, in telephone conversations and similar communications, which are sometimes encountered in practice, are also not necessary according to the view expressed here; even in contracts, an explicit reference to the data protection statement often seems dispensable. In the case of video surveillance, a clearly visible pictogram upon entering the sales area is generally sufficient to establish the required basic transparency, provided that the operator is identifiable under the circumstances. In such cases, interested parties can be expected to consult the website if they wish to obtain more detailed information about the data processing activities of the company concerned. They will also do this intuitively and take it for granted that data protection notices can be found on the website. 54

Active communication to data subjects is only necessary if the data subject does not know (and does not need to know) that the company in question is processing data about him or her. This is often the case when personal data is not collected directly from the data subject, but also in cases of direct collection when the data collection takes place without the awareness of the data subjects (e.g., when people are automatically recorded when entering a public area and walking routes are tracked). In such cases, data subjects must be actively made aware of the data protection statement (which can be done, for example, by providing the URL or providing a QR code), as otherwise they would not even think of calling up the company's website and finding out about the data processing there. 55

For the same considerations, changes to the data protection declaration must be communicated to existing customers in continuing obligations, at least if processing purposes are expanded and the change is therefore equivalent to a new procurement. Otherwise, data subjects would have no indication at all that the data protection statement might have changed and that it might therefore be advisable to visit the website. In practice, such information is usually sent by e-mail or via pop-up banners in an online store or when logging into a customer account. A notice in an invoice dispatch is also conceivable. 56

V. PRACTICAL TIPS

A. Procedure and Tools

57 Data protection notices should be prepared in close cooperation with the business and technical managers in the areas that perform the data processing, since these functions know best which data is used for which purposes and how. Often, relevant knowledge holders are located in business units responsible for data-intensive processing, such as marketing departments, data analytics, and HR areas. In practice, a participative, workshop-based approach involving these knowledge carriers has proven successful. However, it is also possible to collect information via structured questionnaires or interviews.

58 The processing directory pursuant to Art. 12 FADP or Art. 30 DSGVO also provides an initial overview of processing operations and often offers a good basis for identifying the relevant data processing operations. Furthermore, the processing directory in most cases contains information that can be used to prepare the mandatory data, such as information on the types of data processed, the purpose of processing and the (categories of) recipients.

59 In practice, there are various tools that support companies in the preparation of data protection notices, including sample data protection statements that can be used as a starting point and adapted for the company's own needs. The following are examples of offerings that are widely used:

- Template for a general data protection declaration, which covers numerous standard processing activities and is aligned with both the Swiss FADP and the DSGVO, prepared by two renowned Swiss law firms and available at https://dsat.ch/download/ (free of charge);
- Data protection generator by Datenschutzpartner for creating a data protection declaration for websites with sample formulations for numerous common web tools, available at https://www.datenschutzpartner.ch/angebot-datenschutz-generator/ (subject to a fee);
- Sample data protection declaration by German university professor Thomas Hoeren for website operators, available at https://www.itm.nrw/wp-content/uploads/Musterdatenschutzerkaerung-nach-der-DSG-VO_Stand_September_2022-1.docx (free of charge).

According to common governance understanding, the content of the data privacy statement should be approved by the management bodies responsible for data processing, e.g., the executive board. The role of the data protection officer or advisor and other legal and compliance functions should be limited to a coordinating and advisory role, also in view of the sanctions regime. 60

B. Preparation and Design

The Implementing Regulation to the Data Protection Act requires precise and comprehensible information (Art. 13 DPA). However, these are hardly justiciable (and also not punishable) criteria, and in practice, legalistic-looking flow texts still dominate. Many companies apparently believe that it is difficult to achieve a positive positioning with data protection and that it is therefore not worthwhile to invest significant resources in a user-friendly preparation of data protection notices. 61

It also does not help that data privacy law provides incentives to view data privacy notices primarily as a defensive instrument and not as customer-centric communication: on the one hand, in view of stricter regulatory means and sanctions, companies are anxious to include opening formulations and general clauses and thus protect themselves against accusations of incorrect or incomplete data privacy notices. On the other hand, in view of the principle of purpose limitation, companies do not want to block any room for maneuver and merely list possible future processing purposes in data protection notices. 62

Despite this unfortunate incentive structure, there are various promising approaches in practice for making data protection notices more reader-friendly and more closely aligned with the needs of addressees: 63

- Multi-level information ("layered approach"), in which relevant main aspects of data processing are first presented clearly and detailed information only follows at a further level. Layered information also includes fold-out texts and tangible examples to illustrate the sometimes rather abstract explanations.
- Use of data protection pictograms that allow data subjects to quickly gain an initial overview of how their data is processed. One example is the standardized pictograms published by the Privacy Icons association, which

make certain aspects typically relevant to data subjects visible at a glance and are already used by various prominent Swiss companies.

- Privacy dashboards that provide an easy entry point and enable data subjects to set priorities themselves and obtain targeted information on the essential points.
- Explainer videos that introduce data subjects to the topic and give them an easy-to-understand understanding of the most important content.
- Gamification elements that convey key aspects of data processing to data subjects in a playful way.

64 Such "legal design" approaches can significantly increase the accessibility and reader-friendliness of data protection notices and are therefore to be welcomed in terms of transparent data processing. However, there is no legal obligation to use such customer-friendly approaches, not even under the DSGVO.

VI. ENFORCEMENT AND LEGAL CONSEQUENCES

A. Administrative Law

65 If data subjects have not been properly informed about the data processing, the FDPIC may open an investigation and order the provision of legally compliant information as an administrative measure (Art. 51 para. 3 lit. c FADP). The FDPIC may act ex officio or upon notification.

66 The prohibition of data processing or the ordering of an adjustment by the FDPIC is also conceivable in principle (Art. 51 para. 1 FADP). However, in most cases, such a drastic measure is not likely to be proportionate solely on the basis of improper information.

B. Criminal law

67 The obligation to provide information is one of the obligations under the FADP that is subject to criminal penalties. Anyone who fails to provide information pursuant to Art. 19 FADP or provides false or incomplete information may be fined up to CHF 250,000 (Art. 60 para. 1 FADP). The duty to inform is a duty with great external impact and the threat of punishment therefore has

the potential to be used specifically as a means of exerting pressure on a company or the responsible employees or decision-makers.

In some cases, it is questioned whether Art. 19 FADP satisfies the criminal law requirement of Art. 1 StGB and whether a violation of the duty to inform may therefore be sanctioned by criminal law at all. In any case, it must be demanded that, with regard to completeness, only the mandatory information pursuant to Art. 19 para. 2-4 FADP is to be taken into account. Any additional information to be provided under the general clause of Art. 19 para. 2 is not to be taken into account. 68

In principle, it is not the company that is liable to prosecution, but the natural person(s) responsible for the breach (Art. 64 para. 1 FADP in conjunction with Art. 6 VStrR). This can be management personnel who have a legal duty to ensure data protection compliance, or persons who have operational process responsibility within the company and are authorized to make decisions on issues relating to the duty to inform. On the other hand, anyone who merely provides support is an accessory and as such remains exempt from punishment. In certain cases, the natural person may not be punished and the company may be fined instead. This is the case if the identification of the guilty person would require disproportionate investigative measures and a fine of no more than CHF 50,000 is possible (Art. 64 para. 2 FADP in conjunction with Art. 7 VStrR). 69

Only intentional acts are punishable. This also includes contingent intent, i.e. the acceptance of the crime. The negligent commission of an act, on the other hand, remains unpunished. Anyone who forgets a piece of information, formulates something imprecisely or deliberately omits something because he believes it is not part of the mandatory information does not act intentionally and remains unpunished. In order to exclude intentional acts as far as possible, decisions in connection with the duty to provide information should be documented in a comprehensible manner in each case, e.g. for which considerations information is omitted or an item of information is omitted. 70

Art. 60 para. 1 FADP is an application offense. A violation of the duty to provide information is therefore only prosecuted upon application, not ex officio. Criminal charges may be filed by any data subject, but not by the FDPIC. 71

C. Civil law

72 The violation of Art. 19 FADP as a provision of public law does not in itself cause a violation of personality rights and consequently cannot be asserted by data subjects by way of legal action.

73 However, data subjects may, if necessary, assert a violation of the general requirement of transparency as a processing principle and, based on this, bring an action before the competent civil court.

D. DSGVO

74 Within the scope of the DSGVO, violations of the duty to inform can be punished with fines of up to EUR 20 million or 4% of the total worldwide annual turnover (Art. 83 para. 5 DSGVO). This is the higher of the two fine frameworks provided for by the DSGVO. Unlike under the FADP, the DSGVO fine is primarily directed against the company and not against the natural persons acting on behalf of the company.

75 Under the DSGVO, a breach of the duty to provide information can, if necessary, also render the legal basis required for processing obsolete and thus render the data processing unlawful.

VII. CRITICISM OF THE NORM

76 The duty to inform is an expression of a basic understanding of data protection law based on informational self-determination. The basic idea is that data subjects inform themselves about data processing and, based on this, make an informed decision as to whether they consent to the corresponding processing of their data and whether they wish to exercise one of the data protection rights granted to them.

77 In today's digitalized and data-based world, the limits of this basic understanding are becoming increasingly apparent. The processing of personal data now affects all areas of life and data subjects are continually confronted with comprehensive data protection notices for which they often lack the time and usually also the necessary expertise. The result is information overload and a constant feeling of being overwhelmed. For many people, it is economically rational to save themselves this effort and remain uninformed.

The question therefore arises as to whether the duty to inform still achieves its intended goal at all and justifies the effort and expense associated with it. Its conceptual basis dates back to the early days of data protection, when data processing was simpler. Since then, however, our world has evolved considerably in terms of technology, and modern data processing is often complex. It's almost like requiring an airline to publish comprehensive technical information and expecting potential airline passengers to use it to make up their own minds about the airplane's airworthiness. Here, as there, this is neither realistic nor purposeful. It would be worthwhile to develop new approaches to data protection that are not based on superficial transparency. 78

BIBLIOGRAPHY

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).

MATERIALS

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).

COMMENTARY ON

Art. 20 FADP

A commentary by Matthias Glatthaar / Annika Schröder

SUGGESTED CITATION

Matthias Glatthaar/Annika Schröder, Kommentierung zu Art. 20 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Glatthaar/Schröder, N. XXX zu Art. 20 DSG.

Art. 20 Exceptions from the duty to provide information and restrictions

[1] The duty to provide information under Article 19 ceases to apply if one of the following requirements is satisfied:

a. The data subject already has the information concerned.

b. The processing is required by law.

c. The controller is a private person who is required by law to preserve confidentiality.

d. The requirements of Article 27 are satisfied.

[2] If the personal data is not collected from the data subject, the duty to provide information also ceases to apply if any one of the following requirements is satisfied:

a. It is not possible to provide the information.

b. Providing the information requires disproportionate effort.

[3] The controller may restrict, delay or dispense with the provision of the information in the following cases:

a. It is required to do so because of overriding third party interests.

b. Providing the information defeats the purpose of the processing.

c. The controller is a private person and the following requirements are satisfied:

The controller is required to do so because of its own overriding interests.
The controller does not intend to disclose the personal data to third parties.

d. The controller is a federal body and any one of the following requirements is satisfied:

The measure is required to satisfy overriding public interests, in particular to protect Switzerland's internal or external security.

The communication of the information may compromise an enquiry, an investigation or administrative or judicial proceedings.

[4] Legal entities that belong to the same group of companies are not third parties within the meaning of paragraph 3 letter c number 2.

CONTENT

IN A NUTSHELL

Art. 20 FADP contains a number of exemptions from the obligation to provide information: on the one hand, exemptions where the obligation to provide information does not apply at all, e.g. if the data subject already has the relevant information or the processing is carried out in fulfillment of a legal obligation. On the other hand, the provision contains restrictions where the duty to inform continues to exist, but the information can be restricted, postponed or suspended in individual cases, e.g. if information would frustrate the purpose of the processing or overriding interests conflict with information. Art. 20 FADP serves as a corrective to a comprehensive duty to inform and ensures that the duty to inform does not become an excessive burden for data controllers and remains limited to cases where it is necessary for the protection of data subjects.

I. GENERAL

A. Norm Purpose

1 Art. 20 FADP standardizes a number of reliefs from the information obligation. The provision is intended to ensure that the information obligation applies where it is necessary for transparent data processing and the protection of data subjects, while it does not apply in cases where it would be superfluous or disproportionate. It is an expression of the legislative effort to find a balance of interests and to create targeted facilitations. Compared to the DSGVO, the list of exceptions in Art. 20 FADP is quite extensive.

B. History of origins

2 Art. 20 FADP bundles the exceptions and limitations spread over various articles in the old law (Art. 9, Art. 14 para. 4 and 5, Art. 18a and Art. 18b aDSG) and moderately supplements them. Art. 20 FADP remained undisputed in principle in the parliamentary deliberations, although the exception in the case of disproportionate effort was considered too far-reaching by parts of parliament. The group privilege pursuant to Art. 20 para. 4 FADP was added during the parliamentary deliberations.

C. System

The provision distinguishes between exceptions, where the obligation to provide information does not apply at all, and restrictions, where the obligation to provide information continues to apply in principle, but the controller can restrict, postpone or suspend the provision of information in individual cases. Art. 20 FADP applies to both private data controllers and federal bodies, but differentiates between private and federal bodies in the individual exceptions and restrictions. 3

The exceptions and limitations contained in Art. 20 FADP are exhaustive. A breach of the duty to inform cannot be justified under Art. 31 FADP either, since the duty to inform under Art. 19 FADP is of a public law nature and not a concretization of the processing principles under Art. 6 FADP. 4

D. Notes on interpretation

Some of the exceptions to Art. 20 FADP are quite broad and include cases in which the data processing is identifiable (legal basis, para. 1 lit. b) or the confidentiality of the personal data processed is guaranteed (legal duty of confidentiality, para. 1 lit. c), but the data subject's need for information, which is protected by the duty to inform, remains unfulfilled. It is therefore appropriate to interpret the facts rather narrowly and to bring them in line with the purpose of the duty to inform. 5

II. EXCEPTIONS (PARA. 1 AND 2)

A. General

Art. 20 FADP specifies in para. 1 and 2 a total of six situations in which the controller is completely exempt from the obligation to inform data subjects. In these situations, the data subject also does not have to be informed about the applicability of the exemption itself. The only remedy is to exercise the right of access, although the data subject often has no reason to request access to his or her data if he or she is unaware of the data processing, and the right of access is itself subject to similar limitations (Art. 26 FADP). 6

B. Prior knowledge of the information (para. 1 lit. a)

7 The obligation to provide information does not apply if the data subject already has the relevant information. Data subjects do not have to be informed about things they already know, which stands to reason. A comparable exception to the duty to inform is also found in the DSGVO. In the old FADP, the exception was still somewhat narrower and referred to the information process rather than the existence of the information itself (Art. 14 para. 4 and Art. 18a para. 3 aDSG: "if the data subject has already been informed").

8 The exception initially means that data subjects do not have to be informed again in subsequent data procurements if they have already been informed on the occasion of an earlier procurement. The prerequisite is that the procurements are factually related and not too far apart in time. This applies, for example, to individual orders in an online store if information was already provided when the account was created, or to follow-up medical treatment if information was already provided in connection with the initial treatment.

9 Another application of the exception is when the data subject has consented to data processing, since valid consent under Art. 6 para. 6 FADP requires sufficient information by definition. The information required by Art. 19 FADP can therefore also be provided by means of a declaration of consent.

10 According to the dispatch, the exception should also cover situations in which the data subject sends his/her personal data to the controller without the latter's intervention. This is quite far-reaching, since the knowledge of the data subject is limited to the fact of procurement. However, there is a legitimate information interest in further circumstances of the data processing, in the example of a job application mentioned by the dispatch, for example, in whether (and how long) the application documents are also kept for future jobs, to whom they may be passed on and where they are stored.

11 Finally, the exception also includes cases in which it is clear that the data subject has waived the right to the information pursuant to Art. 19 FADP or has no interest in receiving the information. However, this must be limited to clear cases and is in any case not to be assumed already if the data subject has made his or her personal data publicly available (e.g., on a social media profile).

C. Processing required by law (para. 1 lit. b)

The duty to inform also does not apply if the data processing is provided for by law. The reasoning is that in these cases, the legislator has already defined the cornerstones of the data processing, weighing the various interests, and informing data subjects would therefore not provide any significant additional protection. The DSGVO contains a similar exception, but limited to the case of indirect procurement and subject to the condition that the legislative norm explicitly regulates the data processing and provides for appropriate measures to protect the legitimate interests of data subjects. 12

To fall under the exception, either the data processing itself must be prescribed by law or the data processing must be indispensable for the fulfillment of a legal obligation. With respect to private data controllers, a sufficiently precise basis in a law in the substantive sense is sufficient. For federal bodies, the standard of Art. 34 FADP applies and a law in the formal sense is required if it concerns the processing of particularly sensitive personal data, profiling is carried out, or if it concerns a serious encroachment on fundamental rights. 13

Data processing required by law is numerous in the legal system and the exception therefore has great practical significance. Examples include: Keeping the share register as well as convening and conducting the general meeting of shareholders in the case of public limited companies; identification obligations and determining the beneficial owner for the purpose of combating money laundering; notification obligations of the health authorities in connection with communicable diseases; payment of wages and preparation of certificates by the employer in the employment relationship; accounting obligations under tax and social security law. 14

The exception can also be claimed if the data controller has brought about the legal obligation itself, e.g. identification obligations under money laundering law by initiating the business relationship or processing indicated by employment law by concluding the employment contract. 15

If the data processing goes beyond the statutory obligation (e.g. if data collected for the purpose of combating a pandemic is also to be used for marketing purposes), the exception does not apply and information must be provided. Data processing that only takes place at a general level within a legally defined framework but is carried out voluntarily is also not exempt from the duty to inform. In the employee area, information is therefore regularly required, e.g. 16

in the form of an employee data protection declaration. Even if the framework set by Art. 328b OR is not exceeded, data processing in the employee area usually goes beyond what is effectively prescribed by law.

17 In the case of federal bodies, the processing of personal data on the basis of Art. 34 FADP is in most cases based on a legal foundation. However, the corresponding legal provisions are often quite general and are often not able to guarantee the transparency aimed at by the information obligation on their own. In the correct view, para. 1 lit. b therefore only exempts federal bodies from the obligation to provide information if the data processing is expressly provided for by law and described with sufficient precision. As an example of data processing precisely described in the law, Art. 69f and 69g RTVA in conjunction with Art. 67 and 67a RTVA can be used. Art. 67 and 67a RTVV can be cited. On the other hand, to exempt federal bodies from the obligation to provide information for any processing based on the law on the basis of para. 1 lit. b would place an excessive burden on the transparency of federal data processing and make the applicability of Art. 19 FADP to federal bodies per se and the restrictions provided for specifically for federal bodies in Art. 20 para. 3 FADP largely obsolete.

D. Statutory duties of confidentiality (para. 1 lit. c)

18 Natural persons who are subject to a statutory duty of confidentiality are exempt from the obligation to provide information. This applies in particular to the professional groups mentioned in Art. 321 SCC, such as clergy, lawyers, pharmacists and doctors. The exception applies only (but still) to the area of activity protected by secrecy, but not to any other activities of a person belonging to these professional groups. Thus, if the lawyer or general practitioner processes personal data for customer acquisition (invitations to events or sending customer information) or for the provision of her website, for example, she is subject to the duty of disclosure for these activities.

19 The exception does not apply to the legal entity with which the person subject to the duty of confidentiality is employed or for which he/she works. A legal entity or a medical center must therefore also provide information about data processing in the secrecy-protected area of activity (e.g. about legal services in the monopoly area or about health services). The exception does not apply to federal bodies either.

According to the dispatch, the exception under para. 1 lit. c regulates a possible conflict of norms between the duty of confidentiality and the duty to inform, but this is not convincing: even in the secrecy-protected area of activity, the provision of the information required under Art. 19 FADP would not disclose any personal data and thus would not reveal any secrets. For example, a lawyer could easily inform in a general manner that the personal data contained in a legal document will be transmitted to the opposing party and the competent court. Similarly, a physician could inform about the disclosure of personal data to the health insurance company for billing purposes. Professional secrecy would not be affected in such cases. Should a conflict nevertheless exist in an individual case, it could also be resolved by means of one of the restrictions provided for in para. 3 (e.g. in the case of overriding interests). 20

The blanket exemption from the duty to provide information for persons subject to a secrecy obligation is also surprising because, although the confidentiality of the personal data processed is guaranteed if a statutory secrecy obligation applies, the need for information protected by the duty to provide information does not automatically cease to apply. For example, it remains open for which purposes the person subject to the duty of confidentiality processes the personal data, e.g. whether the doctor or the lawyer also carries out profiling and uses the collected data for marketing purposes. 21

The DSGVO contains a comparable exception in the event that the personal data collected is subject to professional secrecy. It is at the same time broader and narrower than the exception of the FADP: The exception of the DSGVO is not limited to private persons, but applies to them only in the case of indirect procurement. 22

E. Media Privilege (para. 1 lit. d).

Another exception concerns the research activities of media with regard to the publication of a journalistic work and the protection of sources. Under the same conditions under which information can be refused, information can also be waived: Art. 20 para. 1 lit. d FADP refers to Art. 27 FADP. The exception protects the information and control function of the media. If persons who are the subject of investigative research had to be informed and sources of information had to be disclosed, journalistic work would be rendered impossible and the media would not be able to fulfill the democratic function assigned to them. 23

24 The exception to para. 1 lit. d is only available in the case of processing of personal data with a view to publication in the editorial section of a periodically published medium (e.g. a newspaper or an online magazine). The exception cannot be invoked for so-called "advertorials" and other publications with a predominantly advertising character, nor for research activities with regard to a documentary film or another non-periodical medium. If necessary, however, another ground for exception or restriction may be invoked for such research activities, e.g., Art. 20 para. 3 lit. b FADP (frustration of purpose).

F. Impossibility of information (para. 2 lit. a)

25 If personal data are not obtained directly from the data subject, i.e. indirectly, the obligation to provide information does not apply even if it is impossible to provide the information. In cases of direct procurement, the exception is not available, which is logical. Logically, it is not possible to obtain the data directly from the data subject, but it is impossible to provide the information.

26 Impossibility to carry out the information exists, for example, if the data subject cannot be identified at all. In the example of the photo of a stranger cited in the message, however, this cannot be assumed without further ado in view of today's technological possibilities. The exception also has little practical relevance in other respects: If it is not possible to identify the data subject, the data concerned are usually not personally identifiable, and the question of the duty to inform does not even arise.

G. Disproportionate effort (para. 2 lit. b)

27 Finally, the duty to inform does not apply if personal data are obtained indirectly and informing the data subjects would require a disproportionate effort. Again, the exception cannot be claimed in the case of direct procurement. Anyone who collects personal data directly from the data subject must be expected to inform him or her about the collection.

28 The extent to which the effort is still proportionate must be determined on a case-by-case basis and is based on the effort required of the controller in relation to the information interest of the data subjects. The decisive factor is not the specific information interest of individual persons, but a generalized information interest. The more sensitive the data processed, the more extensive the processing, the more critical the modalities of the processing, the

greater the criticality of the purpose of the processing and the more novel the technologies used for the processing, the greater the effort that can be expected of the data controller.

The dispatch cites the processing of personal data for archiving purposes as an example of disproportionate effort. In the case of a large number of persons, the information would involve a great deal of effort, while the information interest of the data subjects in such cases would regularly be limited. The analogous exemption provision in the DSGVO lists processing for scientific or historical research purposes and for statistical purposes as further examples. The information of data subjects may also be disproportionate if very large amounts of data are used for the training of Large Language Models and similar AI models, e.g., if the AI is trained with the "entire Internet". In practice, it is advisable to document in each case the considerations on the basis of which information of data subjects is no longer deemed to be proportionate. 29

The facts of para. 2 lit. b are conceived as an exception, but a restriction would have been more appropriate. If information is disproportionate, e.g. because of the large number of persons affected, a complete omission of the information does not seem appropriate. A milder (and obvious) remedy in such cases would be to provide a privacy statement on the website of the company concerned, waiving individual notification. 30

III. RESTRICTIONS

A. General

Art. 20 FADP contains in para. 3 a total of five constellations in which the information may be restricted, postponed or suspended. In contrast to the exceptions under para. 1 and 2, the obligation to provide information does not cease completely in these cases, and the information may only be restricted to the extent required by the corresponding reason in the individual case. If the reason for the restriction subsequently ceases to apply, the information must be provided subsequently. As with the exceptions, the data subject does not have to be informed about the application and scope of the restriction in the case of restrictions pursuant to para. 3, and the data subject's only recourse is to assert the right to information. 31

32 The possibilities for restricting information are largely based on a balancing of interests, in which the specific reason for a restriction must be set in relation to the information needs of the data subjects. In contrast, in the case of exceptions, the existence of a specific circumstance (e.g. that the data subject already has the information) usually determines whether or not the exception can be used.

B. Overriding interests of third parties (para. 3 lit. a)

33 There is a possibility to restrict the information if this is necessary due to overriding interests of third parties. The term "third party" in para. 3 lit. a is not to be understood exclusively in the plural and the overriding interest of an individual third party is also sufficient to be able to restrict the information. This possibility of restriction exists both for private responsible parties and for federal bodies.

34 The restriction can be used in cases where third parties have an interest in not providing information to the data subject and this interest outweighs the data subject's need for information. This is particularly conceivable in constellations in which the data subject would also obtain details of third parties through the information and their confidentiality interests would thereby be impaired. In practice, however, such constellations are likely to occur only rarely, since the information as such does not usually disclose any personal data.

C. Thwarting the Purpose (para. 3 lit. b)

35 It is also possible to restrict information for private data controllers and federal bodies if the purpose of the data processing is frustrated by the information. Art. 20 para. 3 lit. b FADP leaves open whether a mere impairment of the purpose of the processing is sufficient for a restriction of the information or whether a complete prevention must be given. According to the Message, the provisions of Art. 20 para. 3 FADP are to be interpreted restrictively, which is why it must be assumed that the prevention must be complete.

36 In the case of several purposes pursued with data processing, the information to the data subject must frustrate the actual main purpose, which, according to the message, must also be of considerable importance. The possibility of restricting the information is also further limited by the fact that purely eco-

nomic interests generally do not fall within the scope of the restriction pursuant to para. 3 lit. b. In practice, therefore, there will be only a few cases in which private responsible parties can make use of this restriction. The scope of application is broader for federal bodies, especially in the area of criminal prosecution, although here the possibility of restriction under para. 3 lit. d no. 2 is likely to apply in most cases.

One example of application of the restriction is research activities in connection with investigative journalism, which do not fall under the exception of Art. 20 para. 1 lit. d FADP, e.g. because the research is carried out for a documentary and not for a periodically published medium. A suspension of the information based on para. 3 lit. b may also be justified if personal data are processed as part of the preservation of evidence for a later process and the information of the data subject would make the collection of the evidence impossible. Equally conceivable is the postponement of information when conducting behavioral studies in which the data subjects are supposed to exhibit the most natural behavior possible and information before the study is conducted would falsify the results. Similarly, in the case of justified shadowing of a person by a private investigator, its purpose would be frustrated by providing information to the person being observed. 37

D. Overriding interests of the data controller (para. 3 lit. c).

The possibility of restricting information on the basis of overriding interests of the person in charge is open only to private persons in charge. Federal bodies cannot refer to this possibility. 38

In contrast to para. 3 lit. b, economic interests such as sales promotion or product development also come into question here. Since the restriction option is directed only at private responsible parties, in many cases it will be precisely such economic interests that are at issue. However, the actual restriction of information must be preceded by a balancing of the interests of the responsible party and the information needs of the data subjects. This is a rather open-ended standard and it is therefore advisable for data controllers to document why their own interests prevail. 39

Another prerequisite for restricting the provision of information under para. 3 lit. c is that no data is disclosed to third parties. This refers to disclosures to independent responsible parties, e.g. to cooperation partners or advertising 40

networks, but also to authorities. However, disclosures to order processors who carry out data processing on behalf of the data controller in accordance with instructions, as well as to jointly responsible parties, are not harmful. If disclosures to order processors and jointly responsible parties are also to be covered, the FADP generally refers to "recipients" instead of "third parties.

41 Pursuant to para. 4, data disclosures to group companies are also generally harmless, even if the recipient within the group is itself a data controller. In the case of the disclosure of personal data within the own group, for example in the HR area, the requirements for the possibility of restriction are therefore still met. This group privilege was not originally provided for in the draft law and was added during the parliamentary deliberations. Consequently, only disclosures to separate responsible parties outside the group's own group will lead to the exclusion of the restriction option of para. 3 lit. c.

42 para. 3 lit. c offers considerable scope for restricting the provision of information in practice, as an overriding interest of the data controller can be demonstrated for a large number of data processing operations. As a rule, overriding interests are to be assumed, for example, in the case of low-threshold data processing such as simple customer loyalty measures, where the circumstances and the manner of data processing are obvious and comprehensive information would therefore have no added value for data subjects.

E. Overriding public interests (para. 3 lit. d no. 1)

43 For federal bodies, it is possible to restrict information if this is necessary to protect overriding public interests. For private responsible parties, there is no possibility to base a restriction of information on para. 3 lit. d.

44 What is to be understood as a public interest is quite broad. The standard mentions, by way of example, interests in the internal or external security of Switzerland, which may be relevant in particular in the context of intelligence activities. However, public interests are also affected if, for example, compliance with obligations under international law, diplomatic purposes or the maintenance of relations with foreign countries are at stake. A federal body could therefore restrict information, for example, if the communication to the persons concerned would harm foreign policy relations with another country.

45 Here, too, the public interest must "prevail" and a balancing of interests is thus required for a federal organ to make use of the restriction option. However, a

balancing exercise that contrasts the information needs of (individual) affected persons with national security interests is likely to often be in favor of the restriction option.

F. Threat to proceedings (para. 3 lit. d no. 2)

Finally, para. 3 lit. d no. 2 provides for a possibility of restriction if the information would lead to an investigation, inquiry or official or judicial proceedings being jeopardized. This option is also only available to federal bodies and cannot be used by private responsible parties. Private responsible parties must resort to another ground of exception or restriction in cases where proceedings would be jeopardized. 46

The possibility has a substantive proximity to the restriction of information if this would frustrate the actual purpose of the data processing. Unlike para. 3 lit. b, however, where the purpose must actually be frustrated, a threat is sufficient for the restriction option under para. 3 lit. d. The restriction of information is therefore not necessary. It is therefore not necessary that the threat actually materializes; the risk is sufficient. 47

BIBLIOGRAPHY

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).

MATERIALS

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).

COMMENTARY ON

Art. 21 FADP

A commentary by Liliane Obrecht / Anna Kuhn

SUGGESTED CITATION

Liliane Obrecht/Anna Kuhn, Commentary to art. 21 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Obrecht/Kuhn, art. 21 FADP N. XXX.

Art. 21 Duty to provide information in the case of an automated individual decision

[1] The controller shall inform the data subject about any decision that is based exclusively on automated processing and that has a legal consequence for or a considerable adverse effect on the data subject (automated individual decision).

[2] It shall on request allow the data subject to express their point of view. The data subject may request that the automated individual decision be reviewed by a natural person.

[3] Paragraphs 1 and 2 do not apply if:

a. the automated individual decision is directly connected with the conclusion or the processing of a contract between the controller and the data subject and the data subject's request is granted; or

b. the data subject has explicitly consented to the decision being automated.

[4] If the automated individual decision is issued by a federal body, it must designate the decision accordingly. Paragraph 2 does not apply if, in accordance with Article 30 paragraph 2 of the Administrative Procedur

CONTENT

IN A NUTSHELL

Article 21 of the FADP establishes an obligation to provide information in cases of fully automated individual decisions that significantly affect a data subject or result in legal consequences for them. Furthermore, the provision grants the data subject various rights of protection: the right to present their point of view and the right to have the decision reviewed by a human. In addition, the provision requires federal agencies to explicitly label fully automated individual decisions as such. A significant shortcoming of the provision is that it does not include semi-automated decisions within its scope of application.

I. GENERAL

A. Overview and Structure

With the revision of the Data Protection Act in September 2023, the **term** "automated individual decision" was introduced into Swiss law. Art. 21 of the FADP governs the obligations of the controller within the meaning of Art. 5(j) FADP and the rights of the data subject in the case of an automated individual decision. Para. 1 defines the automated individual decision and establishes an obligation to provide information regarding it. Para. 2 sets forth the rights of the data subject, which include the right to be heard and the right to have the decision reviewed by a natural person. Para. 3 provides for exceptions to para. 1 and para. 2. Para. 4 establishes a special provision for federal bodies. 1

The FADP is implemented by the **Data Protection Ordinance** (DSV). To date, the Ordinance has not contained any further provisions regarding automated individual decision-making. 2

B. Purpose of the Provision

According to the Federal Council's explanatory memorandum, Art. 21 of the FADP is intended to comply with existing **provisions under international law**. In terms of substance, the Federal Council justifies the new provision by noting that automated individual decisions are steadily increasing as a result of technological developments. However, there is no detailed examination of the risks associated with automated individual decision-making or the resulting need for regulation. 3

4 The explanatory memorandum does, however, cite examples of how **erroneous** decisions can be made based on incorrect or incomplete data sets. This suggests that one reason for introducing the new Art. 21 of the FADP was also the fear of precisely such decisions. The protection of human dignity can therefore be seen as a potential regulatory objective, the aim of which is, among other things, to protect people from being reduced to mere objects of machine-driven decisions. Another possible regulatory objective can be seen in protection against discrimination by the state: If an automated individual decision is based on machine learning algorithms, it does not follow rules created by humans but rather learns from large amounts of data (so-called "training data"), which may reflect societal disadvantages, patterns, or outdated role models (so-called *data bias*). In this way, an automated individual decision can reproduce disadvantages and have a discriminatory effect. The new provision grants affected individuals the opportunity to exert influence if they are the subject of an automated individual decision ("right to a human hearing"). According to the explanatory memorandum, this is intended to counteract erroneous decisions and their consequences. Furthermore, the legislature thereby implicitly regards human decisions as superior, since, in its view, erroneous automated decisions can be prevented through human intervention. This basic assumption also underlies the provision on automated individual decisions under the DSGVO (see N. 69 ff.), which the Explanatory Memorandum cites as further justification for Art. 21 of the FADP.

C. Historical Background

5 Although the legal discourse surrounding automated individual decisions only gained momentum with the explicit introduction of Art. 21 of the FADP, as will be shown below, the concept dates back several decades. Art. 21 of the FADP is therefore the result of a gradual development built upon earlier reform efforts and international standards.

6 **1981:** The materials accompanying the Directive on the Processing of Personal Data in the Federal Administration of March 16, 1981, highlighted the risks that could arise from the creation of personality profiles and the automated decision-making based on them. However, Swiss law did not at that time provide for explicit regulation of automated individual decision-making.

2003: As part of the partial revision of the FADP in 2003, the Federal Council sought to introduce an explicit duty to inform in cases of automated individual decision-making. Parliament, however, rejected this proposal. 7

2017–2020: The version of Art. 21 of the FADP proposed by the Federal Council in its 2017 message on the total revision was essentially adopted by Parliament. While the consultation process was still controversial, this provision was largely uncontested during the parliamentary proceedings. As the concordance table below shows, the changes made were limited to editorial clarifications: 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.

Table 1: Concordance table on the development of Art. 21 FADP (own presentation)

2018: A renewed impetus to legally address automated individual decisions arose in the course of implementing Directive (EU) 2016/680—which is binding on Switzerland—on the protection of natural persons with regard to the processing of personal data in the context of judicial and police cooperation. To this end, a provision on automated individual decisions was created within the framework of the Schengen Data Protection Act (SDSG; in force until August 31, 2023) (Art. 11 FADP). This provision required federal agencies in the covered areas to inform data subjects about automated individual decisions and granted them corresponding rights to participate in the process. With the entry into force of the revised Data Protection Act, the FADP was repealed (Art. 68 in conjunction with Annex 1 FADP). Art. 21 FADP succeeded Art. 11 SDSG in substance. 9

2019–2023: Furthermore, the introduction of Art. 21 FADP serves to implement Switzerland's obligations under international law. The modernized Data Protection Convention of the Council of Europe (Convention 108+, ER-Conv-108+), which Switzerland signed on November 21, 2019, and ratified on September 7, 2023, expressly obligates the contracting states to ensure a right to information and a right to be heard in the case of automated individual decision-making (Art. 8(1)(e) and Art. 9(1)(a) of the Council of Europe Convention 108+). Furthermore, by introducing Art. 21 of the FADP, the legislature sought to establish a level of data protection that continues to be considered "adequate" in relation to the European Union within the meaning of Art. 45 of the DSGVO. 10

II. DUTY TO PROVIDE INFORMATION IN THE CASE OF AUTOMATED INDIVIDUAL DECISION-MAKING (PARA. 1)

Automated individual decision-making is legally defined in Art. 21(1) of the FADP. In order to contextualize the term (B.), a few preliminary remarks on automation and its technical development must first be made (A.). The key legal requirements will then be clarified (C.). 11

A. Technical Background

1. Levels of Automation

12 The term "automation" refers to the transfer of tasks from humans to machines. An automated individual decision may involve different levels of automation. Broadly speaking, a distinction can be made between partial and full automation.

13 The term "partial automation" has several meanings. On the one hand, it may involve **decision support**. In this case, the automated system prepares the decision (identifying, compiling, or evaluating information; creating overviews). However, the actual decision is made by a responsible natural person.

- *For example, partially automated systems can be used to make medical diagnoses by analyzing X-rays, CT scans, or MRI scans.*
- *Semi-automated systems can be used to draft contract terms.*
- *Semi-automation can also be useful for extracting relevant data from large volumes of text. For example, a decision-support system in tax administration can provide the authorities with additional data not directly derived from the taxpayer's tax return, or highlight relevant clauses in lengthy contracts.*
- *In criminal proceedings, particularly in the United States, semi-automated systems are used to calculate the likelihood of recidivism among offenders.*

14 On the other hand, the semi-automated system can function as a **decision review** by being used to verify a decision made by a natural person.

15 **Full automation**, on the other hand, means that a system carries out every single step of the decision-making process on its own. Strictly interpreted, even the programming and the initiation of the decision-making process must be carried out by the system.

- *For example, in the private sector, decisions on loan applications can be made fully automated by automatically assessing the applicant's ability and willingness to pay. Contracts are then concluded automatically.*
- *Furthermore, the automation of the recruitment process is conceivable. One example is the fully automated pre-selection of applications from po-*

tential employees. In this process, the system decides whether to invite an applicant to an interview with a human recruiter.

- *Fully automated systems can assign prospective students to a program of study and, thereby, to a college or university.*

In the public sector, full automation is particularly well-suited for **mass administration processes** due to standardized procedures and the availability of large amounts of data. These are the areas of public administration in which a large number of decisions are made regarding virtually identical sets of facts. 16

- *For example, due to the availability of large amounts of data, the tax assessment process lends itself to be carried out either partially or fully automated.*
- *In the social insurance sector, the decision regarding eligibility for premium reductions is well-suited for full automation.*
- *In building permit procedures as well, the introduction of fully automated individual decisions is being considered as a possibility.*

The potential of automated systems is considered particularly high in the near future for partially automated systems in public administration. This is intended to ensure that existing tasks are carried out more efficiently, more accurately, and thus with greater legal certainty. 17

2. Development

The origins of automated individual decision-making can be traced back to so-called **expert systems**. These are based on structured "if-then" schemas (so-called rule-based systems) and, in this sense, do not go beyond the cognitive decision-making processes of natural persons. 18

In particular, the emergence of **Big Data Analytics**—the ability to analyze very large, unstructured datasets—and the associated technical developments have enabled machine learning methods (often referred to somewhat broadly as "Artificial Intelligence" [AI]) to become established. This has, in a sense, brought about a shift in perspective: Instead of causal relationships—for example, when using artificial neural networks—correlations or probabilities come into play. The datasets are no longer processed using "if-then" schemes; rather, the systems establish their own rules to arrive at a result. In doing so, it 19

often remains unclear how the systems arrive at such a result. The literature does not always clearly distinguish between "simple" automation or a "simple" automated system and situations where machine learning methods are used.

B. Automated Individual Decision

1. Full Automation

20 An automated individual decision within the meaning of Art. 21 FADP exists when a decision is **based exclusively on automated processing** and has legal consequences for the data subject or significantly affects them (para. 21 FADP) . It is required that a decision be made regarding a specific individual (individual decision) based on the processing of personal data. From a public law perspective, an automated individual decision may also be referred to as an "automated administrative decision."

21 The decisive factor is that the processing takes place "without any human intervention." It therefore involves an **assessment of the facts** and decision-making **separate from any natural person**, and thus constitutes full automation within the meaning of the distinction made in this commentary (see N. 15). However, according to the Explanatory Memorandum, full automation is not precluded by the fact that the decision is communicated to the data subject by a natural person, provided the decision can no longer be modified. Various authors, however, take the view that an automated individual decision still exists even if a natural person is involved in the programming process. If this view is followed, an automated individual decision within the meaning of Art. 21 para. 1 of the FADP need not be made entirely independently of human intervention.

2. Legal Consequence or Significant Adverse Effect

22 An automated individual decision further requires that it be associated with a legal consequence or that it have a significant adverse effect on the data subject. According to the Federal Council's explanatory memorandum, the decision is associated with a **legal consequence** if it entails direct, legally prescribed consequences for the data subject. The decision always has a legal consequence when it affects the legal status of the data subject—that is, when it establishes, modifies, or revokes a right for the data subject. Unlike in the case of adverse effects (see N. 24), the legal consequence does not need to be

particularly significant. As an example, the Federal Council cites the conclusion and termination of contracts, each of which entails a legal consequence for the data subject as a contracting party. Specifically, the automated conclusion of an insurance contract is mentioned. In this context, insurance coverage and the obligation to pay premiums are likely to be considered legal consequences. According to the explanatory memorandum, however, premium invoices sent periodically and automatically based on the insurance contract do not constitute an automated individual decision, particularly since the issuance of invoices is already a legal consequence resulting from the conclusion of the contract. Nor does the following constitute a legal consequence in the sense described above: if no contract is concluded with a person. In this example, however, the failure to conclude the contract may nonetheless be understood as an automated individual decision and trigger a duty to provide information if the data subject is significantly adversely affected as a result (see N. 24).

In the context of public law, a legal consequence essentially arises when **administrative decisions** are issued pursuant to Art. 5 APA, as well as in the case of real acts pursuant to Art. 25a APA. The Explanatory Memorandum cites automated tax assessments as an example. 23

An automated individual decision further gives rise to a duty to inform if the data subject is **significantly adversely affected** by it. This is presumed to be the case if the decision has a negative impact on the data subject's economic or personal interests. The situation must reach a certain level of severity; mere annoyance is not sufficient. Factors such as the importance of the affected interest to the data subject, the duration of the decision's impact, or the possibility of resorting to alternatives. Whether the data subject is significantly affected must therefore be determined by assessing the overall circumstances on a case-by-case basis. As a possible example, the explanatory memorandum cites the allocation of medical services or the failure to conclude a contract based on an automated individual decision. 24

The following are further **examples** of automated individual decisions that result in a legal consequence or significant adverse effect for the data subject: 25

- *the conclusion or non-conclusion of a lease agreement, including its terms (e.g., interest rate, payment terms), provided that these elements depend on*

an automated assessment of the data subject's financial situation (legal consequence or significant adverse effect in the event of non-conclusion);

- *a health insurance company's refusal to enter into a contract with the data subject based on the automated evaluation of their health data (significant disadvantage);*
- *the automated issuance of traffic citations based on photographic evidence of the respective vehicle owner (legal consequence);*
- *the automated rejection of an online loan application or an online job application without human intervention (significant adverse effect);*
- *the determination of contractual terms, e.g., for personalized pricing (legal consequence);*

26 The following, however, do not constitute automated individual decisions:

- *the delivery of personalized advertising, as there is no legal consequence or the required degree of adverse effect.*

3. Additional Requirements

27 According to the Federal Council's explanatory memorandum, the assessment should not be based solely on the criterion of "natural person," but must also take into account the **complexity of the system** and the **particular impact** on the data subject. An automated individual decision exists when the automation exhibits a certain level of complexity and results in a legal consequence that is particularly detrimental to the data subject. Simple "if-then" decisions are not to be classified as automated individual decisions.

- *As an example, the Federal Council cites withdrawing money from an ATM. If the account balance is high enough, the withdrawal is authorized.*

28 Apart from this example, the required level of complexity for such decisions remains open in the message and is thus, for the time being, unresolved. However, if necessary, the Federal Council will specify in an ordinance when a decision is based exclusively on automated processing.

29 In the government context, some authors focus on the discretionary leeway in decision-making. Other voices, however, explicitly state that an automated individual decision may not be made if the authority is granted discretion. Building on the criterion of complexity, Braun Binder notes that the required

level of complexity can be determined by a reverse inference: automated individual decisions are those that do not require any fact-finding.

4. Assessment

Neither the text of the law nor the explanatory memorandum specifies exactly when an automated individual decision exists. The reference to the "complexity" of the system is of little help. This could give the impression that the provision applies only to fully automated decision-making processes based on machine learning (or "AI") , while any process based on if-then schemes would not be covered. This can hardly be true, particularly for public administration, since most of the algorithms it uses are based on if-then schemes. The data protection provision would consequently have no substantive effect. To prevent Art. 21 of the FADP from being rendered ineffective, rule-based "if-then" schemes must also be covered. The hurdle regarding the requirement of complexity is therefore unlikely to be too high in practice. 30

It is also regrettable that decisions based on partial automation—in the form of decision support or review (see N. 13 et seq.) —are not subsumed under the concept of an automated individual decision pursuant to Art. 21 para. 1 of the FADP. In many cases, the applicability of this provision will be blocked in practice. This is all the more troubling given that partial automation, just like full automation, raises issues relevant to personal rights and fundamental rights (such as those concerning discrimination; see N. 4). This is all the more true when partial automation is based on complex machine learning methods. 31

C. Duty to Inform

Art. 21 para. 1 of the FADP stipulates that the controller must inform the data subject of an automated individual decision. In light of the definition of an automated individual decision (see N. 20 et seq.), the duty to inform therefore applies only if the decision results in a legal consequence or a significant adverse effect on the data subject (see N. 22 et seq.) . 32

1. Timing, Content, and Form

Neither the Act nor the Explanatory Memorandum provides detailed information regarding the timing, form, and content of the duty to inform in the case of an automated individual decision. 33

34 With regard to the **timing**, the controller is free to choose whether to inform the data subject before (*ex ante*) or after (*ex post*) the automated individual decision has been made. Even if there were good reasons for providing information in advance—such as the possibility of opting out of an automated individual decision without having to resort to legal action— and although a corresponding statutory clarification would be warranted, this is not provided for under the wording of the provision. In this sense, the exercise of data subjects' rights under Art. 21(2) of the FADP (statement of position and subsequent human review of the decision; see N. 49 ff.) is currently also sufficiently addressed as one of the regulatory objectives of the duty to inform through *ex post* notification.

35 With regard to the **form**, reference can be made to Art. 13 of the General Data Protection Regulation (GDPR), which requires notification to be provided in a precise, transparent, understandable, and easily accessible form. This provision generally refers to the duty to inform when collecting personal data. An analogous application to Art. 21(1) of the FADP is justified due to the identical wording ("informs") justify an analogous application to the provision of information regarding an automated individual decision. The controller may fulfill the duty to provide information, for example, by publishing the details in an easily accessible privacy policy on its website or by including a link to it in a contract. The identification of the automated individual decision (see N. 57 ff.) is mandatory only for federal agencies and, *a contrario*, voluntary for private entities.

36 The duty to provide information serves the purpose of transparency and the goal of making all information available to a data subject so that they may exercise their rights under Art. 21 para. 2 of the FADP. To ensure this, the controller must provide information on the following:

- Information that an automated individual decision will be made or has been made (depending on when the information is provided);
- a clear specification of which decisions or categories of decisions are made automatically (whereby only those falling under Art. 21 para. 1 of the FADP are covered);
- the possibility of exercising the right to present one's point of view and to have the automated individual decision reviewed, along with details on how to exercise these rights (e.g., the controller's contact information).

In our view, based on the logic of automated individual decision-making, there is **no** obligation to provide this information. Rather, to obtain such information, the data subject may exercise the right of access. As a result, the controller must explicitly inform the data subject of the existence of the automated individual decision and the decision-making logic (see para. 2(f) of FADP). 37

The duty to provide information under Art. 21 para. 1 FADP must always be fulfilled by the controller in addition to the general duty to provide information upon data collection under Art. 19 FADP. However, it is possible for the information to be provided in the same place or in the same document (see N. 35 regarding the requirements for form). 38

2. Assessment

The duty to provide information also implicitly requires that the decision be a **fully automated** individual decision. For the authors' assessment of this circumstance, see N. 31. 39

III. RIGHTS OF THE DATA SUBJECT (PARA. 2)

Art. 21(2) FADP grants various rights to the data subject affected by an automated individual decision. The data subject may present their point of view (A.) and have the decision reviewed by a natural person (B.). This suggests that the information provided under para. 1 must enable the data subject to exercise the rights set forth in para. 2. 40

A. Right to Present One's Point of View

The data subject affected by an automated individual decision must have the opportunity to present their point of view. **Upon request**, the data subject should, on the one hand, be able to express their views on the outcome of the automated individual decision. On the other hand, they should be able to receive information about how the automated individual decision was reached. The information regarding the process by which the automated individual decision was reached is intended, in particular, to prevent data processing from being based on incomplete, inaccurate, or outdated data. 41

1. Individuals

42 Private individuals will have an interest in the right to present their point of view, in particular, if the automated individual decision turns out to be **erroneously negative** for the data subject. If, for example, the creditworthiness of the affected private individual is rejected, this can also have negative consequences for the private controller if, as a result of the decision, no contractual relationship is established between the parties.

43 The law does not specify the **timing** for presenting the point of view. Accordingly, this may take place either before or after the decision is made. From the perspective of the private controller, this does not pose any difficulties as long as this opportunity exists at *any* point in time.

44 The private controller may charge **fees** for granting the right to be heard. However, it may be in the controller's interest to keep these fees low so as not to prevent the potential conclusion of a contract.

2. State

45 In the state context, the right to present one's position under data protection law is to be understood as a consequence of the **right to a fair hearing** pursuant to para. 2 of Art. 29 of the FC. As a fundamental constitutional procedural guarantee, the right to a fair hearing must be granted in every state proceeding.

46 According to Federal Supreme Court case law, a person affected by a government decision must be able to comment (in writing) on the relevant elements of the facts **before** a decision is made that affects their legal status. However, according to the explanatory memorandum to the FADP, the presentation of one's position may also take place after the decision has been rendered, e.g., by filing an appeal. Since the right to be heard confers the right to be heard before the deciding authority, only a non-devolutive appeal—such as an objection with appellate effect—is admissible. The goal is to obtain a decision in the form of an objection ruling from the authority that issued the initial decision.

47 The **objection period** is determined by the relevant procedural laws. It is generally 30 days. The legal basis must be adapted accordingly if automated individual decisions are to be introduced.

Presenting one's position in administrative proceedings must not entail such high **(procedural) costs** that the data subject is deterred from doing so. In principle, therefore, fees may be charged for filing an application. However, in light of the principle of legality, this is permitted only if provided for by law. 48

B. Right to Review by a Natural Person

Para. 2 of Art. 21 of the FADP further provides for the data subject's right to a human review of the automated individual decision. This may be particularly important if the data subject suspects that they have been disadvantaged by the automated individual decision. 49

The review must be conducted by a **natural person with decision-making authority** so that they can overturn the decision if necessary. However, they are free to make their own determinations and are not obligated to overturn the decision. The only requirement, in our view, is that the person review the decision in good faith. 50

In practice, this right to subsequent review is considered **insufficient**, particularly with regard to the potential for discrimination. A preventive review should be conducted to determine whether automated decision-making systems are unintentionally making discriminatory decisions. 51

Neither the law nor the explanatory memorandum to the FADP specifies a particular **time limit** within which the right to review by a natural person must be asserted. For private individuals, a time limit cannot be established as a general rule but will depend on the circumstances of the individual case. Federal agencies may refer to the time limits for reconsideration, as these confer a similar right. In principle, the request for reconsideration is not subject to any time limits, subject to provisions in special laws. However, in light of the principle of legality and to prevent arbitrariness, it seems reasonable that a time limit be explicitly specified, at least at the ordinance level. 52

IV. EXCEPTIONS (PARA. 3)

Art. 21(3) of the FADP provides for **two exceptions** to automated individual decisions in which neither the duty to inform nor the additional rights of the data subject apply. As Vasella and Henseler aptly note, given the clear statutory provision and the systematic position of the provision, it must be assumed that the exceptions to the duty to inform provided for in Art. 20 of the FADP 53

regarding the collection of personal data are not transferable to the duty to inform in the case of automated individual decisions pursuant to Art. 21(1) of the FADP. This distinction is also confirmed by the wording of Art. 20(1) of the FADP. Even if an automated individual decision is based on a legal basis (see Art. 20 para. 1 lit. b FADP), the controller cannot invoke an exception to the duty to provide information under Art. 21 para. 1 FADP.

54 The **first exception** under Art. 21 para. 3(a) of the FADP applies if the automated individual decision is directly related to the conclusion or performance of a contract between the controller and the data subject and fully complies with the data subject's request. In such a scenario, the legislature assumed that the data subject has no interest worthy of protection in receiving additional information or in exercising further rights.

55 As the **second exception**, Art. 21 para. 3(b) FADP cites the data subject's explicit consent to the automated individual decision. The legislative materials do not contain detailed information regarding the requirements for such consent. According to the legislature's understanding, valid consent requires, at a minimum, prior and sufficient information. Various authors in the literature, however, assume that the general requirements for consent to data processing are also appropriate in the context of automated individual decision-making.

V. AUTOMATED INDIVIDUAL DECISION-MAKING BY A FEDERAL BODY (PARA. 4)

56 Finally, para. 21(4) of the FADP contains a special provision for federal bodies within the meaning of Art. 5(i) FADP. This provision imposes on them the obligation to label automated individual decisions (A.). Furthermore, in certain cases, para. 21(2) FADP is not applicable (B.). However, due to the lack of detailed regulations, the provision does not permit federal bodies to make automated individual decisions (C.).

A. Identification Requirement

57 The purpose of the identification requirement for automated decisions is to make it clear to the data subject that the **decision was not made by a natural person**. In principle, the data subject has the right to appeal against such decisions. The identification allows the data subject to exercise their right to a

fair hearing (Art. 29 para. 2 of the FC) in the appeal proceedings by presenting their position and having the decision reviewed by a natural person.

It is questionable how the labeling requirement relates to the duty to inform under Art. 21(1) of the FADP. Unlike the duty to inform regarding the collection of personal data under Art. 19(1) FADP, the latter does not lapse if the processing is provided for by law (para. 20(1)(b) FADP). Given that automated individual decisions in public administration are to be introduced in the future, particularly in mass-processing procedures (see N. 16), it is questionable how the government controller is to comply with the duty to inform (in individual cases). Labeling, on the other hand, appears more targeted in light of procedural efficiency. 58

The label must be clearly and easily recognizable on the automated decision. In our view, it makes sense to place the notice after the actual content of the decision, but before the information on legal remedies. In this way, the data subject first learns that the decision was made by automated means before being informed of their options for legal protection. This corresponds to a natural reading sequence. If the label were placed after the information on legal remedies, there would be a risk that the data subject would notice this information too late or not at all, and thus make an uninformed decision regarding legal protection. 59

B. Non-Applicability of Art. 21(2) FADP

The rights of the data subject under Art. 21(2) FADP to present their point of view and to have the automated individual decision reviewed by a natural person generally apply to automated individual decisions made by federal agencies as well. However, pursuant to Art. 21(4) of the FADP, however, these rights do not apply if the data subject is not required to be heard under Art. 30(2) of the APA or another federal law. 60

Art. 30 of the APA specifies the right to a fair hearing under Art. 29(2) of the APA. Pursuant to para. 1, the parties must generally be heard before a decision is issued. This right is restricted in para. 2. Exceptions to the right to a hearing exist, for example, when a decision is subject to appeal (Art. 30, para. 2, lit. b APA) or when the authorities fully grant the parties' requests (Art. 30, para. 2, lit. c APA) . This is intended to avoid duplication in the decision-making process and to ensure that the substance of the right to a hearing is not under- 61

mined. In an objection proceeding, the right to a hearing can be exercised retroactively. If, however, the parties' requests are granted in full, this interest no longer applies.

62 Ultimately, the exception under data protection law means that the FADP does not grant individuals affected by an automated individual decision by a government agency any rights beyond those already provided for by the APA: If the parties are required to be heard under para. 30(1) APA anyway, they are also entitled to the—no more extensive— – rights under Art. 21(2) FADP. If an exception under Art. 30(2) APA applies and the party does not have to be heard, that party cannot rely on the right to be heard under data protection law pursuant to Art. 21(2) FADP. The rights under Art. 21(2) FADP are, with regard to automated decisions under federal law, **of a declaratory nature** and may even have created legal uncertainty for the data subject.

C. Lack of a General Intention to Grant Admissibility

63 Legal scholarship raises the question of whether, by enacting Art. 21(1) of the FADP, the legislature intended to introduce a general admissibility standard for automated individual decisions in Switzerland. According to the Federal Council, state-administered automated individual decisions constitute "ordinary administrative decisions" within the meaning of Art. 5 APA that are issued without human intervention. In contrast to the European regulation, which establishes a general prohibition on automation subject to authorization under Art. 22 para. 1 DSGVO and thus provides for a general inadmissibility (see N. 69 et seq.), Swiss law appears to assume the admissibility of such decisions largely without preconditions. The blanket reference to Art. 21 of the FADP gives the impression that the FADP serves as a general rule of admissibility for the issuance of automated individual decisions in Swiss administrative proceedings. However, such an intent cannot be inferred from the explanatory memorandum to the FADP, nor is it compatible with the principle of legality (Art. 5, para. 1 of the FC). The latter requires not only a formal statutory basis (Art. 164, para. 1 of the FC) but also sufficient specificity of the provision. Although the FADP is a formal law, its specificity appears insufficient with regard to fully automated decisions. It is also problematic that the provision does not specify concrete areas of application but simply implies the existence of automated individual decisions.

In addition, as part of the comprehensive revision of the FADP in 2020, other laws were amended to include the term "automated individual decision." The FADP thus serves as the starting point for these cross-references in the relevant (procedural) laws. 64

VI. ENFORCEMENT

The Act primarily provides for criminal sanctions. Private individuals are subject to fines of up to CHF 250,000 if they provide false, incomplete, or no information whatsoever via an automated individual decision (see para. 60(1)(a) FADP). A prerequisite for imposing a sanction is the timely filing of a criminal complaint as well as intentional conduct. The fine provision does not apply to federal agencies. 65

Furthermore, the FADP provides for **supervisory measures**. Thus, violations of the obligations under Art. 21 FADP may be reported to the FDPIC. In such cases, the FDPIC may require the controller to provide the information to the data subject and to grant the data subject the opportunity to present their point of view or to have the automated individual decision reviewed by a natural person (see para. 51(3)(c) of the FADP). This applies equally to controllers in both the private and public sectors. 66

The FADP contains no provision regarding whether and how the controller must **correct** an erroneous automated individual decision. Consequently, there are occasional criticisms that it does not provide sufficient and effective protection against the consequences of automated individual decisions. In the specific case where a violation of the duty to inform and the right to be heard breaches the processing principles under Art. 6 of the FADP, this may constitute unlawful data processing by a federal agency (para. 41(1) of the FADP) or an infringement of personal rights by a private controller (Art. 30 of the FADP). In the context of automated individual decisions, a violation of the principle of purpose limitation (Art. 6 para. 3 FADP) is a likely outcome. As a result, the data subject is entitled to demand the elimination of the negative consequences of the unlawful data processing (see para. 41(1)(b) of the FADP for federal agencies and para. 32(2) of the FADP for private entities). 67

In the context of law enforcement under public law, it is **unclear** how the aforementioned right to remedy relates to the administrative procedural remedies available in the event of a violation of the right to be heard. This le- 68

gal uncertainty stems from the fact that the right to a hearing or review under para. 21 2 FADP does not confer any rights beyond the existing right to a fair hearing under Art. 30 para. 1 APA. The problem is exacerbated if official action in connection with the issuance of a decision that violates the obligations under Art. 21 FADP were to be classified as unlawful data processing (see Art. 41 para. 1 FADP) . Under the FADP, the data subject has the option in this scenario to demand the elimination of the consequences of unlawful processing (Art. 41 para. 1(b) FADP). This suggests that a decision issued in violation of the right to a fair hearing would have to be revoked as a consequence of unlawful data processing. This would call into question the finality of decisions, particularly after the expiration of appeal periods.

VII. COMPARATIVE LEGAL NOTES

A. European Regulation (Art. 22 DSGVO)

69 The DSGVO contains a provision comparable to Art. 21 of the FADP. Under the heading "Automated individual decision-making in specific cases, including profiling," **Art. 22 para. 1 of the DSGVO** grants a data subject the right not to be subject to a decision based solely on automated processing —including profiling—that produces legal effects concerning the data subject or similarly significantly affects the data subject.

70 The difference from Art. 21 of the FADP lies in particular in the **regulatory approach**. Legal scholars commenting on Art. 22 of the DSGVO are divided on whether the European provision generally prohibits automated individual decision-making or whether data subjects are granted a right to object. The European Court of Justice (ECJ) in The Hague assumes—without providing much justification — that there is a general prohibition on automated individual decision-making. In contrast, the wording of Art. 21 para. 1 of the FADP generally permits automated decisions.

71 **Article 22 para. 2 of the DSGVO**, however, permits automated individual decision-making in exceptional—and exhaustive—cases if the decision is necessary for the conclusion or performance of a contract between the data subject and the controller (subparagraph a), if it is permitted under Union or Member State law to which the controller is subject and such law provides for appropriate measures to safeguard the rights and freedoms as well as the legitimate interests of the data subject (subparagraph b), or if it is based on the

data subject's explicit consent (subparagraph c). Overall, the Swiss regulation is thus less restrictive than the DSGVO.

Pursuant to **Art. 22 para. 3 DSGVO**, in the cases specified in Art. 22 para. 2(a) and (c) DSGVO, the controller shall take appropriate measures to safeguard the rights and freedoms as well as the legitimate interests of the data subject, which includes, at a minimum, the right to have a person intervene on the part of the controller, to state one's own point of view, and to contest the decision. Further requirements for automated individual decision-making arise from a variety of other provisions in the DSGVO, such as the obligations to provide information and the right of access. In this regard, European law goes beyond the scope of Art. 21 of the FADP. 72

Finally, **Art. 22 para. 4 DSGVO**, unlike the provisions of the FADP, provides for specific restrictions regarding (in Swiss terminology) personal data requiring special protection. 73

B. Case Studies

The FADP introduces the concept of automated individual decision-making into Swiss law. To date, there is no case law on this subject in Switzerland. Even though the (Swiss) FADP and the (European) DSGVO establish different principles regarding the use of automated individual decision-making—the FADP assumes the general permissibility of such decisions, while the DSGVO establishes a prohibition with exceptions (see N. 69 ff.) —and EU practice cannot therefore be adopted unconditionally—it nevertheless provides guidance for Switzerland. 74

1. Distinguishing Between Partially and Fully Automated Decisions

Art. 21 of the FADP contains provisions exclusively regarding fully automated individual decisions (see N. 20 et seq.). Initial examples from the European context show that distinguishing these from partially automated decisions can be difficult. The following section presents two selected examples on this issue that have been reviewed by the European Court of Justice (ECJ). 75

a. Austria: AMAS Algorithm

In a first example, the trial implementation of the automated "Labor Market Opportunities Assistance System" (AMAS) by the Austrian Public Employment 76

Service (AMS) led to the systematic discrimination against women and people with disabilities. The system (automatically) sorted job applications for a specific job description based on data from application documents spanning the past twenty years. Since men had been hired more frequently than women in the past, women (as well as people with disabilities) were not even invited to interviews in the first place. The Austrian Data Protection Authority took action against this. In December 2020, the Austrian Federal Administrative Court issued a ruling regarding AMAS. The primary issue was not the prohibition of discrimination, but rather the question of the legal basis for the use of AMAS. The answer to this question ultimately depended on whether the procedure in question was a fully or partially automated process, as these are subject to different requirements.

77 The parties presented the following differing arguments:

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 The Austrian court agreed with the argument put forward by the Public Employment Service. The court held that the directive is specific regarding the procedure and stipulates that the automatically calculated value must be discussed with the job seeker during a counseling session. The court therefore classified the procedure as partially automated.

79 For Swiss case law, this may indicate that, when distinguishing between partial and full automation, the involvement of a natural person in the process need not be the sole determining factor. Rather, the overall circumstances of the individual case must be considered.

b. Germany: The Schufa Example

80 Schufa is an organization established by German credit institutions and other companies through which contracting parties can obtain information about

potential borrowers. Upon request, it provides a score or rating intended to indicate how reliably the person in question fulfills their payment obligations.

After several individuals in Germany filed lawsuits against Schufa—alleging, among other things, that their records had not been deleted and that they had not been granted access to their data—the Wiesbaden Administrative Court referred the case to the CJEU to determine whether Schufa's scoring constitutes a decision based on automated processing—including profiling—within the meaning of Article 22 of the DSGVO. 81

On December 7, 2023, the CJEU ruled that Schufa's scoring system falls under Article 22 of the DSGVO regarding automated decisions. It found that the following three conditions, which must be cumulatively met under Article 22(1) of the DSGVO, were satisfied: 82

- *Decision:* The CJEU considered credit scoring—as the basis for the subsequent denial of credit—to be (also) a decision, particularly since decisions can also include measures, and the term must therefore be interpreted broadly. According to the CJEU, a narrower interpretation carries the risk of circumventing Article 22 of the DSGVO, for example, by allowing the calculation of the credit score to be exempt from the requirements governing the processing of special categories of personal data (Article 22 para. 4 of the DSGVO).
- *Exclusively automated data processing:* This requirement is met, particularly since Schufa's data processing constitutes profiling within the meaning of Article 4 no. 4 4 of the DSGVO, and the probability score was, moreover, determined entirely by automated means.
- *Legal effect or significant adverse effect:* Since Schufa based its decision—and thus the denial of the loan—largely on the probability score derived from the credit scoring, there is a significant adverse effect on the data subject.

The ruling extends the applicability of Article 22 of the DSGVO to the credit scoring performed by Schufa, which takes place prior to the actual decision to deny the loan. However, the CJEU stipulates that the automated decision to deny the loan must be based primarily on the credit scoring as a kind of preliminary decision. The consequences of this ruling are far-reaching in that automated decisions within the meaning of Article 22 para. 1 of the DSGVO are, 83

in principle, prohibited. An exception applies only if the decision, pursuant to para. 2, alternatively:

- is necessary for the conclusion or performance of a contract between the data subject and the controller (subparagraph a);
- is authorized by Union or Member State law (subparagraph b);
- is based on the data subject's explicit consent (subparagraph c).

2. On Significant Adverse Effects under Article 21(2) of the FADP

84 The question of whether the automated individual decision has a significant adverse effect on the data subject can only be assessed based on the circumstances of the individual case. Three cases from the Netherlands will illustrate when an adverse effect is significant and when it is not.

a. Netherlands: SyRI System

85 In 2014, a law was passed in the Netherlands to introduce the SyRI (Systeem Risico Indicatie) anti-fraud system. SyRI was an algorithmic tool for fraud detection that was limited to neighborhoods in the Netherlands with populations affected by poverty or minorities and created risk profiles of individuals to detect various forms of fraud —such as in the areas of taxation and social benefits—to be detected. In 2020, a Dutch court ordered the immediate suspension of the program, as it violated the ECHR.

86 Although the system did not make any automated individual decisions, the case clearly illustrates when a significant interference is evident. According to the court's reasoning, even such a risk alert has a significant impact on the private life of the person to whom the alert relates.

b. Amsterdam District Court: Uber Taxi Service

87 A lawsuit was filed against the Uber taxi service for violating Article 22 of the DSGVO after Uber automatically suspended drivers' accounts upon suspicion of fraudulent activity. Since the drivers were able to have their accounts reactivated following a review, the District Court ruled that there was no violation of Article 22 of the DSGVO. The temporary suspension of the accounts was not associated with significant, long-term, or permanent effects, which would be required under Article 22 of the DSGVO. Furthermore, the data collected

consisted of factual data such as location and traffic, which is recorded independently of the driver's behavior.

c. Amsterdam District Court: Ola App

The "Ola" app had imposed fare deductions or fines on its users based on data collected by the system. The District Court affirmed the existence of significant effects under Article 22 of the DSGVO. By imposing fines, the consequences for the data subjects were direct and definitive. Furthermore, comprehensive "performance data" relating to a person's general and continuous behavior had been collected. 88

3. Implications for the Swiss Legal Situation

Drawing the line between fully automated individual decision-making within the meaning of Art. 21 para. 1 of the FADP and semi-automated decision-making could prove difficult in practice. The degree of human discretion in individual cases may serve as a point of reference. If this discretion is significant, the decision should be considered semi-automated. Similarly, internal administrative guidelines, employee training, and the opportunity for data subjects to present their arguments may serve as indicators of a semi-automated individual decision. In both cases, Art. 21 of the FADP does not apply. If, on the other hand, a decision is made by a third party, it may still constitute an automated individual decision within the meaning of Art. 21 FADP. 89

Likewise, drawing a line between decisions that result in a significant adverse effect and those that do not may prove difficult. The following aspects may aid in classification: 90

- *The directness of the decision's impact on the data subject;*
- *the temporary or permanent effect of the decision;*
- *the potential influence of the decision on the data subject's behavior or decision-making;*
- *the question of whether the decision restricts potential income opportunities or results in a potential financial loss for the data subject.*

VIII. OUTLOOK

91 The automation of processes and decision-making procedures is advancing rapidly in both the private and public sectors. The Federal Council also anticipates that automated decisions will become more common in the future. Under Article 21 of the FADP, data controllers are required to inform data subjects about automated individual decisions and to grant them certain rights. However, it appears problematic that these obligations apply exclusively to fully automated decisions. Partially automated decisions (decision support or review) are not covered by the scope of the provision. This is problematic because such systems are more widespread in practice and—depending on the complexity of the algorithm used—can have a significant influence on the outcome of the decision. This creates gaps in protection, particularly with regard to transparency and the protection of fundamental rights. Against this backdrop, it is necessary to extend the scope of Article 21 of the FADP to include partially automated decisions. This concern has been addressed in legal scholarship on the use of automated systems. Furthermore, the need for action was also taken into account in the legislative process.

BIBLIOGRAPHY

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.

MATERIALS

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).

COMMENTARY ON

Art. 22 FADP

A commentary by Rehana C. Harasgama / Dario Haux

SUGGESTED CITATION

Rehana C. Harasgama/Dario Haux, Kommentierung zu Art. 22 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Harasgama/Haux, N. XXX zu Art. 22 DSG.

Art. 22 Data protection impact assessment

[1] If processing is likely to result in a high risk to the data subjects personality or fundamental rights, the controller shall carry out a data protection impact assessment beforehand. If several similar processing procedures are planned, a joint assessment may be carried out.

[2] The existence of a high risk, in particular when using new technologies, depends on the nature, extent, circumstances and purpose of the processing. A high risk arises in particular:

a. in the case of the large-scale processing of sensitive personal data;

b. if public areas are systematically monitored on a large scale.

[3] The data protection impact assessment shall include a description of the planned processing, an evaluation of the risks to the data subjects

personality or fundamental rights and a description of the measures to protect personality and fundamental rights.

[4] Private controllers are exempt from having to carry out a data protection impact assessment if they are required by law to process the data.

[5] A private controller may dispense with carrying out a data protection impact assessment if it uses a system, product or service that is certified under Article 13 for the intended use, or if it complies with a code of conduct under Article 11 that satisfies the following requirements:

a. The code of conduct is based on a data protection impact assessment.

b. It provides for measures to protect the personality and the data subjects fundamental rights.

c. It has been submitted to the FDPIC.

CONTENT

IN A NUTSHELL

Art. 22 FADP regulates the requirements for conducting a data protection impact assessment (DPIA). The article is based on the provisions of Art. 35 f. DSGVO. With the help of the data protection risk analysis, an assessment of these risks should be carried out in advance in the case of planned data processing that is likely to lead to high risks for the personality or fundamental rights of the data subjects. In this way, appropriate measures for risk minimization are to be defined and taken before data processing begins. According to the law, a high risk exists in particular in the case of (i) the extensive processing of data requiring special protection (e.g. health data) or (ii) the systematic extensive monitoring of public areas (e.g. the installation of surveillance cameras in a park). However, the list of high risks mentioned in Art. 22 is not exhaustive. Typically, high risks will arise from the use of new technologies and processes, such as algorithmic systems ("artificial intelligence"), DLT systems or Big Data analytics. However, the planned processing activity may also be classified as a high risk to the personality or fundamental rights of the data subjects due to other factors, e.g. because children are involved, automated individual decisions are made or personal data is passed on to a complex network of order processors. However, the violation of the obligation under Art. 22 is not directly punishable.

I. GENERAL

A. Overview

1 In contrast to the DSGVO, the revised FADP does not provide for a general accountability obligation. However, it introduced the obligation to conduct a data protection impact assessment (DPIA) for high-risk data processing operations, which effectively constitutes an accountability obligation for certain data processing operations. The DSFA is not only enshrined in law at the federal level, but also in numerous cantons. In Zurich, for example, the corresponding obligation can be found in Section 10 para. 1 IDG, in connection with prior checking (cf. on the prior consultation procedure at the federal level the commentary on Art. 23).

With the revision, the DSFA is anchored in the Swiss Data Protection Act for all data controllers - for private data controllers as well as for federal bodies. For this reason, the wording of the provision covers both high risks to the personality (for data processing by private controllers) and fundamental rights (for data processing by federal bodies) of the data subjects. The DSFA serves to identify the potential risks of a planned data processing at an early stage, to evaluate them and to define and implement risk mitigating measures. These steps must be taken before the planned data processing is started (see further on the purpose N. 8 ff.). The application of Art. 22 is an outgrowth of the risk-based approach of the FADP, which is particularly evident in the implementation of Art. 22 and 23. 2

DIA is considered to be of increasing importance. This is mainly justified by the increasing spread of advanced algorithmic systems or comparable new technologies in all areas of life, such as distributed ledger technologies or the Internet of Things. In many of the aforementioned applications, personal data is involved and it cannot be ruled out that the personality or fundamental rights of the data subjects are exposed to high risks when using these technologies. In these cases, a DPA is therefore required. The data controller is urged to analyze the planned data processing in advance. At the same time, it should be noted that, particularly in the case of algorithmic systems, certain processes are hardly traceable and their potential cannot be conclusively defined (so-called "black box" problem). Accordingly, it may not be possible to clearly define and delimit the personal data processed and the processing purposes in individual cases, especially since many contract processors and other third parties are often involved in processing the data and the Big Data analyses underlying the systems offer a potential that cannot yet be foreseen. Thus, DSFA in these cases may well be an "ambitious undertaking(s)," but its implementation must be taken all the more seriously. The better this is done, the more likely it is to ensure trustworthy and transparent use of such technologies. 3

B. History of origins

Prior to the total revision, the Swiss FADP did not explicitly require private data processors to conduct a DSFA. However, federal bodies were already required under the old FADP to notify the internal data protection officer or the FDPIC of projects involving the automated processing of personal data (Art. 4

20 para. 2 aVDSG). This notification was linked to the fact that the respective federal authorities had to draw up an information security and data protection concept ("ISDS concept") for the planned data processing. According to the dispatch, this procedure was comparable to the DSFA. For private data controllers, the DSFA was in individual cases possibly based on Art. 7 aDSG. In addition, the data processing principles have always required that the consequences of data processing must always be taken into account. In addition, the FDPIC has in the past required private data processors to submit a DIA in certain cases as part of its advice, especially in the case of high-risk data processing. The introduction of the obligation to conduct a DIA was not least due to EU-wide requirements pursuant to Art. 8bis E-SEV 108 and Art. 27 et seq. of Directive (EU) 2016/680. Art. 35 et seq. DSGVO contain analogous provisions for data controllers that fall within the scope of the DSGVO but do not directly oblige Switzerland in the context of lawmaking.

5 Internationally, the instrument builds on a long history dating back to the 1990s. During this period, the first privacy impact assessments were developed both in the EU Data Protection Directive (Art. 20, Directive 95/46/EC), which was superseded by the DSGVO, and in the Anglo-Saxon world. Other EU member states such as France and Germany have issued corresponding recommendations based on Directive 95/46/EC. These non-binding guidelines aimed at minimizing or, if possible, eliminating potential risks from the outset, especially since such a preventive orientation always proved to be simpler and more cost-effective than adapting processes, e.g., after the fact, to an investigation by the competent supervisory authority. These goals were to be achieved, among other things, by describing the "information flows," involving and discussing with "stakeholders," and writing reports. The provisions of the former Federal Data Protection Act (aBDSG) in Germany, which provided for increased protection for special types of data in Section 3 para. 9 aBDSG, can also be cited as an example. These special data included data on political opinion or health. Before these data could be processed by organizations, the responsible data protection officer had to conduct a so-called "prior check" to ensure proper handling (Section 4d para. 5 aBDSG).

6 The legislative process in Switzerland apparently followed all these developments by providing for a DPA in all preliminary versions of the totally revised FADP. In the preliminary draft, Art. 22 and the related Art. 23 FADP were combined into one Article 16 VE-FADP. However, Art. 16 para. 3 VE-FADP

was more stringent than the provision now in force. The article provided that both the result and the measures taken of any DSFA must be reported to the FDPIC. In the FADP, the impact assessment was then put into two articles and adapted to the structure of Art. 35 DSGVO. In the draft, the list of high-risk processing operations, which thus mandatorily require the performance of a DIA, also included profiling (Art. 20 para. 2 lit. b FADP). However, this processing operation was removed from the list of high-risk data processing operations in the final text of the law as a result of the parliamentary deliberations and in accordance with the applicable legal system. This step is to be welcomed, especially since in many cases profiling will not be classified as particularly sensitive and a DIA would therefore not be justified.

DIA is now standardized in Art. 22 FADP and is applicable to both private data controllers and federal bodies. Thus, the legal norm goes beyond the previously existing obligation for federal bodies from Art. 20 para. 2 FADP and expands it. Within the framework of the new norm introduced with the total revision, there is a lack of further implementing provisions - with the exception of Art. 14 FADP on the obligation to retain data for two years - which could simplify implementation in practice. 7

C. Purpose of the Norm

Compliance with the requirements of Art. 22 serves to ensure that a planned data processing does not lead to a violation of the FADP. The DPA is intended to raise the awareness of the data controller for high-risk data processing, such as the use of algorithmic systems ("artificial intelligence") or Big Data analytics, the use of facial recognition software, the introduction of a patient database or in the context of high-risk profiling. It is therefore a "data protection self-assessment" in the case of particularly high-risk data processing. Art. 22 is an outgrowth of the data protection principles as well as the principle of data protection by design and data protection-friendly default settings (Art. 7). The aim is to identify risks in a first step and to evaluate them analytically in a second step. In this process, the controller should make a forecast about the possible consequences of a planned data processing operation for the data subjects. What matters here is how and to what extent the planned data processing will affect the data subjects. Finally, the standard aims to develop and implement appropriate measures, based on the results of the analysis carried out, in order to (i) mitigate the identified risks of the planned data processing, 8

(ii) draw long-term conclusions from them, and (iii) behave in a data protection-compliant manner overall. If this is successful, the DSFA also offers the possibility to prove compliance with regulations from data protection law to the FDPIC and to save costs in the long run. In this sense, Art. 22 requires the data controller to independently think ahead and examine the risks arising in relation to the planned data processing: Is the planned data processing in compliance with the requirements of data protection legislation? Are the general data protection principles complied with? Is the data processing proportionate? Is data security endangered by the planned processing? Do other risks arise for the personality or fundamental rights of the data subjects? These questions must be addressed regardless of the level of risk, whereby the legislator relies to a large extent on a "hands-on mentality". This should serve to reduce the risks associated with data processing to a level that is perceived as appropriate.

9 The documentation and retention obligations under Art. 14 DPA supplement the obligation to conduct a DIA for high-risk data processing. Thus, the controller is obliged to document a DSFA that has been carried out and to retain it for at least two years after the end of the data processing. In this way, in the event of an investigation by the FDPIC, the data controller is in a position to justify the high-risk data processing and to show how the high risks are countered. From this provision, the character of the DIA as a complementary accountability both to the FDPIC and to data subjects is clear.

II. CONTENT

A. Addressees

10 Art. 22 addresses two actors in particular: federal bodies as well as private data controllers, since it concerns both a risk assessment of the data processing in question in relation to the personality as well as the fundamental rights of the data subjects. Federal bodies already had a similar obligation under the aDSG. Private data controllers as well as federal bodies are affected by this obligation if they fall within the scope of the FADP according to Art. 3 para. 1. This means that private data controllers based abroad are also subject to this obligation, provided that their data processing activities have an impact in Switzerland in accordance with the impact principle and the other require-

ments of Art. 22 are met (see the commentary on Art. 3 for details on the impact principle).

Contract processors are rightly not covered by the obligation to conduct a DIA, especially since they process the data on behalf of a controller and the controller basically decides on the purpose and means of data processing. The risk assessment is therefore fundamentally not within their sphere. While the FADP, in contrast to Art. 28 para. 3 lit. f DSGVO, does not stipulate a duty of support for data processors vis-à-vis data controllers when carrying out a DIA, a duty of support for data processors can, however, also be in their interest. In practice, a corresponding obligation will often be part of the contractual agreements between the controller and the order processor. However, from the data protection principles in Art. 6, an obligation can be derived for commissioned processors to ensure that the data processing transferred to them is carried out in accordance with the data protection principles. If this is not the case, the data controller must be informed that the data processing activity should be adapted. If necessary, it should even be suggested that a DSFA be performed. 11

B. The high risk

Para. 22 provides that the DIA must be carried out in any case where a high risk to the personality or fundamental rights of the data subject can be assumed. Accordingly, a DSFA is not to be performed for every data processing operation. This corresponds to the risk-based approach of the FADP, whereby the risks for the data subjects are specifically in the foreground and not risks that arise for the data controllers. 12

The high risk results from the nature, scope and circumstances as well as the purpose of the data processing. These criteria are comparable to the risks that must be taken into account when determining data security measures pursuant to Art. 1 para. 3 DPA. In this sense, the high risk is present in particular, but not exclusively, when new technologies are used. The more extensive and sensitive these actions and data files are, the more likely the existence of a high risk can be assumed. The planned data processing must be examined, among other things, with regard to the impact on the identity, self-determination or dignity of the person concerned. The high risk does not have to manifest itself effectively: It is a matter of identifying and assessing potential risks that could arise in the course of data processing. 13

14 Pursuant to lit. a and lit. b, a high risk in the sense of a fiction exists if (i) personal data requiring special protection is processed extensively (e.g., when criminal record information is published in a public register, when health applications are used that evaluate the data and make diagnoses, or in clinical trials) or (ii) public areas are monitored extensively and systematically (e.g., the monitoring of a public playground or park or the systematic monitoring of employees' Internet use). The law does not list any other data processing operations for which a DSFA must necessarily be performed. In contrast, the DSGVO provides, for example, that supervisory authorities must publish lists of data processing operations for which a DIA is mandatory.

15 According to the wording of Art. 22 para. 2, neither high-risk profiling nor automated individual decision-making are classified as data processing activities that require a mandatory DIA. At first glance, this seems surprising, especially since high-risk profiling by definition entails a high risk for the data subject and automated individual decisions lead to legal consequences or other consequences that significantly affect the data subject. Against this background, a DSFA must always be performed for high-risk profiling. In the case of automated decisions, however, the situation is different and more complex, especially since a DIA evaluates the data processing itself, which is not necessarily sensitive in the case of these automated individual decisions. What is sensitive here is primarily the result of the decision, which is regulated in Art. 21. A DIA must nevertheless be carried out if the data processing leading to the automated individual decision could in itself lead to a high risk for the personality or fundamental rights of the data subject.

16 The dispatch lists further data processing that could lead to a high risk, namely in the case of processing large amounts of data, the transfer of data to third countries (in this context, reference should be made to the so-called Data Transfer Impact Assessment; see the commentary on Art. 16 f.) or if a large number of persons can access the data. In individual cases, however, it must always be examined whether there is actually a high risk.

17 Neither the FADP nor the FADP contain more precise requirements for determining high risk. Thus, it must always be checked on the basis of the specific planned data processing whether a DIA must be carried out. The EU guidelines, which provide nine criteria for the regulation in Art. 35 et seq. DSGVO provide nine criteria according to which a high risk can be determined. According to the guidelines, as soon as a planned data processing operation

meets two of these nine criteria, there is an obligation to conduct a DIA. The nine criteria are as follows:

- Evaluation or classification of persons or personality aspects with the help of data;
- Automated decision making with legal effect on natural persons or similarly significant effect;
- Systematic monitoring;
- Processing of confidential or highly personal data;
- Large-scale data processing;
- Matching or merging of different data sets, unless this was to be expected;
- Data processing of vulnerable persons (e.g. children, employees or patients);
- Innovative use or application of new technological or organizational solutions (e.g., artificial intelligence, Big Data analytics, or blockchain-based technologies), as their data protection risks have often not yet been accurately elicited; and
- Cases where data processing prevents data subjects from exercising a right or using a service or performing a contract.

While the guidelines from the EU are not applicable in Switzerland, they can be consulted for conducting a DSFA in Swiss and EU data protection law due to the comparable legal requirements. Furthermore, it cannot be ruled out that the FDPIC will publish similar guidelines or apply the lists of data processing operations of the various EU supervisory authorities pursuant to Art. 35 para. 4 DSGVO, which mandatorily require a DSFA, to Switzerland by analogy. The practice will provide more legal certainty with respect to the assessment of high risk.

C. Implementation of the DSFA

1. Introduction

Art. 22 provides clear guidance on the cases in which the controller must conduct a DSFA and what must be observed when conducting it. This includes 18

that the risk assessment must be carried out and documented in a structured manner. The documentation must also stand up to consultation with the FDPIC if, despite the measures implemented, the data processing still results in a high risk to the personality or fundamental rights of the data subjects (Art. 23 para. 1; cf. in detail the commentary on Art. 23).

2. Procedure

19 The DIA must be carried out by the data controller before starting a new or updated data processing activity. This serves to identify the risks of the planned data processing in advance and to implement appropriate measures before legal violations occur. The rule here is: the sooner, the better. However, the one-time, initial performance of the DSFA is not sufficient. Rather, further runs are also necessary during the respective project in order to check whether any adjustments made to the data processing lead to a different assessment and thus other measures appear more appropriate or even obsolete.

20 In terms of content, the DSFA requires three steps, which are defined in para. 3. This is, first, the preparation phase, in which the processing of the data is described as precisely as possible. Secondly, in the assessment phase, the risks are evaluated, and based on this, in a third step, measures are taken to deal with or manage these risks.

21 Before carrying out these three steps, however, private data controllers should check whether they are legally obliged to process data. If there is a legal obligation to process, they are exempt from the obligation to perform a DIA (Art. 22 para. 4). Furthermore, the federal authority or private controller should first conduct a preliminary assessment. This is a general, rather superficial risk assessment to check whether there could potentially be a high risk in the planned data processing (cf. on high risk n. 12 ff.). In this way, it can be clarified in advance whether a DIA is necessary at all. If the controller concludes that the planned data processing is not likely to lead to a high risk, a DIA is not required. However, such a decision should be documented and retained for evidentiary purposes. However, if the controller concludes on the basis of this preliminary assessment that the data processing in question could lead to a high risk, the DIA must generally be performed. An exception exists only in the cases of Art. 22 para. 5.

The preparatory phase includes a detailed description of the (planned) data processing activity. The law does not specify what this description must include, nor how detailed it must be. Depending on the complexity of the planned data processing activity, the DPA may therefore be longer or shorter. However, the description should at least include the type of data processed and categories of data subjects, an explanation of the purpose pursued, the retention period, the processing operations, the recipients, and the place of processing and retention. Otherwise, a complete risk assessment is not possible. This description should indicate why which personal data are to be processed and how. Within the scope of this description, the underlying technologies and systems must be addressed, as well as relevant legal foundations, so that a possible need for legislative action can be identified and implemented at an early stage. 22

This is followed by the evaluation phase, during which the necessity and proportionality of data processing are put into relation with the possible risks. The negative consequences of the data processing for the personality or fundamental rights of the data subject are assessed. High risks or negative effects of data processing can manifest themselves in different ways: For example, data processing can lead to damage to a person's reputation, or the processing of incorrect data can result in incorrect prognoses or diagnoses being made in the medical environment. Situations are also conceivable in which a person is unjustifiably dismissed or loss of confidence in the authorities, the private person in charge or in friends and family occurs. In addition, data processing can also have a financial impact. These and comparable risks must be analyzed in terms of their probability and severity during the assessment phase. 23

In assessing the risks, the data protection principles - above all those of data minimization, data protection by technology and data protection-friendly default settings - must be observed (see n. 4). The informational self-determination of the data subject is also of particular importance, but not the interests of the controller. However, a balancing of interests with regard to the measures to be taken between the interests of the data subject (data protection interest, interest in the freedom to dispose of one's own data) and the data controller (data processing interest) may take place at a later point in time. Although the data relevant for the DSFA does not necessarily have to be "particularly worthy of protection", the "sensitive nature" of the data must be taken into account in the context of the respective DSFA and the measures to be 24

taken. Accordingly, the number as well as the sensitivity of the data are to be considered in this phase. The assessment phase includes the assessment of the severity of the risks and likelihood of those risks occurring. Although this phase is intended to identify a potentially high risk, the risks may also arise after the DSFA has been performed. In this sense, the three phases mentioned above cannot be strictly demarcated from each other.

25 After the evaluation phase has assessed whether the processing of the data involves a high risk to the personality or fundamental rights of the data subject, measures to reduce the risk are defined in the third phase. In this phase, the data controller must therefore not only be aware of what risks exist, but must also make a decision on how to counter these risks. The measures can be organizational, technical or legal or contractual. The data controller must analyze how the planned data processing activity can be adapted so that the high risk is reduced to a reasonable level. Such measures may include, for example, limiting the categories of data, limiting access to the data, encrypting data, changing an order processor involved, changing the place of processing, including certain obligations in the contracts with third parties regarding data processing, etc. However, the measures must be suitable to mitigate the specifically identified risks and cannot be applied by default, i.e. generally with respect to all risks of data processing activities that require a DSFA. They must be defined on a case-by-case basis.

26 The FADP does not specify whether a DIA must be performed only once or on a regular basis. This depends on the data processing activity: If it is one-time, a DSFA performed once is sufficient. However, if the data processing is carried out over a longer period of time and new or higher risks arise due to changed circumstances, the DSFA should be repeated. In principle, however, the DSFA should be repeated approximately every three years. It remains to be seen whether this recommendation will prove effective in the long term in view of rapidly advancing and increasingly comprehensive technological innovations, but it seems rather unlikely from the current perspective.

27 In terms of time, the retention period must also be taken into account. According to Art. 14 DPA, the required documentation of the DIA must be retained for two years. The time limit begins to run with the end of the data processing.

3. Conducting a joint DSFA

The controller has the right to conduct a joint DSFA in the case of several comparable data processing operations. However, this only applies if both the risks and the countermeasures are similar. This option serves to reduce the effort and costs for the controller. However, it is doubtful whether this right will actually lead to a reduction in the burden on data controllers; unless a particular processing platform or application is used in different sectors or projects. 28

4. Organization

The performance of a DSFA is not the responsibility of only one particular person, body or department at the controller. Like any other risk analysis, it is a process in which several persons, bodies and departments must be involved across the board. Within an organization, the DSFA typically involves project management, the IT department and/or chief information security officer, the data protection office or data protection consultant, the legal department, the risk and compliance department, and other key individuals. Each person involved is essential to certain steps of the DSFA. For example, the project management is particularly important for the preparation phase because it can best describe the (planned) data processing. The data protection and legal department is responsible for assessing the risks according to data protection and applicable law. Other departments are of particular relevance for determining the risk mitigating measures. Contract processors who will be used in the planned data processing operation should also be involved in the DSFA. As with any project, it is particularly significant that one person, office or department takes the lead in the DSFA and maintains an overview of the entire process. This leadership is usually provided by the data protection consultant or the project manager at the operational level. Commissioned processors who are used in the planned data processing operation should be involved in the DSFA. 29

From the point of view of the data controller, it therefore makes sense to define an office or department that is familiar with the legal requirements for a DSFA and has the necessary expertise to perform a DSFA. This is usually the office or department responsible for data protection. Depending on the focus or business model of the responsible parties, it may be helpful to create a template including instructions for performing a DSFA that can be referred to 30

in individual cases. In this way, the legal requirements are met without certain aspects being forgotten.

D. Exceptions

31 In addition to the general obligation to conduct a DSFA in cases where data processing leads to a high risk for the data subjects, para. 4 and 5 define some exceptions.

32 Art. 22 para. 4 provides that private data controllers may be exempt from the obligation to perform DIA in individual cases, provided that they are required by law to process the data. In the legislative process, this exemption was justified by the fact that possible risks in these cases have already been weighed and thus there is no further need to conduct a DIA. However, it is rightly pointed out that the exception relates solely to the question of the permissibility of the data processing, not to the manner of the respective processing of data. Thus, the DSGVO is stricter in this respect and requires that the risk analysis carried out in the context of the legislation must relate to the specific processing activity in order for the exception to apply (cf. n. 40). In addition, those cases in which the processing of data does not take place exclusively for the fulfillment of the respective legal obligation must also be taken into account. Legal obligations to process data by private parties can be found, for example, in the Federal Act on Combating Money Laundering and Terrorist Financing (Art. 30 AMLA) or the disclosure of employee data by an employer to fulfill social security obligations (Art. 84 KVG). It is obvious that federal authorities are not covered by this exemption: They may always process data only on the basis of a legal foundation.

33 Art. 22 para. 5 then provides for a further exception. Accordingly, private data controllers may waive the requirement to prepare the DIA if certain conditions relating to the certification of a data processing operation or compliance with approved codes of conduct are met. These exemptions do not apply to federal agencies. On the one hand, this is the case if the controller uses a system, product or service that is certified for use under Art. 13 (see the commentary on Art. 13 FADP for more details). On the other hand, the obligation does not apply in cases where the controller complies with a code of conduct as defined in Art. 11, (i) which is based on a DPAA, (ii) which takes specific measures to protect the personality and fundamental rights of the data subjects, and (iii) which has been submitted to the FDPIC. Currently, no such

codes of conduct exist in Switzerland. However, such codes are conceivable for industries in which the industry participants work closely together and jointly develop standardized processes, such as in banks and insurance companies, in technology or media companies, or in the advertising industry. In the EU, the development of comparable codes of conduct or regulations is governed by Art. 40 DSGVO, with the EU Cloud Code of Conduct, which serves as a harmonized code of conduct for the cloud industry within the EU, currently being known, among others.

III. VIOLATION OF THE OBLIGATION TO CONDUCT A DSFA

If a controller does not perform a DSFA, although a corresponding obligation would exist according to Art. 22, Art. 51 para. 3 lit. d must be observed. According to this article, the FDPIC may order the controller to perform a DIA under penalty of a fine. In contrast, however, data subjects have no right to take legal action to enforce the performance of a DIA. 34

If the FDPIC determines in the course of an investigation that a data processing operation leads to a high risk, he may order that the data processing operation be adapted, suspended or stopped altogether until a DIA has been carried out (Art. 51 para. 1 in conjunction with Art. 49 f). This can lead to considerable delays for the data controller, which in turn entails high costs and additional effort for the data controller. Moreover, since the results of an investigation can be published by the FDPIC (Art. 57 para. 2), there are significant reputational risks for the responsible party. 35

The violation of the obligation to conduct a DSFA is not independently subject to a fine. This provision seems reasonable in light of the fact that this obligation is primarily a due diligence obligation (consisting of a documentation and accountability obligation). In the EU, however, this is handled differently (cf. n. 40 ff.). However, it can be assumed that data controllers will nevertheless comply with their obligations under the FADP. On the one hand, because authorities already had to take such an obligation into account under the aDSG. On the other hand, private data controllers, in particular corporate groups, also carried out FADPs before the entry into force of the totally revised FADP, e.g. because the data processing in question fell under the FADP or the FDPIC had required this. 36

IV. CHALLENGES AND PRACTICAL RELEVANCE

37 With the entry into force of the revised Art. 22, it is apparent that the normative requirements for a DPA have a high degree of complexity. This is particularly true in the case of implementation by small and medium-sized enterprises (SMEs), which have an economic importance in Switzerland that should not be underestimated. For them, it is likely to prove challenging to carry out the individual steps in accordance with Art. 22. This applies in particular to the preparation and the measures phase (see n. 18 ff.), which are time-consuming simply because of the necessary analytical procedure. This is likely to generate considerable costs in individual cases. Accordingly, it can be assumed that the need for templates, advice and assistance from the FDPIC will increase significantly in the near future. In this respect, the obligation of the European supervisory authorities to publish lists defining when a DIA is mandatory must be seen as a step in this direction (Art. 35 para. 4 DSGVO; cf. n. 43).

38 With the increasing use of algorithmic systems and other applications (see n. 2), DPA will also become more important. Data controllers must carefully consider in each individual case which risks appear appropriate and whether the use of such systems is worthwhile. This analytical approach prior to the actual start of the project should not be new, particularly for large companies, especially since corresponding privacy impact assessments were already carried out prior to the total revision (see n. 4 f. and 35) and they should be familiar with comparable obligations at the EU level due to the DSGVO.

39 The DPA also makes clear that in the area of new disruptive technologies, the different areas of law overlap and an increasing blending of legal issues and those regarding the technology used can be observed. One example of this development is the discussions surrounding the Artificial Intelligence Act ("AI Act"). Comparable to the DIA pursuant to Art. 22 FADP, the most recently discussed text is based on a strongly risk-based approach, according to which a differentiation is made between limited, high and unacceptable risk. Thus, especially in the case of high-risk applications, which are defined in Annex III of the AI Act, a conformity assessment procedure must be carried out in accordance with Art. 43 AI Act, which is based, among other things, on Annex VI These requirements, like the DSFA under the FADP, are to be understood as a preventive, ongoing process that includes both legal and technical aspects, as well as serving to further transparency and thus user trust.

V. COMPARISON WITH EU LAW

In general, the implementation of the DSFA according to the FADP is comparable to the EU-wide requirements of the DSGVO. At the same time, Art. 22 f. FADP are less strict than Art. 35 f. DSGVO. In the EU, for example, a DPA must also be carried out if data processing may lead to a high risk to the rights and freedoms of natural persons. In contrast to Art. 22 FADP, Art. 35 para. 3 lit. a DSGVO also explicitly provides for a DIA for automated individual decisions. 40

The lit. a to d of Art. 35 para. 7 regulate comparable steps to Art. 22 FADP, which must be taken into account when a DIA is performed. Thus, the preparatory phase is comparable to lit. a, the evaluation phase is comparable to lit. b and c, and the implementation phase of the measures is comparable to lit. d. Although in Switzerland it can also be assumed that a DIA may have to be carried out again in the course of data processing due to changed circumstances, Art. 35 para. 11 DSGVO even explicitly provides for this in certain cases. 41

While Art. 35 para. 2 DSGVO contains an obligation to consult the data protection officer, at least if one has been appointed, Art. 35 para. 9 DSGVO even provides that the controller may consult the data subjects when carrying out the DSFA. The FADP does not contain such a provision. The consultation of the data protection officer has no influence on the DSFA in terms of content, especially since the role of the data protection officer is not specified. Obtaining the views of the data subjects, on the other hand, is aimed at transparency on the part of the controller as well as self-determination on the part of the data subjects. These consultations reinforce the purpose of the DPA by demonstrating once again that the risks to be assessed are those of data processing for the data subjects and thus not primarily risks for the controller. 42

Unlike in Switzerland, Art. 35 para. 4 DSGVO requires supervisory authorities to keep a list of processing operations for which a DIA must be carried out in any case (so-called positive lists). Basically, the European legislator thus establishes a de facto obligation to conduct a DIA in the cases defined by the supervisory authorities. In addition, supervisory authorities are also authorized to optionally maintain lists of data processing activities for which a DPA is not required (so-called negative lists; Art. 35 para. 5 DSGVO). These lists are subject to the consistency procedure if they include "processing activities which 43

are related to the offering of goods or services to data subjects or the monitoring of the behavior of such data subjects in several Member States or which could significantly affect the free flow of personal data within the Union" (Art. 35 para. 6 GDPR). The FADP does not provide for an obligation to maintain positive or negative lists, although this would be conducive to legal certainty.

44 While Art. 22 para. 5 FADP explicitly states that a DIA need not be performed if a code of conduct pursuant to Art. 11 FADP is complied with and the additional requirements under para. 5 are met, such codes of conduct under the FADP are only to be taken into account in the DIA as part of the assessment of the impact of the data processing in question. However, they do not release the controller from the obligation to conduct a DIA if it is mandatory by law.

45 Finally, similar to Art. 22 para. 4 FADP, Art. 35 para. 10 FADP provides that a DIA does not have to be performed if a data processing operation is based on a lawful basis. However, the exception in the DSGVO is more narrowly defined: The exception only applies if a DIA was carried out as part of the enactment of the legal basis and the legal basis regulates the specific processing operation or operations. The practical significance is therefore likely to be limited. In addition, there is an exception pursuant to Art. 35 para. 10 DSGVO if the data processing is carried out in the fulfilment of public interests or in the exercise of official authority.

46 The DSGVO provides for fines of up to €10 million or up to 2% of the total annual worldwide turnover of the preceding business year for violations of the obligation to conduct a DSFA (Art. 83 para. 4 lit. a DSGVO). This fine contrasts with the FADP, which does not provide for a fine for such a violation (see n. 35).

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 23 FADP

A commentary by Rehana C. Harasgama / Dario Haux

SUGGESTED CITATION

Rehana C. Harasgama/Dario Haux, Kommentierung zu Art. 23 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Harasgama/Haux, N. XXX zu Art. 23 DSG.

Art. 23 Consultation of the FDPIC

[1] If the data protection impact assessment indicates that the planned processing despite the measures planned by the controller will still pose a high risk to the personality or the data subjects fundamental rights, the controller shall seek the FDPICs opinion beforehand.

[2] The FDPIC shall inform the controller within two months of any objections to the planned processing. This deadline may be extended by one month if the data processing is complex.

[3] If the FDPIC objects to the planned processing, he or she shall propose suitable measures to the controller.

[4] A private controller may dispense with consulting the FDPIC if it has consulted the data protection officer under Article 10.

CONTENT

IN A NUTSHELL

Art. 23 is the follow-up regulation to Art. 22. If the controller determines in the course of a DIA that there is a high risk to the personality or fundamental rights of the data subject despite risk-mitigating measures taken, consultation with the FDPIC is required. Its requirements, deadlines and consequences are listed and specified. The FDPIC reviews the planned data processing with regard to compliance with the FADP. If there are objections to the planned data processing, the FDPIC issues an opinion, which also contains recommendations regarding possible measures. This opinion is forwarded to the data controller. The FDPIC may also exercise his powers pursuant to Art. 49 and 51 ff. subsequently to the consultation pursuant to Art. 23. However, a violation of the obligation under Art. 23 is not punishable.

I. GENERAL

A. Overview

Art. 23 describes the requirements for consulting the FDPIC. This is a procedure that is closely related to the data protection impact assessment (DPIA) from Art. 22. If the data controller determines during a data protection impact assessment that, despite the measures taken, there is still a high risk to the personality or fundamental rights of the data subject as a result of the planned data processing, then the FDPIC must be consulted in advance. In this case, the FDPIC checks the compatibility of the planned data processing with data protection law and the requirements for information security. The FDPIC then informs the data controller of his objections by means of an opinion within two to three months. In doing so, the FDPIC is obliged to propose suitable measures to counter the identified risks. 1

B. History

The obligation to conduct a DIA and to consult the FDPIC if the planned data processing leads to a high risk for the data subjects despite the measures taken did not exist before the total revision of the FADP. The obligation also did not exist for federal authorities, which had to conduct a DPA pursuant to Art. 22 aDSG. The European Data Protection Convention (ETS 108+) also does not 2

require the introduction of this obligation. However, the obligation was already provided for in some cantonal data protection laws, for example in the Canton of Zurich in Art. 10 IDG or in the Canton of Bern in Art. 17a KDSG.

3 The possibility or necessity of consultation is, however, based on European legal requirements from 2008, in particular Art. 20 of Directive 95/46/EC, according to which processing operations involving certain risks for individuals, in particular relating to rights and freedoms, must be examined in advance by the data protection officer. This provision continues to have an impact today in Art. 28 of the current Directive 2016/680/EU, which also had to be implemented in Switzerland due to the Schengen acquis in the area of cross-border prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, as well as in Art. 36 of the DSGVO, which was implemented in a comparable manner.

4 The VE-FADP provided in Art. 16 para. 3 VE-FADP for notification of the FDPIC about the results of the DSFA in any case. In line with today's regulation, the FDPIC had to notify the controller of his objections within a certain period of time. The obligation to inform the FDPIC in every case about the result of a DSFA was strongly criticized in the public consultation. The Federal Council then softened the obligation with Art. 21 para. 1 FADP. This weakened standardization was adopted in the current regulation of Art. 23 para. 1, in that the FDPIC only has to be consulted if, despite the measures taken, there are still high risks for the personality or for the fundamental rights of the data subject.

C. Norm Purpose

5 According to the Message, the consultation requirement was included as part of the total revision in 2020 "because it allows the officer to act in a preventive and advisory capacity." This, it is argued, is most efficient for the controller, as potential data protection problems can be identified and addressed at an early stage. Consultation allows the FDPIC to obtain and evaluate the information necessary to assess a planned high-risk data processing operation. This is also beneficial to the democratic process.

6 The purpose of Art. 23 is also to develop solutions already before the implementation of a project that provides for corresponding data processing. This serves to ensure a high standard of data protection from the outset and to

guarantee information security. The legislator thus aims at proactive behavior in order to reduce possible legal violations to a minimum from the outset or, ideally, to exclude them altogether. In addition, it serves to protect the responsible party retrospectively - when data processing has already begun - from additional effort and additional costs. This also appears to make sense in light of the fact that subsequent damage and violations are often difficult to remedy. Overall, the article thus fits into the risk-based approach of the totally revised FADP.

II. CONTENT

A. Addressees

As in Art. 22, the addressees of Art. 23 are federal authorities and private data controllers. This does not include order processors. With regard to the role of these order processors, reference can be made to the corresponding commentary in Art. 22. 7

Federal authorities and private data controllers are thus obliged to consult the FDPIC if a planned data processing leads to a high risk for the personality and fundamental rights of the data subjects despite the implemented measures. The FDPIC, on the other hand, is obliged to carry out the consultation in accordance with the FADP and to adhere to the applicable deadlines (cf. n. 25). 8

B. "Planned" processing

The normative text of Art. 23 provides in para. 1 that the consultation of the FDPIC must be carried out in the case of planned processing involving a high risk to the personality or fundamental rights of the data subject. This provision only applies if the data controller has already taken measures to mitigate the resulting risks and the data processing nevertheless poses a high risk. 9

While the wording suggests that this can only concern new, planned data processing operations, it also covers changes to already existing data processing operations or procedures (cf. the commentary on Art. 69). This means that the FDPIC must be consulted whenever there are changes in the data processing process or changed factual or legal circumstances. However, these changed circumstances must suggest or make it clear that there is a high risk within the meaning of Art. 22. In addition, the measures taken in the context of a re-per- 10

formed or repeated DIA may not be sufficient to reduce this high risk. With regard to the concept of high risk, reference can be made to the explanations on Art. 22 (Art. 22 n. 12 ff.). In favor of the assessment that the FDPIC must also be consulted in the event of changes to existing data processing activities is the fact that, in such a disruptive environment characterized by rapid changes, data controllers must always include the risks in their own considerations and planning of data processing activities so as not to endanger or specifically violate the rights of data subjects (cf. Art. 7).

C. Consultation

1. Introduction

11 First, Art. 23 requires that the data controller has conducted a DIA with respect to a planned or modified data processing pursuant to Art. 22. If the controller concludes that, despite the measures provided for, the data processing poses a high risk to the personality or fundamental rights of the data subject, the controller must consult the FDPIC. Although the law does not contain any formal requirements, this request should be made in writing, if only for reasons of proof. If this high risk does not exist, the controller can still voluntarily submit the DIA to the FDPIC. Although this is conducive to legal and information security, private data controllers are likely to refrain from doing so on a regular basis (cf. n. 34 ff.).

12 The consultation must be carried out before the data processing in question begins. Only after the consultation has been completed, i.e. after the FDPIC has issued an opinion, may the federal authority or the private controller begin processing the data.

13 Three points regarding the consultation must be considered in advance:

- First, the consultation is subject to costs for private data controllers (see Art. 59 para. 1 lit. c FADP; Art. 44 FADP). The respective costs depend on

the personnel expenses in the individual case. In contrast, no costs are incurred for federal bodies.

- Secondly, the FDPIC may, for his part, contact the controller and request an evaluation of the risks and consultation if he becomes aware of planned processing operations.
- Thirdly, the FDPIC may combine this request with the performance of investigative acts (cf. n. 23).

2. Information to be submitted

The provision in Art. 23 specifies the cases in which the FDPIC must be consulted. However, it does not define what information must be submitted to the FDPIC for his evaluation. Due to this initial situation, it can be assumed, or has already been announced, that the FDPIC himself will make corresponding specifications shortly after the entry into force, which the responsible party can use as a guideline. However, the responsible party should at least ensure that the documents created in the course of the DSFA are available in a comprehensive manner so that it is possible for the FDPIC to issue a corresponding opinion at all on this basis. These documents should therefore contain, among other things, information about the planned processing - including the purpose of the processing, if applicable - about the possible risks to the personality or fundamental rights of the data subject, and about the planned technical and organizational measures. It must also be explained why the risk is still considered high despite the measures described. This is important, as otherwise no consultation would be required. 14

The DSGVO can serve as a guide here, as it contains a list of the information to be submitted (cf. n. 39). It can also be helpful to proceed according to the so-called ISDS concept. This provides for a description of the project that is as precise as possible, including an explanation of the legal situation and the organizational and technical measures. In the description of the project, information on the controller and data processor, the purpose and type of data processing, as well as the recipients and data subjects are provided. In contrast, the description of the organizational and technical aspects requires a description of the applications, networks, technologies as well as roles and authorization concepts. It should be noted that in individual cases, more detailed concepts or action plans may be requested. 15

16 In addition, the submitted documents should be submitted in a structured manner and include the applicant's own name and a contact address. This serves as a means of communication with the FDPIC in the event that queries arise in individual cases or there is a need for other clarification.

3. Procedure of the FDPIC

17 Once the relevant documents have been submitted in full (cf. n. 15 ff.), the FDPIC usually proceeds in three steps (i)-(iii): In a first step, the submitted information is reviewed and it is checked whether further information, documents or other details are required for clarification. If this is the case, this information is requested from the responsible party (i). The documents are then carefully examined and analyzed for their comprehensibility and validity (ii). In a third step, the procedure is concluded, with objections being communicated if necessary and measures to be taken being proposed (iii). In these three steps, the FDPIC assesses whether the proposed measures are sufficient to ensure the protection of the personality and fundamental rights of the data subject and to mitigate the high risk.

18 In the first step, the FDPIC examines the information submitted by the data controller and ensures that it understands the data processing operation. In particular, the focus is on the factual as well as the technical description of the data processing in question. If the FDPIC requires further information, he will ask for it and, if necessary, request an oral discussion of the planned data processing with the data controller in order to clarify specific questions. It should be noted here that it is not clear from the wording of the law whether the period for the FDPIC to comment only begins to run after this step or directly upon submission of the request for consultation. However, according to the view taken here, the time limit to comment only starts to run after the complete submission of all information requested by the FDPIC. This means that the duration of the consultation may thus be longer than these two to three months, depending on what additional information and documents the FDPIC still requests.

19 On this basis, the actual review of the data processing in question begins. In this second step, the FDPIC examines in particular the risk assessment and proposed measures of the data controller. This assessment includes a review of the legal requirements, which primarily includes compliance with data protection principles. In addition to proportionality (keyword: data economy and

data avoidance), this includes, among other things, any legal or contractual basis or justification for data processing, outsourcing of data processing or disclosure of data abroad, data security, and the guarantee of data subject rights such as, in particular, the right to information and the right to correction and deletion of data. Both the sensitivity of the data and the parties involved as well as their responsibilities must be taken into account. Furthermore, the technical and organizational measures are examined. This is done in connection with the technologies used and, if applicable, the providers behind them. In the age of increasing cyberattacks and hacker attacks, this serves information security.

After the FDPIC has dealt with these aspects in depth, in a third step it generally draws up an opinion for the attention of the responsible party. In this opinion, it lists its observations regarding the planned data processing and offers an assessment from both a legal and a technical/organizational perspective. If he comes to the conclusion that the data processing complies with data protection requirements, there are no further requirements for the data controller. In this case, the FDPIC does not make any recommendations. In such a case, the FDPIC may even refrain from issuing a statement to the data controller. If the FDPIC raises objections, he combines them with proposals for concrete measures (cf. on measures Art. 22 N. 26.). These measures aim to ensure compliance with both data protection and information security. As a rule, the FDPIC will set a deadline for the responsible party to implement these measures. 20

In this context, a special case should be noted: If, following the data processing carried out, the FDPIC concludes that the measures were not sufficient or that no measures exist at all to reduce the identified risks, he is authorized to conduct an investigation (Art. 49). For this purpose, the FDPIC has at his disposal all administrative measures under Art. 51. The investigation can thus result in, among other things, a suspension or even a ban on data processing. Although it can be assumed that the FDPIC will generally only issue formal orders in isolated cases, the law explicitly leaves this option open to him if data controllers do not handle the risks appropriately. 21

It should also be emphasized that the opinion of the FDPIC is a non-binding recommendation. It does not have the character of an order and can therefore in no way be understood as an approval or even authorization to carry out the planned data processing. 22

4. Time limit

23 If the FDPIC is consulted, he must notify the data controller of his opinion within two months of the complete submission to the FDPIC, in accordance with Art. 23 para. 2. The FDPIC may extend the deadline by a maximum of one month if the data processing is complex. If the data controller does not receive any communication from the FDPIC within this period, it can be assumed that the FDPIC will not raise any objections to the planned data processing.

D. Exceptions

24 Art. 23 provides for some exceptions to the basic obligation to consult. These exceptions are governed by para. 4 and apply only to private data controllers. Federal authorities are thus excluded from the exceptions.

25 Paragraph 4 states that consultation is not required if the controller consults a data protection advisor regarding the planned data processing. In this regard, the message states that the data protection advisor must actually be actively involved in the DPA. He must therefore have been in a position to comment comprehensively on the measures and risks. In view of this circumstance, it appears reasonable to regulate the process of a DSFA as well as the competences and the involvement of the data protection advisor in internal guidelines or directives in a conclusive manner.

26 According to the dispatch, the exception is intended to reduce the administrative burden on private data controllers. From an economic perspective, this exception is to be welcomed. This is especially true since, from the perspective of the private responsible parties, delays, additional costs and potentially negative consequences due to the consultation of the FDPIC can thus be avoided. Although the FDPIC had spoken out against this exception during the consultation, it was nevertheless integrated into the text of the law in the end.

27 The exception should also be interpreted as an incentive for private responsible parties. Thus, the regulation offers them a very specific reason to appoint a data protection advisor. This incentive is important because, in contrast to Article 37 of the FADP, the appointment of a data protection advisor is always voluntary under the FADP.

However, the exception only applies if the requirements of Art. 10 para. 3 are met. Accordingly, the data protection advisor must be professionally independent and not bound by instructions, must be free of conflicts of interest and must have the necessary expertise (see the commentary on Art. 10 for a detailed discussion of these requirements). The controller, on the other hand, must publish the contact details of the data protection advisor and communicate them to the FDPIC. This exception is reminiscent of the exception applicable under Art. 11a para. 5 lit. e aDSG regarding the obligation to notify data collections, which was deleted from the FADP without replacement. Private data controllers are thus already very familiar with these requirements. 28

Private controllers who develop or implement business models or technologies that potentially lead to high risks for data subjects will, based on experience, appoint a data protection advisor and make use of this exception. This will allow them to avoid consulting the FDPIC. This is all the more likely since internationally active private controllers in such industries are already required to appoint a data protection officer under the DSGVO anyway. 29

III. VIOLATION OF THE OBLIGATION TO CONSULT THE FDPIC

In the event that a controller fails to consult the FDPIC in advance despite the obligation under Art. 23, Art. 51 para. 3 lit. e provides that the FDPIC may order the controller to consult him in advance under penalty of a fine. In contrast, however, data subjects have no right to take legal action to enforce consultation of the FDPIC. 30

If the FDPIC determines in the course of an investigation that a data processing operation leads to a high risk, he may order that the data processing operation be adapted, suspended or completely terminated. This applies until a DIA has been carried out and the FDPIC has been consulted (Art. 51 para. 1 in conjunction with Art. 49 f). This step can lead to considerable delays and thus high costs and additional effort for the responsible party. Moreover, since the results of an investigation may be published by the FDPIC (Art. 57 para. 2), reputational risks are to be expected in such cases. 31

However, the violation of the obligation to consult the FDPIC is not independently subject to a fine. This seems logical, especially since it is a duty of due 32

diligence and the FDPIC has corresponding competences (cf. the comments in Art. 22 n. 37). In the EU, a fine is provided for in these cases.

IV. CHALLENGES AND PRACTICAL RELEVANCE

33 The practical relevance of Art. 23 remains to be seen. For example, at least private data controllers will try to avoid the obligation as far as possible by adapting the planned data processing until it no longer leads to a high risk for the data subjects within the framework of the measures taken. It can thus be assumed that the FDPIC will only be consulted in exceptional cases. There are further reasons for this: On the one hand, private data controllers will not want to wait up to three months until they receive an assessment of their data processing and can proceed with their project. Especially since it can be assumed that this time limit will not start until the FDPIC has received all the information it considers necessary from the data controller. In individual cases, this could lead to projects having to be interrupted for significantly longer. The projects may then also involve business-relevant processes and facts which, as soon as they are submitted to the FDPIC, could become public. The latter, for example, because the FDPIC must report on the DSFA in its activity report or is obliged to disclose certain information on the basis of a public request under FoIA. This cannot always be countered by the fact that the FDPIC undertakes to maintain confidentiality. Finally, the consultation of the FDPIC pursuant to Art. 59 para. 1 lit. c FADP is subject to a fee for private data controllers according to the time spent by the FDPIC and is based on an hourly rate of CHF 150-250 (Art. 44 para. 2 FADP), which should not be an underestimated cost in the context of complex data processing procedures. The fees can be increased up to double if the consultation of the FDPIC can be further used commercially (Art. 44 para. 3 and 4 FADP). These costs are in addition to a private data controller's own costs that a DSFA triggers anyway.

34 In cases where a data processing operation is in the public eye and the FDPIC, due to this or the accompanying political pressure, e.g., makes an inquiry towards the controller or conducts an investigation, private controllers are likely to be obliged to conduct a DIA by means of an order, as has been the case in the past (cf. Art. 51 para. 2 lit. d and Art. 49). Such orders will presumably also provide for an obligation to consult the FDPIC for that particular data processing operation.

V. COMPARISON WITH EU LAW

The DSGVO provides in Art. 36 para. 1 for the obligation to consult the competent supervisory authority if a data processing operation could lead to high risks for the data subjects despite measures taken. In this respect, the provision is identical to Art. 23 para. 1 FADP. 35

Similar to Art. 23 para. 2 FADP, according to Art. 36 para. 2 FADP, the competent supervisory authority must notify the controller and, if applicable, the processors involved of any objections to the planned data processing within eight weeks. Such objections may arise because the supervisory authority concludes that the controller "has not sufficiently identified or mitigated the risk." The deadline, on the other hand, may be extended by six weeks, not just one month, from the date of receipt of the request. Such an extension of time must be communicated to the responsible party within one month and must also be accompanied by a statement of reasons. The supervisory authority may suspend these deadlines until it has received the necessary information pursuant to Art. 36 para. 3 DSGVO. The regulations in the EU are correspondingly more detailed than in Switzerland and appear to make sense, especially since they regulate the process and also the obligations of the supervisory authorities with regard to the deadlines in more detail. 36

If the supervisory authority has objections, it must send written recommendations to the controller and, if applicable, to the involved processors, which is very similar to the Swiss regulation, although in Switzerland the recipient of the opinion is generally the controller. The supervisory authority also has the explicit right to exercise its other powers under Art. 58 DSGVO. This is not explicitly mentioned in the FADP. 37

While Art. 23 FADP does not contain any more detailed provisions on what information controllers must provide to the FDPIC in the context of the consultation, Art. 36 para. 3 DSGVO contains a list of the information to be provided: Information on the responsibilities of the controller, joint controllers and, where applicable, the commissioned processors, the purposes and means of the planned data processing, the measures and safeguards provided for the protection of the rights and freedoms of data subjects [as per the DSGVO], the contact details of the data protection officer, where applicable, the data protection impact assessment itself, and any other information requested by the supervisory authority. 38

39 Articles 36 para. 4 and 5 DSGVO then regulate certain rights and obligations of Member States as well as additional requirements that Member States may provide for in their local law.

40 Violation of the obligation to consult the supervisory authority is punishable by the DSGVO, as is the obligation to conduct a DSFA. Thus, the DSGVO provides for fines of up to €10 million or up to 2% of the total annual worldwide turnover of the preceding fiscal year for breach of the duty to consult (Art. 83 para. 4 lit. a DSGVO). This is in contrast to the FADP, which does not provide for fines in these cases (see n. 33).

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 25 FADP

A commentary by Martin Steiger

SUGGESTED CITATION

Martin Steiger, Kommentierung zu Art. 25 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Steiger, N. XXX zu Art. 25 DSG.

Chapter 4 Rights of the Data Subject

Art. 25 Right to information

[1] Any person may request information from the controller on whether personal data relating to them is being processed.

[2] The data subject shall receive the information required to be able to exercise their rights under this Act and to guarantee transparent data processing. In every case, they are entitled to the following information:

a. the identity and the contact details of the controller;

b. the processed personal data as such;

c. the purpose of processing;

d. the retention period for the personal data or, if this is not possible, the criteria for determining this period;

e. the available information about the source of the personal data, if it has not been collected from the data subject;

f. if applicable, whether an automated individual decision has been taken and the logic behind the decision;

g. if applicable, the recipients or the categories of recipients to which personal data is disclosed, as well as the information specified in Article 19 paragraph 4.

[3] The data subject may consent to having personal data relating to their health communicated by a health profession of their choice.

[4] If the controller arranges for personal data to be processed by a processor, it remains under a duty to provide information.

[5] No one may waive their right to information in advance.

[6] The controller must provide information free of charge. The Federal Council may provide for exceptions, in particular if the effort required is disproportionate.

[7] The information shall in general be provided within 30 days.

CONTENT

IN A NUTSHELL

Art. 25 FADP regulates the right of data subjects to information as the "cornerstone of data protection law". Any data subject may request information from data controllers as to whether personal data about him or her is being processed. The right to information is highly personal. Data subjects cannot waive the right to information in advance. The information must include all details that are necessary to enable the data subject to assert his or her rights and to understand the data processing. The minimum content of the information is regulated by law. The information must be provided in a comprehensible form, free of charge and within 30 days. In the case of processing by a processor, the controller remains obliged to provide information. Data subjects have various legal options to enforce their right to information.

I. GENERAL

A. Purpose

1 Chapter 4, "Rights of Data Subjects", comprises the right to information (Art. 25 ff. FADP) and the right to data disclosure or data transfer introduced by the FADP (Art. 28 f. FADP; also: right to data portability). The right to information can be derived from Art. 13 FC on the "protection of privacy" and from Art. 8 ECHR on the "right to respect for private and family life" and is a "cornerstone of data protection law". The right of access must therefore also be explicitly included in data protection clauses in a contract (Art. 16 para. 2 lit. b FADP) and in specific guarantees (Art. 16 para. 2 lit. c FADP) when personal data are disclosed abroad.

2 The right of access is a central legal right for data subjects to find out - within certain limits - what data about them is being processed by whom and for what purpose. In particular, data subjects should be able to use the right of access to check whether their data is being processed in accordance with the principles of data protection law (Art. 6 ff. FADP). The right to information should thus have a control function as well as a preventive effect.

3 The right to information enables data subjects to exercise their right to informational self-determination, if and to the extent that such a right has been implemented in the FADP. The right to information and the correspondingly

provided information often form the basis for the exercise of further legal claims of data subjects such as correction and deletion (Art. 32 and 41 FADP) or objection (Art. 30 para. 2 lit. b FADP), ultimately for the enforcement of the protection of personality.

The right to information pursuant to Art. 25 et seq. FADP supplements the duty to inform pursuant to Art. 19 ff. and goes further in terms of content. Data subjects may receive information that goes beyond what the controller is required to provide, thereby increasing transparency. 4

The three articles on the right to information are structured as follows: Art. 25 FADP determines who can request information and what information data controllers must provide and to what extent. Art. 26 FADP clarifies the conditions under which the right to information can be restricted. Art. 27 FADP regulates the conditions under which the right to information can be further restricted in connection with the media. In the Data Protection Ordinance, Art. 16-19 DPA specify the right to information. 5

B. History of origins

Art. 25 is based on the previous Art. 8 aDSG. Compared to Art. 8 aDSG, individuals may request information from all data controllers (Art. 5 lit. j FADP) and no longer only from the "controller of a data collection" (Art. 3 lit. i i.V.m. Art. 8 para. 1 aDSG). By and large, the previous provisions on the right to information pursuant to Art. 8 aDSG et seq. have been retained and supplemented in places. 6

The duty to provide information - from the point of view of the data controller the counterpart to the right to information of the data subjects - is no longer limited to specific information (as was still the case, in particular, in Art. 8 para. 2 aDSG), but information must be provided that is necessary to enable the data subject to assert his or her rights under the FADP and to ensure transparent data processing (Art. 25 para. 2 FADP). At the same time, an attempt is made to limit the "usual misuse of the right to information to obtain evidence" under the aDSG. In the parliamentary debate, it was also added in particular that information must be provided about "the processed personal data as such" (Art. 25 para. 2 lit. b FADP). 7

II. RIGHT OF ACCESS (PARA. 1)

8 Art. 25 para. 1 FADP sets out the right to information in general terms. Any natural person may request that a controller or person in charge provide information as to whether personal data (Art. 5 lit. a FADP) about him or her are being processed. Responsible private persons and responsible federal bodies are obliged to provide information (Art. 5 lit. j FADP). A justification for or a legal interest in the requested information are generally not required. In the case of federal bodies, the provision of information is an order pursuant to Art. 5 APA, which means that a statement of reasons and instructions on how to appeal pursuant to Art. 35 APA are required.

9 The right to information is of a highly personal nature and is limited to access to personal data. The right to information is non-transferable and non-inheritable. For persons incapable of judgement, the legal representative acts (Art. 19c para. 2 CC).

10 The data subject requesting information must have the data controller take reasonable measures to identify him/herself and cooperate in proving his/her identity (Art. 16 para. 5 DPA). Whether identification with a copy of an official ID is appropriate must be assessed on a case-by-case basis. The obligation under Art. 1 para. 1 aVDSG, according to which the data subject must prove his or her identity, no longer exists. Depending on the data available about a person, the information in an official ID card may not be suitable for identification. In the case of Internet platforms, for example, the persons responsible often only know the e-mail address or a mobile phone number. In this case, identification can be carried out in this way. The general request for a copy of an ID, if necessary even certified, would violate the data protection principles of necessity, proportionality and purpose (Art. 6 para. 2, 3 and 4 FADP).

11 A data subject's request for information as to whether data about him or her is being processed must always be made in writing (Art. 16 para. 1 sentence 1 FADP). The controller may also allow oral requests for information (Art. 16 para. 1 sentence 2 DPA). The right to information is thus potentially made somewhat more low-threshold. The electronic way is equal to the written way (Art. 16 para. 3 DPA). Written form includes any form that enables proof by text.

12 Information about the processed data is provided in writing or in the form in which the data are available (Art. 16 para. 2 sentence 1 DPA). The electronic

way is equal to the written way (Art. 16 para. 3 DPA). The data controller may offer on-site access, which the data subject does not have to agree to (Art. 16 para. 2 sentence 2 GDPR). The data controller may also provide the information orally with the consent of the data subject (Art. 16 para. 2 sentence 3 DPA). In the case of on-site inspection, there is a right to copies. The personal data of the data subject must be protected from access by unauthorized third parties when information is provided (Art. 8 FADP). The data controller may respond in the same form in which the data subject requested information, for example by means of an e-mail that is not end-to-end encrypted. The encryption of e-mail is often impractical and not appropriate. An alternative to e-mail can be instant messaging with standard end-to-end encryption, for example with Signal, Threema or WhatsApp, provided that the data subject requesting information uses such an instant messaging service.

In the case of electronic means, such as the use of e-mail in particular, it should be noted that a request for information or information provided electronically without confirmation of receipt may not be deemed to have been delivered. The burden of proof lies with the sender. In the case of Internet platforms, it may be offered to process requests for information and the provision of information via the platform. However, the data subjects are free to request information in writing. 13

The information must be provided in a form that is comprehensible to the data subject (Art. 16 para. 4 DPA). Comprehensibility, for example in the case of an unusual or not easily readable format of the data, can be ensured by appropriate explanations. According to the wording, comprehensibility concerns the form and not the content of the information. 14

III. CONTENT OF THE INFORMATION (PARA. 2)

In the sense of a general clause pursuant to Art. 25 para. 2 FADP, the information must include the information required to enable the data subject to assert his or her rights under the FADP and to ensure transparent data processing. If no personal data is available, negative information must be provided. 15

Independently of this, Art. 25 para. 2 FADP defines a minimum list of information that must be provided to data subjects: Identity and contact details of the data controller (lit. a, analogous to Art. 19 para. 2 lit. a FADP), processed personal data as such (lit. b), purpose of processing (lit. c, analogous to Art. 19 16

para. 2 lit. b FADP), retention period or, if not possible, criteria for determining the retention period (lit. d), available information on the origin of the personal data (source), if not obtained from the data subject, since in this case the data subject already had to be informed pursuant to Art. 19 f. FADP (lit. e), existence and logic of any automated individual decision pursuant to Art. 21 FADP (lit. f) and any recipients (lit. f, analogous to Art. 19 para. 2 lit. c FADP). The extent to which information that is not listed must be disclosed by the controller only upon request or whether such information must be indicated from the outset is disputed.

17 In the case of the person responsible pursuant to Art. 25 para. 2 lit. a, it may be unclear who is responsible at all, possibly together with others (Art. 5 lit. j FADP). The identity and contact details must be stated or, if already known, confirmed. Whoever receives a request for information will have to inform the data subject - also in view of the general clause - if there is no exclusive responsibility or if no information can be provided due to lack of responsibility. In the case of joint responsibility, the provision of information among the data controllers must be coordinated, whereby data subjects should always be able to request information from one or more data controllers in Switzerland, which is particularly important in the case of additional data controllers abroad. If there are several data controllers, each individual data controller is obliged to provide information (Art. 17 para. 1 DPA). If there is no data controller, in particular in the case of processing by data processors (Art. 8 FADP), the request for information must be forwarded to the data controller or, at the very least, reference must be made to the data controller. The burden of proof that information designated as complete is in fact complete rests with the person responsible. Responsible parties will not normally want to give the impression that the information provided is complete, nor are they obliged to confirm this.

18 According to Art. 25 para. 2 lit. b, only the processed personal data as such must be supplied, i.e. not, for example, individual documents, e-mails, notes or contracts as a whole, but only personal data contained therein. Documents as a whole may be supplied voluntarily, which in practice may be easier for the person responsible or the person in charge, depending on the data. The right of access may only cover processed personal data covered by the FADP (Art. 2 para. 2 FADP), for example, not personal data processed by individuals exclusively for personal use (Art. 2 para. 2 lit. a FADP e contrario). In the case

of large amounts of data being processed, the data controller may request the data subject to provide more details.

Only "data that exists in writing or 'physically' and can therefore be objectively viewed in the long term [...], but not data that can merely be retrieved from memory" may be disclosed. "Irrelevant is the type of storage or the designation" of the data. 19

The right of access to data of deceased persons pursuant to Art. 1 para. 7 aVDSG has not been incorporated into the FADP or the DPA. The provision was most recently qualified in case law as contrary to federal law. 20

What constitutes personal data in the sense of the right to information must be assessed on a case-by-case basis, especially with regard to the criterion of identifiability (Art. 5 lit. a FADP). The standard and at the same time the restriction is the general clause: "Data protection law is only about helping a data subject to be able to assert his or her data protection rights (at least the enforceable claims) and to ensure transparency of data processing (motivated by data protection law)". In particular, the right of access is not intended to be a means of obtaining evidence (cf. n. 7 above). 21

The purpose of processing (Art. 25 para. 2 lit. c) corresponds to that under the duty to inform (Art. 18 para. 2 lit. b FADP). 22

The retention period or, if the communication of a period is not possible, the criteria for determining this period (Art. 25 para. 2 lit. d FADP) can be taken by data controllers from any existing list of processing activities (Art. 12 para. 2 lit. e FADP). As a criterion, reference will have to be made at least to the principle of necessity (Art. 6 para. 4 FADP). 23

In the case of the origin pursuant to Art. 25 para. 2 lit. e FADP, the controller cannot be required to clarify the origin of data. 24

In the case of an automated individual decision, information must be provided in accordance with Art. 25 para. 1 lit. f FADP about this fact on the one hand and about the logic on which the decision is based on the other. The existence in itself should in principle already be known to the data subject due to the obligation to provide information in the case of an automated individual decision (Art. 21 para. 1 FADP; exceptions pursuant to Art. 21 para. 3 FADP). The logic, i.e. the criteria and the underlying data, must be requested by the data subject with reference to his or her right to information. Algorithms may 25

be protected as trade secrets, but the basic assumptions of the algorithm logic must be stated. In the case of "artificial intelligence", the right to information has its limits in this respect, since the person responsible often does not know (and cannot know) which personal data led to the visible result and why.

26 In the case of any recipients pursuant to Art. 25 para. 2 lit. g, it is sufficient to disclose the categories. Categories are, for example, authorities or group companies, whereas names do not have to be disclosed. In addition, information on disclosure abroad must be provided in accordance with Art. 19 para. 4 FADP.

IV. SPECIAL CASES

A. Information by health professionals (para. 3)

27 For personal data relating to health, Art. 25 para. 3 FADP provides that such data may be disclosed with the consent of the data subject by a health professional designated by the data subject. Health data are personal data requiring special protection pursuant to Art. 5 lit. c no. 2 FADP.

28 The provision largely corresponds to Art. 8 para. 3 aDSG. The required consent has been added to enable the data subject to make a free choice. The information can no longer be provided only by physicians, but by all healthcare professionals who are qualified for the case in question. In particular, medical professionals with an entry in the Medical Professional Register (MedReg) must be considered as health professionals.

B. Processing by order processors (para. 4)

29 In the case of processing of personal data by order processors (Art. 9 FADP), the controller remains obliged to provide information. The provision corresponds to the first sentence of the previous Art. 8 para. 4 aDSG, the second sentence of which has been deleted without replacement.

30 A processor who is requested to provide information without being responsible must forward the request for information to the controller(s) or at least refer to the controller(s). Pursuant to Art. 17 para. 2 FADP, commissioned processors must assist the controller(s) in providing information if they have not been commissioned to provide the information. The controller will have to

regulate the provision of information in the contract with the order processor (order processing contract) (Art. 9 para. 1 lit. a FADP).

V. MODALITIES

A. No waiver of the right to information (para. 5)

According to Art. 25 para. 5 FADP, the right to information may not be waived in advance. The provision corresponds to Art. 8 para. 6 aDSG. 31

B. Free provision of information (para. 6)

According to Art. 25 para. 6 FADP, information must in principle be provided free of charge. The corresponding partial provision of Art. 8 para. 5 aDSG ("as a rule [...] free of charge") has thus been taken over. The right to information is based on the assumption that the provision of information is generally possible without great effort if the data is processed in accordance with the law and the ordinance. 32

The Federal Council is given the authority to provide for exceptions to the right to information free of charge, "namely if the effort involved is disproportionate". The Federal Council has made use of this competence with Art. 19 DPA. 33

In the case of disproportionate effort, the provision of information may exceptionally be made dependent on a reasonable contribution to costs of up to 300 Swiss francs (Art. 19 para. 1 and 2 FADP). 34

There is no disproportionate effort if information must be provided about a large amount of personal data because the controller collects (as much as possible) data in his or her own interest. The same applies if the disproportionate effort results from a deficient organization of the data controller. In the case of requests for information to the meineimpfungen foundation following the discontinuation of the meineimpfungen.ch internet platform, the FDPIC recommended that the data subjects who had requested information be reimbursed the fees for certified copies of identity documents that the foundation had demanded. 35

The controller must inform the data subject who requested information about the amount of the cost sharing before providing the information (Art. 19 para. 36

3 sentence 1 FADP). If the data subject does not adhere to the requested information within ten days, the request for information shall be deemed to have been withdrawn without incurring any costs (Art. 19 para. 2 FADP). The first deadline for providing the information pursuant to Art. 18 para. 1 DPO is thereby extended by this cooling-off period of ten days (Art. 19 para. 3 sentence 2 DPO).

37 In practice, cost sharing by the data subject is of little significance. In the case of full cost accounting, the effort of the person responsible in connection with cost sharing often reaches the maximum possible 300 Swiss francs. This effort increases further if the data subject adjusts his or her request for information due to the required cost sharing, so that the person responsible can no longer claim disproportionate effort. It is usually easier for the responsible person to request a specification of the requested information (cf. n. 18 above).

C. Time limit for providing information (para. 7)

38 An initial time limit of 30 days from receipt by the data controller applies to the provision of information (Art. 18 para. 1 FADP). The controller may extend the time limit if the information cannot be provided within 30 days, and in this case must inform the data subject of the new time limit (Art. 18 para. 2 FADP). The information must be provided prior to the expiry of the first 30-day period, as must the information on the postponement, restriction or refusal of the information (Art. 18 para. 3 FADP; cf. Art. 26 et seq. FADP on restrictions to the right of access).

VI. ENFORCEMENT

39 The right to information must be enforced by civil action against responsible private individuals, whereby failure to comply does not in principle constitute a direct violation of privacy. The non-fulfillment cannot be justified according to Art. 31 FADP. The place of jurisdiction for civil actions is at the registered office or domicile of one of the parties (Art. 20 lit. d CPC), whereby no advance on costs must be paid (Art. 99 para. 3 lit. d CPC) and no court costs are awarded (Art. 113 para. 2 lit. g and 114 lit. g CPC). The simplified procedure applies to actions to enforce the right to information (Art. 243 para. 2 lit. d CPC).

The right to information against responsible federal bodies must be enforced by means of a complaint. The data subject who requests information is entitled to a contestable ruling. 40

The FDPIC may, in administrative proceedings pursuant to Art. 49 ff. FADP, the FDPIC may order the provision of information and attach a penalty to the order (Art. 51 para. 3 lit. g and 63 FADP). The data subject has no party status in these proceedings (Art. 52 para. 2 FADP e contrario). 41

The intentional provision of false or incomplete information is punishable by a fine of up to 250,000 Swiss francs at the request of the data subject (Art. 60 para. 1 lit. a FADP). The data subject is entitled to file an application (Art. 30 SCC, in particular Art. 30 para. 1 SCC). In contrast to the DSGVO, the FADP does not recognize administrative fines (Art. 83 DSGVO), although a fine for companies is possible by way of exception (cf. n. 44). 42

Anyone who, as a data controller or responsible party, does not respond to a request for information or falsely claims not to be obliged to provide information is not liable to prosecution. This criminal liability loophole already existed under Art. 34 para. 1 lit. aDSG, with a maximum possible fine of 10,000 Swiss francs (Art. 106 para. 1 SCC). 43

The penalty provision is basically limited to natural persons in the case of responsible private individuals. The risk of a fine is essentially borne by those individual natural persons who provide information, which can also be a subordinate person. Companies can only be punished as an exception; the maximum possible fine in this case is 50,000 Swiss francs (Art. 64 FADP). The criminal liability for the intentional provision of incomplete information does not apply if the impression is not created that the information is complete. There is no obligation to issue a declaration of completeness. For employees of the federal administration and other federal bodies, only disciplinary means are available. 44

BIBLIOGRAPHY

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).

COMMENTARY ON

Art. 26 FADP

A commentary by Martin Steiger

SUGGESTED CITATION

Martin Steiger, Kommentierung zu Art. 26 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Steiger, N. XXX zu Art. 26 DSG.

Art. 26 Limitations on the right to information

[1] The controller may refuse to provide information, or restrict or delay the provision of information if:

a. a formal law so provides, in particular in order to preserve professional secrecy;

b. this is required to safeguard overriding third-party interests; orc.the request for information is obviously unjustified, in particular if does not serve the purpose of data protection or is clearly frivolous.

[2] Furthermore, it is possible to refuse, restrict or delay the provision of information in the following cases:

a. The controller is a private person and the following requirements are satisfied:

The controller's own overriding interests require the measure.
The controller does not intend to disclose the personal data to third parties.

b. The controller is a federal body, and one of the following requirements is satisfied:

The measure is required to satisfy overriding public interests, in particular Switzerland's internal or external security.
The communication of the information may compromise an enquiry, an investigation or administrative or judicial proceedings.

[3] Legal entities that belong to the same group of companies are not third parties within the meaning of paragraph 2 letter a number 2.

[4] The controller must indicate why it is refusing, restricting or delaying the provision of the information.

CONTENT

IN A NUTSHELL

Art. 26 FADP regulates the possible restrictions of the right to information of the data subjects. The controller may postpone, restrict or refuse to provide information for various reasons. In particular, legal obligations such as professional secrecy, overriding interests of third parties and obvious unfoundedness or obvious querulousness can be considered as grounds for restriction. Private responsible parties may invoke their own overriding interests, federal bodies overriding public interests. Restrictions must be proportionate and examined on a case-by-case basis and justified to the person concerned.

I. GENERAL

1 The right of data subjects to information under Art. 25 FADP exists within the limits of Art. 26 f. FADP. FADP. Information may be postponed, restricted or refused by the controller on various grounds of limitation (Art. 26 FADP). The media may invoke further grounds to restrict information (Art. 27 FADP).

2 The "may" provision gives the impression that data controllers are free to decide whether to restrict information. This is not the case, however, because data controllers may often be obliged to restrict information. Art. 26 para. 1 FADP lists legal obligations (lit. a), overriding interests of third parties (lit. b) and obvious unfoundedness (lit. c) as reasons. Further reasons are listed in Art. 26 para. 2 FADP depending on whether the person responsible is a private person (lit. a) or a federal body (lit. b) (cf. n. 8 ff. below).

II. TYPES OF RESTRICTION (PARA. 1 AND 2)

3 Information may be postponed, restricted or refused (Art. 26 para. 1 and 2 FADP). The restriction must be proportionate, also in accordance with Art. 6 para. 2 FADP and Art. 36 para. 3 FC, i.e. necessary, suitable and appropriate or proportionate in the narrower sense. In particular, the restriction must be suitable in form and scope as well as in terms of time to achieve the desired goal.

4 In the event of a refusal, no information is provided at all. The data subject requesting information shall not receive any information for an unlimited period of time. The controller does not inform the data subject whether personal

data about him or her is being processed (Art. 25 para. 1 FADP). If the refusal is limited in time, it is a deferral (cf. n. 6 below).

Restriction means that only partial information is provided, for example by blacking out certain information. Restriction may also mean that information is provided in whole or in part, but that the information is subject to conditions. Such a condition may be that the information provided may not be made available to third parties and may not be published. The data controller may require the data subject requesting information to confirm in advance that he or she will comply with any conditions, also in the form of a confidentiality agreement. Further protection, for example by agreement of a contractual penalty in the case of a responsible private person or by a threat of punishment under Art. 292 SCC in the case of a responsible federal body, is likely to be permissible only in exceptional cases in view of proportionality (cf. n. 3 above). The restricted provision of information, including any conditions, may be limited in time. In this case, it is a postponement (cf. n. 6). 5

In the case of a deferral, the information is not provided in whole or in part within the time limit (Art. 25 para. 7 FADP), but only at a later date. In the case of a responsible federal body, for example, the provision of information may be postponed in order not to interfere with the free formation of opinion and will. 6

In contrast to Art. 9 para. 3 aDSG, Art. 26 FADP does not regulate how to proceed if the grounds for restriction cease to apply. According to Art. 9 para. 3 aDSG, a federal body had to provide the information in this case, unless the provision of information was impossible or only possible with a disproportionate effort. For responsible federal bodies, it can be assumed that this fundamental duty to reconsider will continue to apply. On the other hand, an obligation to reply retrospectively can only be assumed with restraint in the case of private responsible parties, i.e. logically in the case of postponement. 7

III. GROUNDS FOR RESTRICTION (PARA. 1-3)

Art. 26 para. 1-3 FADP conclusively list the possible grounds for restriction. If there is no ground for restriction, the information may not be restricted in any possible way (cf. n. 3 ff. above). If there is more than one ground for restriction, the persons responsible may invoke all the grounds for restriction. All data controllers may invoke the grounds for restriction pursuant to Art. 26 8

para. 1 FADP. The grounds for restriction under Art. 26 para. 2 FADP distinguish between private data controllers and federal bodies. Art. 26 para. 3 FADP concerns only private persons. Whether a responsible person or a responsible person is considered a federal body is determined by Art. 5 lit. i FADP.

A. Legal obligations, in particular professional secrecy (para. 1 lit. a)

9 According to the wording, this ground for restriction applies exclusively to obligations under a law in the formal sense. This reason for restriction was taken over from Art. 9 para. 1 lit. aDSG, except for the now explicit mention of professional secrets. Legal obligations according to an ordinance are not sufficient in the reverse conclusion. Whether the information can be restricted by reference to general official secrecy must be examined in each individual case.

10 Moreover, the duty must relate to the restriction of information to the data subjects. Legal provisions that generally exclude access to personal data are not relevant. A lawyer, for example, may invoke professional secrecy vis-à-vis third parties, inter alia pursuant to Art. 13 FCA, but not vis-à-vis a client as a data subject.

B. Overriding interests of third parties (para. 1 lit. b)

11 Data or information need not relate solely to a data subject requesting information. A reference can also exist to other data subjects (Art. 5 lit. b FADP), but also to other third parties, for example to legal entities. Third parties include, for example, employees of the data controller. Such a relationship and thus any interests of third parties are even possible without personal data about such third parties being affected. Thus, a third party or a third party about whom the controller does not process any personal data could nevertheless have an interest in having the information provided to a person requesting information restricted.

12 If the interests of third parties are affected, the controller must check whether there are overriding interests and, if so, whether these overriding interests require the information to be restricted. The examination, including the weighing of interests, must be carried out on a case-by-case basis. The necessity of

overriding interests shows that the interests of the data subject requesting information are not overriding per se. Conversely, the interests of the respective third party in the restricted information must outweigh the interests of the data subject, i.e., a "certain materiality of the impairment of the position of the third party or parties must be presumed". The reason for restriction was taken over unchanged from Art. 9 para. 1 lit. b aDSG. The exception applies equally to the duty to inform pursuant to Art. 20 para. 3 lit. a FADP.

C. Obvious unfoundedness or obvious querulousness (para. 1 lit. c)

According to Art. 26 para. 1 lit. c FADP, information may be restricted if the request for information is manifestly unfounded, namely if it pursues a purpose contrary to data protection, or is manifestly querulous. These grounds for restriction represent an innovation compared to the grounds for restriction under Art. 9 aDSG and were supplemented in the course of the parliamentary debate, also supported by case law. Abusive requests for information should also be prevented at this point. 13

These grounds for restriction are to be interpreted narrowly. The person responsible may not assume without further ado that a request for information is obviously unfounded or obviously querulous. In particular, requests for information are considered to be obviously querulous if they are obviously intended to "harass or exercise a responsible person (for example, by repetition or in the knowledge of the uselessness of the information)". A request for information is considered manifestly unfounded if it does not attempt to claim data protection rights or to create transparency motivated by data protection law. 14

If a request for information is indeed manifestly unfounded or manifestly querulous, the solution most favorable to the data subject must be chosen. The solution chosen, in particular deferral or restriction rather than denial, must be proportionate (see n. 3 above). 15

D. Overriding interests of private data controllers (para. 2 lit. a and para. 3)

Private controllers may restrict information beyond the grounds of Art. 26 para. 1 FADP if their own interests outweigh the interests of the data subject 16

requesting information (para. 1) and the data concerned are not disclosed to third parties (para. 2). These requirements apply cumulatively. The examination, including any balancing of interests, must take place on a case-by-case basis (see also n. 12 above). The content of the provision corresponds to Art. 9 para. 4 aDSG and also exists as an exception to the obligation to provide information (Art. 20 para. 3 lit. c FADP).

17 Data that serve to protect against theft in a department store, the protection of manufacturing and trade secrets or a high level of financial expenditure are examples of possible overriding self-interest, whereby in the case of the latter, cost sharing in accordance with Art. 26 para. 6 FADP must be examined.

18 Data that is not disclosed to third parties or "real" third parties, i.e. internal data, is basically data that is disclosed only to persons who belong to the same organizational or corporate structure, i.e. not to another organizational or corporate structure, and who may be pursuing different purposes with the data processing than the controller. During the parliamentary debate, a group privilege was created with Art. 26 para. 3 FADP, according to which companies that belong to the same group are not considered third parties within the meaning of Art. 26 para. 2 a no. 2 FADP (the same for the duty to inform; Art. 20 para. 3 c no. 2 i.V.m. para. 4 FADP). The aDSG did not yet know such a privilege and group companies were considered third parties.

19 The exception also applies to companies abroad that belong to the same group. In all other respects, the applicable data protection obligations apply to the disclosure of data to group companies abroad, for example for the disclosure of personal data abroad (Art. 16 f. FADP).

20 Contractors pursuant to Art. 5 lit. k FADP are not considered third parties (see also Art. 9 and 24 para. 4 FADP).

E. Overriding interests of federal bodies (para. 2 lit. b)

21 Federal bodies as data controllers may restrict information beyond the grounds of Art. 26 para. 1 FADP if public interests outweigh the interests of the data subject requesting information (no. 1) or if the information would jeopardize an investigation, inquiry or judicial proceedings (no. 2). The provision essentially corresponds to Art. 9 para. 2 aDSG and also exists as an exception to the obligation to provide information (Art. 20 para. 3 lit. d FADP).

No. 1 mentions in particular the internal or external security of the Confederation as a possible overriding public interest, the safeguarding of which may require a restriction of information. The naming is exemplary, i.e. all public interests can be considered as a reason for restriction, provided that they are overriding and the restriction is necessary to safeguard the corresponding interests. Other public interests that may be considered are - also in accordance with Art. 7 para. 1 FoIA - for example the free formation of opinion and will of authorities, judicial bodies and other public bodies, the implementation of specific official measures in accordance with the objectives, the foreign policy interests or the international relations of Switzerland, the relations between the Confederation and the cantons or the economic, monetary and currency policy interests of Switzerland. 22

No. 2 mentions as a further reason for restriction the possible endangerment of an investigation, an inquiry or official or judicial proceedings. This restriction applies only if and to the extent that the FADP is applicable at all to such investigations and proceedings (Art. 2 para. 3 FADP). In the literature, it is argued that internal investigations which precede disciplinary proceedings, for example, could fall under this provision. 23

Both grounds for restriction must be examined on a case-by-case basis, including any balancing of interests (see also n. 12 and 16 above). 24

IV. DUTY TO STATE REASONS (PARA. 4)

The data controller must give reasons to the data subject for the restriction of information, as already provided for in Art. 9 para. 5 aDSG. The justification must enable the data subject to understand the reason or reasons for the restriction and to examine its lawfulness. In the case of responsible federal bodies, the restriction must be ordered at least at the request of the data subject in the form of a contestable order (Art. 5 APA). There is no obligation to retain the reasons given, but for reasons of proof, it is obvious for the person responsible to retain the relevant communication with the person concerned. 25

The burden of proof for the reason(s) for restriction lies with the person responsible, also with regard to proportionality. In the case of abusive requests for information pursuant to Art. 26 para. 1 lit. c FADP, it is sufficient to show that a request for information "obviously serves in a relevant way a purpose that does not concern data protection," which is a burden of proof. 26

BIBLIOGRAPHY

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).

COMMENTARY ON

Art. 27 FADP

A commentary by Martin Steiger

SUGGESTED CITATION

Martin Steiger, Kommentierung zu Art. 27 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Steiger, N. XXX zu Art. 27 DSG.

Art. 27 Limitation on the right to information for the media

[1] If personal data are processed exclusively for their publication in the editorial section of a periodically published medium, the controller may refuse, restrict or delay the provision of information for one of the following reasons:

a. The data reveals the sources of the information.

b. The provision of information would allow access to drafts of publications.

c. The provision of information would compromise the freedom of the public to shape their own opinions.

[2] Journalists may also refuse, restrict or delay the provision of information if they are using the personal data exclusively as an aid to their own personal work.

CONTENT

IN A NUTSHELL

Art. 27 FADP regulates the media privilege. Under certain conditions, the media and media professionals can restrict the right of data subjects to information beyond the general grounds for restriction. The media privilege is only applicable to personal data for editorial publications in periodically published media. The media privilege serves to protect media freedom.

I. GENERAL

1 It is undisputed that the FADP also applies to the media. Due to the special role of the media, especially in the context of media freedom including editorial secrecy (Art. 17 FC), Art. 10 aDSG already knew a media privilege (restrictions on the right to information for media professionals). This media privilege was adopted essentially unchanged, as was the corresponding justification (Art. 31 para. 2 lit. d FADP, albeit with adjustments compared to Art. 13 para. 2 lit. d aDSG). The title now mentions the media and no longer media professionals, although the provision still applies to media and media professionals.

2 The general types of restrictions (Art. 26 para. 1 and 2 FADP) and the same obligation to give reasons (Art. 26 para. 4 FADP) apply to the media privilege. Likewise, restrictions must be proportionate and must be examined on a case-by-case basis.

II. PREREQUISITES FOR MEDIA PRIVILEGE

3 Data controllers who wish to restrict information with reference to the media privilege must cumulatively meet the following requirements: The personal data concerned may be processed exclusively for publication in the editorial section of a periodically published medium (para. 1).

4 Exclusive processing: The personal data concerned may not be processed for any purpose other than publication in the editorial section of a periodically published medium. Any other purpose that is not mandatory by law, such as professional secrecy (cf. Art. 26 n. 9 f.), means that the information cannot be restricted with reference to the media privilege. Personal data in media archives that are accessible to the public are not covered by media privilege.

Editorial use: Articles, reports, photo spreads, interviews, commentaries and opinion pieces are considered editorial. Viewed comments from readers, traditionally in the form of letters to the editor, are also considered editorial. Internal and other non-editorial purposes, in particular reader marketing and advertising or communication opportunities for the audience without editorial reference, such as chat rooms, are not considered editorial. Reader comments that are not screened prior to publication are also not considered editorial. 5

Publication: The personal data concerned must be processed with the aim of publishing this personal data or at least contribute to a publication. The wording "processed for publication [...]" means that the restricted information is not limited to processing prior to publication, but is dependent on the purpose of the processing, regardless of the time. 6

Periodically published medium: According to Art. 27 para. 1 FADP, media are all means of disseminating information, including digital means such as email newsletters, social media channels and newsletters. The term "medium" is deliberately formulated in an open and technology-neutral manner. Publication must be periodic, i.e., recurring, without the interval or period always having to be the same. Accordingly, a website published once with editorial contributions or a magazine published once with journalistic content does not qualify as a periodically published medium. 7

III. GROUNDS FOR RESTRICTION

A. Protection of sources (para. 1 lit. a)

Any inference from the personal data concerned to sources of information of any kind shall be considered a ground for restriction. The ground for restriction goes beyond the protection of sources under Art. 28a SCC, but at the same time requires that the data actually "provide information" and not merely that there is a corresponding possibility. In the case of source protection alone, it should be noted that this does not guarantee protection of sources, but rather allows media and media professionals to protect their sources under certain conditions. 8

B. Protection of drafts (para. 1 lit. b)

9 This ground for restriction is intended to prevent pre-censorship even if protection of sources (para. 1 lit. a) is guaranteed. It is also referred to as protection of publication: the possibility of prior sifting via the right of access could lead to media and media professionals not publishing content as planned or not publishing it at all. The restriction ground can thus also prevent a "chilling effect".

C. Protection of the public's freedom of opinion (para. 1 lit. c)

10 Freedom of expression and information includes, among other things, the right of every person to form his or her opinion freely (Art. 16 para. 2 FC), including on the basis of the content of the media and media professionals (Art. 16 para. 3 FC). The corresponding justification is intended to protect a well-functioning media landscape.

D. Personal working tool of media professionals (para. 2)

11 This ground for restriction concerns personal data that is not already excluded from the scope of the FADP as personal data processed by a natural person exclusively for personal use (Art. 2 para. 2 lit. a FADP) and is processed by media professionals.

12 Personal information collections or notes would not fall under the exception of Art. 2 para. 2 lit. a FADP if they are disclosed to third parties by media professionals. There may often be a need for this for media professionals, for example in contact with sources and in research.

13 Media professionals are all natural persons who work for the media in the sense of para. 1 in a journalistic, artistic or editorial capacity, on a permanent basis or as freelancers or self-employed, whether paid or unpaid. In 2008, Rosenthal/Jöhri still required a certain level of professional activity and excluded "hobby journalists," which can no longer apply in view of today's media landscape.

BIBLIOGRAPHY

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).

COMMENTARY ON

Art. 28 FADP

A commentary by Samuel Mätzler

SUGGESTED CITATION

Samuel Mätzler, Commentary to art. 28 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Mätzler, art. 28 FADP N. XXX.

Art. 28 Right to data portability

[1] Any person may request the controller to deliver the personal data that they have disclosed to it in a conventional electronic format if:

a. the controller is carrying out the automated processing of the data; and

b. the data are being processed with the consent of the data subject or in direct connection with the conclusion or the performance of a contract between the controller and the data subject.

[2] The data subject may also request the controller to transfer their personal data to another controller if the requirements in paragraph 1 are met and no disproportionate effort is required.

[3] The controller must deliver or transfer the personal data free of charge. The Federal Council may provide for exceptions, in particular if the effort is disproportionate.

CONTENT

IN BRIEF

The right to data disclosure or transfer is, alongside the right of access, the second data protection right of the data subject. It is often referred to as the right to data portability. This right allows a data subject to request certain data that has been actively provided to the controller or collected by the controller, or to have that data transferred directly to a third party. The data must be transferred in a commonly used electronic format. This is intended to enable direct reuse by the data subject or another provider. The new right to data portability was adopted from the GDPR and falls within the scope of both data protection and competition law. It is intended to give data subjects in the data economy the ability to exercise self-determination over "their" data.

I. PRELIMINARY REMARKS

1 Art. 28 of the FADP establishes the data subject's right to have certain data concerning them disclosed (para. 1) or transferred (para. 2). This is also referred to as the **right to data portability** and—alongside the right of access—constitutes the second data subject right within the framework of the FADP. The subsequent Art. 29 of the FADP must be read in conjunction with Art. 28 of the FADP and sets forth possible grounds for restriction.

2 The natural person making the request, whose data is being processed by a controller, has **active standing** to exercise Article 28 of the FADP. The controller who processes the data covered by the right to data portability—or who has such data processed by a processor—has **passive standing**. This may include private individuals and, in rare cases, federal agencies.

II. GENERAL REMARKS

A. Legislative Purpose

3 The legislative purpose of Art. 28 of the FADP remains controversial to this day. While the Federal Council, for example, views the right to data portability as serving competition law objectives (see N. 10), other voices in the literature emphasize consumer protection or data protection objectives. A further

complication in determining the purpose of the provision is that, although the Chambers focused on social networks during the drafting of the regulation, they did not include a corresponding restriction to social networks in the right to data portability. Art. 28 FADP can therefore **apply in numerous contexts and industries**—such as the mobility sector, the healthcare sector, internet platforms, cloud services, or human resources. The only commonality among all these use cases is that they stem from fundamental changes in modern data processing (see also N. 23 ff.). It is only the recently emerged **data economy** that has made the right to data portability necessary. This must be taken into account in determining the purpose of the provision.

From a data protection perspective, the data subject's right to portability is intended to enable **self-determined control over data**. It is intended to break through the de facto power of exclusion that the controller would otherwise have without a right to portability and to elevate the individual—who has hitherto been reduced to the status of a data object—to that of a data subject by allowing them to have a say in how their data is used. This addresses the imbalances between stakeholders created by the data economy. For the first time, the data subject is given a legal means to independently intervene in the data economy and participate in the potential of the data. 4

Closely intertwined with this, however, are **competition law considerations**. In this regard, the right to data portability aims to promote competition in general and foster the free flow of data. Other objectives frequently cited in the literature—such as reducing switching costs or barriers to market entry and preventing lock-in effects—can, in the view expressed here, play only a secondary role: Art. 28 of the FADP is not limited to cases in which a lock-in-effect exists or could potentially exist, and there is no need to prove that barriers to market entry exist or are being reduced. Furthermore, the data controller need not hold a specific market position or even operate in a market at all. 5

Thus, the competition law objectives diverge from a classical antitrust understanding and align more closely with "regulatory law," which operates *ex ante*. These objectives are also underpinned by the idealism of the so-called **Open Web**. This movement, which emerged in the late 2000s, is rooted in the American IT scene and is based on the idea that it is only the free interlinking of content on the Internet (and especially on the World Wide Web), as well as access to it, that has enabled innovation and made today's offerings possible. 6

However, this Open Web is threatened by monopolies and data silos (so-called "walled gardens"), as large internet platforms, in particular, are increasingly isolating themselves from one another. Consequently, the right to data portability can also be seen, on a much more fundamental level, as a response to an internet consisting of walled gardens. The data economy—as it predominantly manifests on the World Wide Web—should be freed from proprietary data silos, and data subjects should be able to switch providers without facing barriers that distort competition.

7 Given the breadth of possible use cases, the aforementioned objectives—which are sometimes very different—are not always easy to reconcile. That said, the right to data portability pursues both data protection and competition law objectives. However, it **should primarily be regarded as a data protection instrument** that *also* pursues competition law objectives. This follows systematically from the fact that the right to portability applies only to personal data and can be exercised solely by data subjects (under data protection law). Accordingly, there is a clear connection to the data subject's personality and their right to informational self-determination. Conversely, no competition law requirements need to be met for the right to be exercised. It is not even necessary for the controller to operate in a market or in a manner relevant to competition.

8 Consequently, the right to data portability in data protection law is **not** (as some argue) **foreign to the system, but rather "system-creating"**. It is an expression of a fundamental legislative decision, according to which the data subject should have the opportunity to have a say in the data concerning them. By enshrining it in the FADP, the legislature made it clear that the focus in the future should be on the data subject.

9 Particularly in light of its somewhat non-linear development in Switzerland (more on this shortly), the right to data portability must also be understood in a broader context: it is an instrument of **Swiss data policy** par excellence and not "merely" an instrument of data protection law. The right to data portability stems from fundamental data policy considerations and is intended to enable the free flow of data in the age of the data economy. In this sense, while it may—as is now the case—be structured under data protection law, it does not necessarily have to be closely linked to the FADP. Indeed, at the very beginning of the deliberations on the FADP revision, the spokesperson for the relevant committee aptly noted: "It is not simply a matter of data protection, but

also of other data policy issues such as portability, etc., which we [...] must address."

B. Legislative History

Art. 28 of the FADP has no counterpart in the aDSG. It is a genuine innovation of the revision, adopted from the DSGVO (see N. 12) . However, **its introduction remained uncertain until the very end**: The Federal Council considered such a provision "problematic" and refrained from including a right to data portability in the (preliminary) draft. It justified this by arguing that such a right was aimed more at enabling data subjects to reuse their data to foster competition than at protecting their privacy. Furthermore, it feared high costs and doubted the successful implementation, as it would require an agreement on data carriers and IT standards among the data controllers. Instead, the Federal Council wanted to examine the introduction of sector-specific portability rights. 10

During the **parliamentary deliberations**, however, the SPK-N nevertheless included a general right to data portability in the bill. This was intended to open up new economic opportunities and shift the balance of power between small and large platforms. A minority also called for the right to be defined even more broadly, so that all data relating to an individual would be subject to the right to data portability. However, the majority of the National Council and the Federal Council were of the view that such a right would go too far in light of potential issues regarding trade secrets. Ultimately, the Chambers decided to enshrine the right to data portability in its current form, "always with the underlying consideration of what will and will not compromise its appropriateness." 11

C. Comparative Legal Notes

The right to data portability was **adopted virtually unchanged** from the DSGVO, which is why the provision in Art. 20 DSGVO can be used as a basis for Swiss interpretation. However, there are specific differences in the wording, which—where relevant—will be addressed in the discussion of the individual requirements. 12

III. CONDITIONS

A. Personal Data of the Data Subject

13 Art. 28(1) of the FADP first provides that the data subject may request the controller to provide "their personal data." It follows that only data relating to a **natural person** is portable (Art. 2(1) and Art. 5(a) FADP). Thus, data not related to the data subject is not covered, unless the controller can link the data to the data subject. Examples include anonymous performance metrics in software, such as information on CPU utilization or memory usage on a user's device. The requirement, therefore, is that the data be closely linked to the data subject's identity.

14 Consequently, data relating to legal entities is not subject to the right to data portability. Data that a data controller **subsequently anonymizes** is also not covered. If the data is pseudonymized, it must be regarded as personal data if the data controller can link it to the data subject.

15 As the Latin language versions make clear, the data must relate to the person making the request. However, nothing can be inferred from the ambiguous wording in the German language version ("ihrer Personendaten"), which would also allow for a different, broader interpretation. It follows that **purely third-party data**—that is, data relating exclusively to third parties—is not subject to the right to data portability.

16 However, there is debate regarding data that relates *also* to third parties, such as photos in which multiple people are depicted.

Since the grounds for restricting the right to data portability in Art. 29(1) in conjunction with para. 26(1)(b) of the FADP refer to the overriding interests of third parties, it can be assumed that personal data that also relates to third parties may be subject to the right to data portability. This therefore also covers **data with a "dual reference"** that has a certain connection to the data subject, even if the data does not (solely) relate to that person. This applies, for example, to entire chat or email histories or archived bank transactions (including information on payers or payees). Only if there are overriding interests of third parties (or if the data pertains exclusively to third parties) is the data not subject to the right to data portability. If this were not the case, Art. 28 of the FADP would be rendered ineffective in many of the very cases intended by its legislative purpose.

Therefore, the following procedure must be followed to determine whether certain data is subject to the right to data portability: As a first step, the controller must clarify whether the requirements of Art. 28 of the FADP are generally met, in particular whether the personal data in question was provided by the data subject. If the data *also* concerns third parties (but not *only* third parties) and exhibits a dual relationship, a second step must be taken—in the sense of a "restrictive corrective measure"—to weigh whether overriding interests of third parties necessitate a restriction. If there are no overriding interests of third parties, the data may be ported. 17

B. Disclosed Data

The right to data portability is limited to data that the data subject has "disclosed" to the controller. The concept of disclosure is**not to be understood within the meaning of the legal definition in Art. 5(e) of the FADP**. However, this is not necessary for its interpretation: It was already established in the legislative materials during the legislative process which data are meant. The Federal Council subsequently defined the scope of this characteristic in the DSV. In addition, the Federal Office of Justice (BJ) commented on its scope in its explanatory notes. For this reason, the requirement of disclosure in Switzerland (unlike under the DSGVO) is, at least in theory, largely undisputed. In practice, however, difficult questions of demarcation may still arise. 18

According to Art. 20 para. 1(a) of the DSV, data is considered disclosed primarily when a data subject knowingly and voluntarily provides it to the controller (**so-called master data; also "provided data**"). This includes all data disclosed directly and intentionally, such as address information entered as part of an online order or data that must be provided when registering on a platform or filling out a medical history form at a hospital. Passwords or private keys are not included in this category, provided they are encrypted—which should generally be the case—and cannot be linked by the controller to the data subject. 19

Furthermore, data is considered to have been provided if a controller has collected it about the data subject and their behavior in the context of using a service or device (para. 20(1)(b) of the GDPR) . Such **observed data** is generated—knowingly or unknowingly—by the data subject indirectly while using a service or device. This includes, for example, metrics from a fitness app on a 20

smartwatch generated based on athletic performance, the songs listened to on a streaming service, or consumption and location data from a smart vehicle.

21 Not included are **derived data**, i.e., data that the controller generates through its own analysis of data (Art. 20 para. 2 of the Data Protection Act). Since this constitutes an independent activity on the part of the controller, such data is excluded from portability. In this case, the legislature has given greater weight to the protection of the controller's own work and investments than to the data subject's right to enable the further use of "their" personal data.

22 The distinction between observed and derived data must be made on a case-by-case basis and may not always be straightforward. For example, in the healthcare sector, "observing" usually also means "measuring," and a simple measurement is often underpinned by complex technology that operates according to scientific methods. In such cases, the transition from pure observation to derivation can be fluid and difficult to determine.

C. Automated Processing

23 Another limitation is that only data processed automatically by the controller is subject to the right to data portability (para. 28(1)(a) FADP). This is primarily intended to exclude data that is**stored in paper form**. Examples include physical medical history forms in a doctor's office, as long as these are not subsequently transferred to electronic patient records.

24 Only **electronically processed data** is covered. This is because, despite the FADP's inherent technology neutrality, the right to data portability is aimed at digital data traffic and is intended to apply specifically to data traffic on the Internet. However, this requirement **hardly constitutes a restriction** today, as most data processing is likely to be automated.

25 The data controller is under no obligation to digitize data stored in paper form or in any other analog format. However, if data is processed **only partially automatically**, the data controller may be obligated in individual cases to transfer this data, because the restriction does not specify exclusively automated processing. Since the data controller must, in this case, provide or transfer the data in a commonly used electronic format, additional obligations may then apply.

D. Consent or Direct Connection to a Contract

As a further requirement, Art. 28 of the FADP provides for a restriction on data processed with the consent of the data subject or in direct connection with the conclusion or performance of a contract between the controller and the data subject (para. 1(b)). This requirement refers to the **grounds for justifying data processing set forth in Art. 31 of the FADP** and was adopted *tel quel* from the DSGVO. 26

However, the DSGVO is based on the principle of a prohibition subject to exceptions. In Switzerland, by contrast, data processing by private individuals is generally permitted as long as the data subject's privacy is not unlawfully infringed (permission subject to exceptions). Accordingly, under the FADP, a justification within the meaning of Art. 31 FADP is not required in every case for data processing by private individuals. Rather, data processing cannot **unlawfully infringe upon the data subject's personality in the first place**, for example because it is carried out in accordance with the data protection principles (Art. 30, para. 1 and para. 2, subparagraph a, FADP *a contrario*). However, this misinterprets the requirement under para. 28(1)(b) of the FADP. 27

A literal interpretation would thus mean that only data processing operations are subject to the right to data portability if they can be based on the justifying grounds of consent (para. 31(1), Option 1, FADP) or an overriding interest due to a direct connection to a contract (para. 31(2)(a) FADP). While this would ensure that data processing based on a legal obligation is not covered by the right to data portability, there is no apparent reason why **data processing that does not require a legal basis** should be excluded from portability. 28

The legal literature therefore assumes legislative oversight and, in light of the purpose of the provision, advocates for a broader interpretation. The focus should therefore be on the**voluntary nature of the data processing**. Consequently, the initiative for the specific data processing must at least (also) have originated from the data subject. The data processing must not take place completely detached from the will of the data subject. If this is the case, the requirement in Art. 28(1)(b) of the FADP is met, regardless of whether a justification within the meaning of Art. 31 of the FADP is invoked. 29

Conversely, this means that data processing based on another justification is not subject to the right to data portability. This is particularly relevant when a legal basis for data processing exists (Art. 31(1), para. 3, FADP). While the DS- 30

GVO provides for an explicit exclusion of processing carried out in the performance of public tasks (Art. 20(3), second sentence, DSGVO), this is not the case under the FADP. Nevertheless, the restriction in Art. 28(1)(b) FADP already makes it clear that data processing based on a **legal basis** is generally excluded. Accordingly, data processing by federal bodies, which are bound by the principle of legality, is generally not covered by the right to data portability.

IV. LEGAL CONSEQUENCE: PORTABILITY

31 If the conditions set forth in Section III are cumulatively met, the data subject may request that the data be provided to them (para. 1) or transferred to another controller (para. 2). Both the provision and the transfer of the data must be made in a commonly used electronic format (see N. 38 et seq.).

32 Exercising the right to data portability does not alter the **legal relationship** between the data subject and the controller. Consent that has been granted is not deemed revoked, nor is any contractual relationship between the parties affected. The controller may continue to assert grounds for justification. Consequently, the controller is not required to delete the ported data.

A. To the data subject (disclosure of data; para. 1)

33 Under the basic provision of Art. 28(1) FADP, the controller discloses the data **to the data subject**. The data subject may then use the data for purely personal purposes (such as storing a photo collection locally on their computer) or independently transfer it to a third party of their choice. The latter, however, is not a process based on Art. 28 FADP.

B. To a Data Controller (Data Transfer; para. 2)

34 According to Art. 28 para. 2 FADP, a **direct transfer to third parties** (referred to in Art. 28 as "another data controller") is also possible upon request by the data subject. To this end, all the requirements under para. 1 must first be met. In addition, however, the transfer must not entail a disproportionate effort. Para. 2 is satisfied if the third party can obtain the data directly from the controller with passive legal standing, for example because the controller grants the third party access via an application programming interface (API). However, there is no legal entitlement to this.

Art. 21 para. 3 of the DSV specifies that a disproportionate burden exists if the **transfer is technically impossible**. Such an impossibility, however, is unlikely to ever arise, since the disclosure of data to the data subject is, from a technical standpoint, neither simpler nor more complex than the transfer of data to another controller. Since the controller is legally obligated to disclose the data under para. 1, a data transfer under para. 2 should also generally be possible (without disproportionate effort). This is all the more true given that the controller must design its systems from the outset in such a way that it can fulfill its legal obligations (Art. 7 FADP). 35

Of course, a third party is not obligated to accept the data or to ensure the technical feasibility of the transfer. It has **no role under data protection law** as long as it has not received any personal data and is therefore not processing it. In this respect, the term "other controller" in the law is misleading, especially since Art. 28 FADP—unlike Art. 20 DSGVO—does not include a prohibition on obstruction that would impose obligations on the "other controller" regarding the right to data portability. Under EU regulations, it is therefore posited that technical feasibility must relate to the relationship between the controller and the third party. A transfer is always considered disproportionate if the data processing systems of the controller and the third party are incompatible. The requirement thus relates to a characteristic of the third party without imposing any obligations on it. 36

No disproportionate burden can be inferred from the costs incurred by the controller. The right to data portability is a right of the data subject that must be granted regardless of any implementation costs. The costs incurred for the transfer to a third party therefore cannot be invoked, especially since it is difficult to see how such a transfer would entail higher costs than the disclosure of the data to the data subject. 37

C. Data Format

Art. 28 of the FADP provides for the disclosure or transfer in a **common electronic format**. These should be data formats that enable the data to be transferred with reasonable effort and reused by the data subject or another controller (see Art. 21 para. 1 of the FADP). 38

Since this clarification is of little help, **the provision in Art. 20 of the DSGVO must be consulted**, even though the Swiss wording was modeled more 39

closely on that of the right of access in Art. 15 para. 3 of the DSGVO. Art. 20 of the DSGVO refers to a "structured, commonly used, and machine-readable format."

1. Common

40 A format is considered common if it is widely used in the relevant industry for the type of data in question and within the relevant geographic area. However, too much emphasis should not be placed on the geographic area. In the globalized data economy, Switzerland is not a technological island, and the requirement for commonality would thus be set unnecessarily high. Nor does commonality correspond to the state of the art. What matters is not which format appears to be the "best," but rather what **is most widely used** and has thus proven itself in practice. Consequently, a format is considered common when it has established itself as a standard. The focus should therefore primarily be on industry standards and common practice.

41 Excluded from this, however, are **proprietary formats**, which may be widespread but can only be licensed at high cost. They are not to be considered common, nor are formats used solely for internal purposes. Conversely, **open formats are not common per se**, but must be generally used and widespread. If no common formats exist (yet) in a particular sector, the responsible party should resort to such generally used open formats, such as XML, JSON, or CSV.

42 Common use must be assessed from the **perspective of the data controller with passive legal standing**: A DICOM file (for Digital Imaging and Communications in Medicine, with the file extension .dcm) may be unfamiliar to a patient but is commonly used in radiology. This also applies if the controller operates in a different industry than the third party to whom the data is to be transferred. However, this can pose a practical obstacle to cross-sector transfers.

2. Electronic

43 An electronic format essentially corresponds to machine readability under the DSGVO. There, machine-readability is regarded as a fundamental "form requirement" for the digital society, since only this enables the automated processing of information by computers. Since the right to data portability is aimed at the data economy, the format must ensure that the data can be auto-

matically imported into a computer system in a structured form. The data must therefore be **electronically processable** and capable of being further processed automatically.

In certain cases, however, Swiss regulations may be more restrictive than the machine-readability requirement. While there is sometimes debate under the DSGVO as to whether computer printouts should be considered machine-readable due to the technical possibility of automated text recognition (so-called optical character recognition; OCR), these are clearly not classified as an electronic format under the FADP. 44

3. No Interoperability Requirement

The requirements regarding data format do not imply a requirement for interoperability. Interoperability does not refer to data (formats) anyway, but rather to systems that engage in bidirectional exchange. This would therefore require not only the exchange of data, but also **interaction across different systems**. For example, a social network could allow a user to transfer her photos to another provider. Interoperability between two social networks, by contrast, would only be achieved if, for example, a comment posted under a photo on one social network could be displayed on another social network and interacted with there (such as through a new comment). The different systems must therefore not only be capable of exchanging data but must also agree on the conditions that apply to that data. 45

Art. 21 para. 2 of the GDPR clarifies in this regard that the right to data portability imposes **no obligation** on the controller to adopt or maintain technically compatible data processing systems. Needless to say, this obligation does not apply to third parties either, who are not required to accept the ported data in the first place. Nor do the provisions of the FADP and the DSV impose an obligation to ensure interoperability between systems. 46

In its explanatory notes, the Federal Office of Justice (BJ) further suggests that the transferred information should be precisely described in interoperable formats with appropriate and comprehensible metadata so that it can be meaningfully transferred to a new system. The metadata should be comprehensive enough to enable the use and reuse of the data without disclosing trade secrets. This suggests an obligation to prepare (new) metadata, which should not be followed. Art. 28 of the FADP merely establishes—and particu- 47

larly in light of Art. 21 para. 2 of the FADP—a**right to the data** *"as is"*. This also covers any metadata that, for example, enables the structuring of a larger dataset. However, no obligation to supplement the metadata (including, in some cases, data that the controller may not even need in its system) can be inferred from this. This is particularly true since the Swiss regulation, unlike Article 20 of the DSGVO, does not explicitly require the data to be structured. Furthermore, the specific metadata that can technically be included in a format may vary depending on the (common) format in question. Therefore, only those metadata pertaining to the data subjects that are contained in a commonly used electronic format within the meaning of Art. 28 of the FADP must be disclosed.

V. MODALITIES (PARA. 3 AND DSV)

48 Art. 28 para. 3 of the FADP provides that the controller must, in principle, transfer personal data free of charge. In addition, Art. 22 of the FADP specifies the time limit, jurisdiction, and other modalities. Art. 22 of the FADP, however, limits itself to referring, mutatis mutandis, to the **modalities of the right of access**, without addressing the substance of the right to data portability. In principle, therefore, reference can be made to the comments on the right of access.

A. Form and Time Limit

49 Article 22 in conjunction with Article 16(1) of the DSV requires the data subject to submit a **written request**. In this request, the data subject must identify themselves (Article 22 in conjunction with Article 16(5) of the DSV). This can be done, for example, by enclosing a copy of their identification document with the request. More commonly, however, identification is likely to occur when the data subject submits the request **directly from their (logged-in) account** with the controller. In such cases, however, the controller should take special precautions in light of data security requirements (for example, by implementing mechanisms to detect unusual login attempts from external IP addresses). With the controller's consent, the request may also be made verbally; however, this is likely to occur rarely.

50 The porting must take place **within 30 days of receipt of the request** (Art. 22 in conjunction with Art. 18(1) of the Data Protection Ordinance). If the porting cannot be completed within this period, the data controller must in-

form the data subject of this and specify the timeframe within which the porting can be completed (Art. 22 in conjunction with Art. 18 para. 2 of the Data Protection Act). Any potential restriction must also be communicated within the same timeframe (Art. 22 in conjunction with Art. 18(3) of the Data Protection Act).

A continuous or periodic data flow is not required. Nor is the controller required to grant the data subject or the other controller unrestricted access to the data (for example, through access to an interface). The right to data portability is conceived as a **static transfer mechanism** and thus provides merely a "snapshot." 51

Like the right of access, the right to data portability can therefore, in principle, be granted **in any form**. For example, a USB drive could be sent by mail, or the data could be sent electronically via email. Furthermore, particularly in the case of larger data sets, the controller may offer access via an API or the option to download the data directly from its servers (e.g., from an SFTP server, a secure web interface, or a web portal). 52

B. Jurisdiction

The right to data portability is directed **against the controller**, even if the data is stored by a processor. If there are multiple controllers, the data subject may assert their right against each one individually (Art. 22 in conjunction with para. 1 of the Data Protection Act). In each case, the controllers are obligated to process the request themselves and not merely to forward it. Processors must assist the controller in responding to the request or, on behalf of the controller, respond to it themselves (Art. 22 in conjunction with Art. 17 para. 2 of the GDPR). The processor must therefore provide the controller with data relevant to portability if the controller does not have it at its disposal. 53

C. No Cost

The controller must provide or transfer the data **free of charge** (para. 28(3) FADP). In exceptional cases, a **fee of up to CHF 300 is permissible** if the porting involves a disproportionate effort (Art. 22 in conjunction with Art. 19(1) and (2) of the Data Protection Ordinance). This may be the (rare) case, for example, when a complex process of separating third-party data from that of the data subject is necessary. The controller must inform the data subject of 54

the amount of the fee in advance (Art. 22 in conjunction with Art. 19(3) of the Data Protection Ordinance).

Note:

The structure and content of this commentary are based on the author's dissertation on the right to data portability. The footnotes refer specifically to the dissertation only when they contain more detailed explanations.

BIBLIOGRAPHY

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.

MATERIALS

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).

COMMENTARY ON

Art. 29 FADP

A commentary by Samuel Mätzler

SUGGESTED CITATION

Samuel Mätzler, Commentary to art. 29 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Mätzler, art. 29 FADP N. XXX.

Art. 29 Restrictions on the right to data portability

[1] The controller may refuse, restrict or delay the delivery or transfer of personal data for the reasons set out in Article 26 paragraphs 1 and 2.

[2] The controller must give reasons why it has decided to refuse, restrict or delay the delivery or transfer.

CONTENT

IN A NUTSHELL

Article 29 of the FADP addresses the possible grounds for restricting the right to data disclosure or transfer under Article 28 of the FADP. It refers to the grounds for restricting the right of access. This is intended to prevent the data subject from using the right to data portability to obtain data that is not subject to the right of access. However, the blanket reference to the right of access does not sufficiently take into account the specific nature of the right to data portability, which can lead to inconsistencies in various cases.

I. GENERAL

A. Purpose and Background of the Provision

Article 29 of the FADP specifies the grounds on which a controller may restrict the disclosure or transfer of data pursuant to Article 28 of the FADP (also known as the right to data portability). However, the provision does not list these grounds independently but refers to the **grounds for restricting the right of access** in Art. 26 para. 1 and 2 of the FADP. For this reason, the explanations provided there can largely be applied to the right to data portability. 1

The blanket reference to the grounds for restricting the right of access is not without controversy, as the two data subject rights **pursue different objectives** and the grounds for restriction do not always apply to the **various use cases**. Nevertheless, this reference does prevent the restrictions on the right of access from being circumvented through the right to data portability. 2

Along with the right to data portability, Art. 29 FADP was only inserted during the **parliamentary deliberations** as part of the FADP revision. The provision was not debated separately and was uncontroversial. 3

B. Comparative Law Notes

Art. 29 FADP was adopted **by analogy from the DSGVO**. However, the DSGVO does not contain a separate provision. Rather, the DSGVO restricts the right to data portability in various places. Under Article 12(5)(1) of the DSGVO, the controller may charge a reasonable fee for data portability in the case of 4

manifestly unfounded or excessive requests (lit. a) or refuse the request entirely (lit. b). In doing so, the controller must provide evidence that the request is abusive (Art. 12(5), para. 2, DSGVO).

5 According to Art. 20(4) DSGVO, the right to data portability must not **infringe upon the rights and freedoms of others**. According to the prevailing view, this also applies to the controller. Consequently, the right to data portability under the DSGVO may be restricted by trade and business secrets or intellectual property rights, such as copyrights.

6 Furthermore, the DSGVO contains in para. 20, second sentence, an **explicit exclusion** for processing carried out in the public interest or in the exercise of official authority. Furthermore, under the conditions set forth in Article 23 of the DSGVO, additional restrictions may be provided for in Union law or in the law of a Member State. In accordance with Article 85(2) and Article 89(3) of the DSGVO, further derogations are also possible, which may limit the right to data portability in certain circumstances.

II. GROUNDS FOR RESTRICTIONS (PARA. 1 IN CONJUNCTION WITH ARTICLE 26)

A. Legal Basis, Specifically Professional Secrets (Article 26(1)(a))

7 A restriction on the right to data portability is permissible if provided for by a law in the formal sense (Art. 29(1) in conjunction with Art. 26(1)(a) of the FADP). Such a legal basis must relate to the right to data portability and would have to be **assessed on a case-by-case basis**. To date, however, no such legal bases exist.

8 The provision relating to the right of access cites the protection of professional secrecy as an example. This makes it clear that the reference to the right of access**is not very convincing**, since the right to data portability covers only data that relates to the data subject and has also been disclosed by the data subject to the controller. Professional secrecy, on the other hand, is primarily intended to protect the data subject. Since the data subject always exercises their right to data portability on their own initiative—and thus consent has been given—professional secrecy is not violated (see Art. 321 no. 2 of the SCC).

B. Overriding Interests of Third Parties (Art. 26 para. 1(b))

The data controller may restrict the right to data portability if this is necessary due to overriding interests of third parties (Art. 29(1) in conjunction with para. 26(1)(b) of the FADP). In this context, the **dual or third-party use** of data is the primary concern, but trade secrets or intellectual property rights of third parties are also conceivable. Restrictions based on the controller's interests, by contrast, must be considered under para. 2 of Art. 26 of the FADP. 9

With regard to the interests of third parties, a **balancing of interests** must take place. It should not be readily assumed that the interests of third parties prevail: The data in question always relates (at least in part) to the data subject and consists of information that the data subject has already disclosed to the controller. In light of the legislature's decision to grant the data subject the right to data portability so that they may dispose of "their" data, the grounds for restriction must therefore **not be interpreted too broadly**. However, it is also true that, in cases of doubt, the controller is more likely to accept a potential violation of the right to data portability—which is not subject to sanctions under the FADP—than a violation of third-party rights. 10

C. Manifestly Unfounded (Art. 26(1)(c))

If a request is manifestly unfounded, the controller may also restrict the right to data portability (Art. 29(1) in conjunction with Art. 26(1)(c) of the FADP). By way of example, Art. 26 of the FADP—which is tailored to the right of access—lists cases in which a request pursues a **purpose contrary to data protection** or is **manifestly vexatious**. However, the possibility of restricting portability in the event of a purpose contrary to data protection is difficult to reconcile with the right to portability in light of the objectives of data protection and competition law. The right to data portability aims, among other things, to ensure the free flow of data; therefore, a request should **not be readily deemed manifestly unfounded**. This reference to the right of access is thus also unsatisfactory. The right to data portability is intended to enable the transfer of data between different parties in as standardized a manner as possible, free from case-by-case considerations. Accordingly, it is unclear in which cases the controller may refuse a request under this provision. 11

However, a request may be presumed to be unfounded, for example, if the right to data portability is exercised **in abuse of the law**. The text also men- 12

tions the case of **evidence gathering** against the data controller in civil proceedings.

D. Further Grounds for Restriction (Art. 26 para. 2)

13 Art. 29(1) FADP also refers to Art. 26(2) FADP. That provision sets forth additional grounds for restriction for private individuals (lit. a) and for federal bodies (lit. b). Since the latter are rarely parties to proceedings regarding the right to data portability, the grounds for restriction **for federal bodies** can hardly be considered relevant from the outset.

14 It is conceivable, however, that a **private data controller** might wish to restrict data portability because its overriding interests so require (lit. a, no. 1). A data controller may thus invoke its **own trade secrets and intellectual property rights** as grounds for restriction under Art. 29(1) in conjunction with para. 2(a) of the FADP. Overall, however, this is likely to be rare, since only data disclosed by the data subject is covered by the right to data portability, while derived data—i.e., data based on a service provided by the controller—is excluded from the scope of application. In principle, the legislature has already subordinated the controller's interests to those of the data subject and competition by introducing the right to data portability; therefore, the controller is unlikely to be able to invoke trade secrets very often.

15 If the controller wishes to restrict portability on the basis of its overriding interests, para. 2 of Art. 26 of the FADP lists an additional requirement that must be met. The controller must not be permitted to **disclose personal data to third parties** (no. 2). However, this condition is incompatible with the right to data portability under Art. 28(2) of the FADP and is therefore, in our view, **irrelevant** as a condition for restriction. It is also possible to conclude that the controller cannot rely on Art. 26(2)(a) of the FADP at all if the data subject requests data portability.

III. LEGAL CONSEQUENCES

16 If there is a valid ground for restriction, the controller may **refuse, restrict, or postpone** the porting. In doing so, the controller must ensure proportionality and **enable the right to data portability as fully as possible**. Thus, before refusing a request, the controller must always first consider whether to postpone or restrict it.

IV. DUTY TO PROVIDE REASONS (PARA. 2)

Pursuant to Art. 29(2) of the FADP, the controller must state why it is refusing, restricting, or postponing the porting. This corresponds to the obligation that a controller must also fulfill under the right of access (see Art. 26(4) of the FADP). The controller must **inform the data subject** *that* the porting is being refused, restricted, or deferred and **provide reasons** for this. A **30-day deadline** from receipt of the request also applies here (Art. 22 in conjunction with Art. 18 para. 3 of the Data Protection Ordinance). For further details, please refer to the commentary on Art. 25 of the FADP. 17

Note:

The structure and content of this commentary are based on the author's dissertation on the right to data portability. The footnotes refer specifically to the dissertation only when they contain more detailed explanations.

BIBLIOGRAPHY

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. ...).

MATERIALS

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).

COMMENTARY ON

Art. 31 para. 2 lit. e FADP

A commentary by Philipp do Canto

SUGGESTED CITATION

Philipp do Canto, Commentary art. 31 para. 2 lit. e FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-do Canto, art. 31 para. 2 lit. e FADP N. XXX.

Art. 31 Grounds for justification

[1] [...]

[2] The controller may have an overriding interest in the following cases in particular:

a. [...]

b. [...]

c. [...]

d. [...]

e. The controller processes the personal data for purposes not related to specific persons, in particular for research, planning or statistics, provided the following requirements are satisfied:

The controller anonymises the data as soon as the purpose of processing permits; if anonymity is impossible or if it requires disproportionate effort, the controller shall take appropriate measures to prevent the identification of the data subject.
If the matter involves sensitive personal data, the controller shall disclose such data to third parties in such a manner that the data subject is not identifiable; if this is not possible, it must be guaranteed that the third parties only process the data for purposes unrelated to the data subject's person.
The results are published in such a manner that data subjects are not identifiable.

f. [...]

CONTENT

IN A NUTSHELL

[In the introduction to Article 31, by other author(s)]

I. GENERAL

[General on Art. 31; Preamble and background, by other author(s)]

II. PARA. 1, CONSENT, OVERRIDING INTEREST, LEGAL GROUNDS FOR JUSTIFICATION

[on Art. 31 para. 1; by other author(s)]

III. PARA. 2

A. General information / test steps

[General to para. 2; by other author(s)]

B. List of legal cases

1. Lit. a - d

[By other authors(s)]

2. Lit. e, Processing for non-personal purposes

1 Processing for non-personal purposes is the provision on overriding interests that has been expanded the most compared to its predecessor provision in Art. 13 para. 2 lit. e aDSG. In addition to the previous regulation on the publication of results (new in no. 3 of the provision, below n. 15), there is an obligation to anonymize or pseudonymize at the earliest possible time (no. 1) and, as a qualified offence, a requirement for the disclosure of particularly sensitive personal data to third parties (no. 2). The regulator thus no longer starts with the publication of the results, but intervenes directly in internal process management during processing. On the one hand, the higher density of regulation is the result of a legal concretization of existing principles; on the other hand,

it means a tightening of the requirements for controllers when processing for non-personal purposes.

a) Non-personal purpose as a basic offense

The central element of the provision is processing for non-personal purposes. 2
Non-personal purposes are defined as purposes for which the identity of the data subject is irrelevant. In other words, the purpose of the activity is also fulfilled if anonymized or encrypted data is processed. There is a wide range of possible processing purposes that can fall under this justification. Not only large numbers of people are covered, but the processing of the data of an individual person or a group can also serve non-personal purposes, as long as it is only about the characteristics and not the identity. The identity of the data subject may, however, be of practical importance to the data controllers themselves, for example in the area of longitudinal studies in which information is collected from data subjects at regular intervals.

The law itself does not define the term "non-personal purpose", but mentions 3
private research, statistics and planning as examples. The regulation is therefore also referred to as a "research privilege" under data law. Population, spatial and transport planning are mentioned in the doctrine as examples of planning. The privileged status of these areas is justified by the fact that they not only provide an important basis for economic decision-making, but also meet a variety of social and public needs. The list of areas is not exhaustive. In particular, the evaluation of internet and app usage data or the use of AI models in the context of big data analysis, where any interest in the individual is eliminated in advance, should be considered. On the other hand, the explicit mention in the law does not mean that data processing in the areas of research, statistics and planning always serves non-personal purposes. An example of personal purposes is precision medicine, where positive study results should also benefit the persons concerned. Other activities for other purposes include historical and genealogical research, which are not covered by the privilege if they relate to specific persons or groups.

The provision regulates data processing by private individuals. This includes, 4
for example, private pharmaceutical research, private clinical studies or studies carried out by private organizations, market research and planning in companies. As a result of Art. 40 FADP, the provision also covers activities of federal bodies under private law. For government activities, Art. 39 FADP applies,

which contains an analogous provision on data processing for non-personal purposes by federal bodies.

5 There will also be processing purposes that have both personal and non-personal components, namely in research. For such activities, the question arises to what extent the justification ground can be invoked. For federal bodies, Art. 35 DPO states that the exceptions under Art. 39 para. 2 FADP only apply to processing for non-personal purposes. An analogous regulation for private controllers is therefore understandable; it leads to a separate data law consideration for different aspects of a specific activity.

6 With regard to the three areas mentioned in the Act and other areas, special legislation must then be taken into account, which, depending on the enactment, ranges from a general reference standard to detailed regulations. Of particular importance is human research law (currently under revision) with the HRA and related enactments such as the Cancer Registration Act, which contain their own provisions on pseudonymization and triage provisions regarding the application of the HRA and FADP (e.g. Art. 28 KRG). In the electricity supply sector, Art. 17c para. 1 StromVG refers to the FADP with regard to smart metering. In statistics, the special legislation under the Federal Statistics Act (BStatG) applies insofar as it covers private institutions (Art. 2 para. 3 BStatG, cf. also principles pursuant to Art. 4 BStatG).

7 If processing is carried out for non-personal purposes, the various provisions of no. 1 to 3 apply. The provisions in detail:

b) No. 1, anonymization or pseudonymization (encryption)

8 Data controllers must anonymize the data as soon as the purpose of the processing permits. The provision thus takes up the principle of Art. 6 para. 4 FADP and at the same time qualifies it with an exception. According to this provision, data controllers can take other appropriate measures to prevent the person from being identifiable if anonymization is technically impossible or involves disproportionate effort. Due to the development of biometric recognition software, the anonymization of personal portraits, for example, is de facto impossible today, whereas a black bar across the eye area used to be sufficient. In view of the purpose of the standard, the exception must be applied with a sense of proportion despite the technical and financial consequences and requires a balancing of interests in individual cases, which balances the

interests of those affected against the intended privileging of the activities in question.

Appropriate measures include, in particular, pseudonymization, encryption or coding. Pseudonymization plays an important role in practice and at the same time represents a technical challenge. Especially with regard to data obtained from biological material (biosamples), i.e. from parts of the human body such as tissue or blood samples, the technical requirements for pseudonymization have increased. Laboratory technology, above all DNA analysis, facilitates identification, possibly in combination with characteristics of other samples. Human research law makes corresponding provisions for the handling of biological material and genetic data (Art. 32 ff. HRA). 9

In connection with measures to prevent identifiability, reference should be made to the extensive catalog of technical and organizational measures in Art. 3 DPA, in particular the rules on confidentiality and integrity. There are also various guidelines on encryption, such as the binding scientific linking guidelines of the Federal Statistical Office or the cross-industry guidelines of the European Cybersecurity Agency (Enisa). The guidelines contain, among other things, requirements for handling the codes and for de-pseudonymization. 10

c) No. 2, Disclosure to third parties

The second requirement concerns the processing of particularly sensitive data (for the term, see commentary on Art. 5 lit. c FADP). The provision refers to Art. 30 para. 2 lit. c FADP, according to which the disclosure of such data to third parties constitutes a violation of personality rights. As in no. 1, a principle is established and this is mitigated with an exception. The exception was not yet included in the draft bill and was introduced in the National Council. 11

If the additional criterion of particularly sensitive data is fulfilled, the principle applies that this data may only be passed on to third parties in such a way that the data subject cannot be identified. Data may therefore also only be transferred in anonymized or encrypted form. The transfer of data to third parties is thus initially treated no differently to publication (no. 3). No. 2 aims to prevent the disclosure of non-anonymized, particularly sensitive personal data from being justified on the grounds that it is being processed for research, planning or statistical purposes. 12

13 The exception applies if measures to prevent identifiability are not possible, which may be the case with a person's extensive genetic data, for example. According to the wording, disproportionality of the measure is not a justification (see no. 1). In the event of impossibility, it must be ensured that third parties only process the data for non-personal purposes. The provision does not require that the processing purpose of the third party must be the same as that of the controller, which is understandable in view of the different areas of responsibility in research, statistics and planning. The duty of guarantee primarily applies to the controller, whereby no. 2 does not contain any methodological requirements for (contractually) ensuring the non-personal purpose limitation vis-à-vis third parties.

14 The dispatch on the aDSG then refers to statutory confidentiality provisions. Where these prohibit the disclosure of data to third parties, they take precedence as special regulations, such as professional secrecy protected under criminal law (e.g. medical confidentiality). Statistics departments or researchers can therefore not justify the disclosure of secret data on the basis of no. 2. The same applies to contractual or otherwise stipulated confidentiality obligations.

d) No. 3, Publication of results

15 no. 3 incorporates the previous provision according to which data subjects must not be identifiable when the results are published (Art. 13 para. 2 lit. e aDSG). In other words, there is still no requirement for anonymization in the publication. In the doctrine, it is noted that the publication of studies with a small number of affected persons may give rise to a risk of conclusions being drawn about the individual, for example in the case of studies on rare diseases or planning for small geographical areas. However, when publishing results based on data from a large number of affected persons, this appears to be less of a problem insofar as the identification of the person by a human being is more difficult. The machine recognition systems mentioned above, on the other hand, function independently of geographical or numerical restrictions, meaning that it is ultimately technical progress that is constantly increasing the requirements for the publication of results.

BIBLIOGRAPHY

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).

MATERIALS

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).

COMMENTARY ON

Art. 33 FADP

A commentary by Sandra Husi-Stämpfli

SUGGESTED CITATION

Sandra Husi-Stämpfli, Kommentierung zu Art. 33 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Husi-Stämpfli, N. XXX zu Art. 2 DSG.

Chapter 6 Special Provisions on Data Processing by Federal Bodies

Art. 33 Control and responsibility in the case of the joint processing of personal data

The Federal Council shall regulate the control procedures and responsibility for data protection in cases in which a federal body processes personal data jointly with other federal bodies, with cantonal bodies or with private persons.

CONTENT

IN A NUTSHELL

Since the processing of personal data is increasingly not only carried out jointly by several federal agencies, but also jointly with cantonal or municipal agencies or even private individuals, there is a need for clear regulations on responsibilities. Art. 33 FADP empowers the Federal Council to define responsibilities in these constellations.

I. GENERAL

A. History

The predecessor provision in Art. 16 aDSG was split up with the data protection revision. Art. 16 para. 1 aDSG, which governed general responsibility, was transferred to Art. 5 lit. j. Art. 16 para. 2 aDSG, which regulated the responsibility in the case of several data processors involved, was transferred to Art. 33 FADP. 1

B. Purpose of the Norm

Art. 5 lit. j FADP defines who is to be subsumed under the term "data controller" (see OK-Hofmann on Art. 5 lit. j FADP): the connecting factor is the decision-making authority over the purpose and means of the data processing operations. Which federal body has this decision-making authority is determined by the respective special laws that serve as the legal basis for the data processing. 2

Since the processing of personal data is increasingly not only carried out jointly by several federal agencies, but data processing operations that cross the federal levels are also part of everyday life and even private persons can access common information stocks, there is a need for clear regulation of responsibilities. Otherwise, there is a risk that many agencies will process the personal data in question, but no one will feel responsible. 3

II. NO VACUUM OF RESPONSIBILITY

Art. 33 FADP empowers the Federal Council to regulate the responsibilities for compliance with data protection law as well as the associated controls if 4

several federal bodies, or federal bodies and cantonal or private third parties are jointly involved in data processing operations. This regulation does not take place in the DPA, but in the respective special legislation or in the associated implementing ordinances. Thus, Art. 33 FADP explicitly states that the Federal Council shall regulate the control procedures and responsibility in the case of joint processing of personal data.

III. SHARED RESPONSIBILITY

5 Three constellations are conceivable for the joint processing of personal data:

- A special law or the Federal Council may, in an ordinance, assign sole responsibility for joint data processing to a federal body (Art. 5 lit. j FADP).
- From a special law or an ordinance, a relationship of superiority or subordination can be identified for joint data processing, which is reflected in a primary and a secondary responsibility. An example of this is commissioned data processing (Art. 5 lit. k FADP).
- A parallel responsibility for joint data processing may arise from a special law or an ordinance (Art. 33 FADP), which must be differentiated by a clear division of labor in the special law or ordinance.

IV. CONTROL PROCEDURE

6 The concept of the control procedure is to be understood as supervision of the data processing operations. In the first constellation of sole responsibility, as well as in the case of clear primary and secondary responsibility, there is unilateral supervision of the sole responsible party or the primary responsible party vis-à-vis those involved in joint data processing. In the second constellation of parallel responsibility for joint data processing, reciprocal control procedures must naturally be established. The details regarding the scope, the manner as well as the regularity of the control procedures shall be regulated in the special law or ordinance.

V. REGULATORY REGIME

7 In the case of joint data processing by federal bodies with cantonal bodies and private persons, different regulatory regimes shall apply. For federal bodies,

the special provisions on data processing pursuant to Art. 33 ff. FADP, for private persons the special provisions in Art. 30 ff. FADP apply, and cantonal law applies to cantonal bodies. Even if joint data processing is involved, a clear distinction must always be made as to which actor is bound by which obligations.

VI. LIABILITY ISSUES

The liability of federal bodies, cantonal bodies and private persons is governed by different standards: For federal bodies according to the Liability Act (VGG), for cantonal bodies according to the cantonal liability laws and for private persons according to civil law. The extent to which a responsible party can be liable externally for the entire damage caused by the joint data processing (cf. joint and several liability) is unclear. It is also unclear to what extent breaches of duty by third parties can be imputed to a data controller on the basis of the obligation to control. 8

The author provides her personal assessment in this commentary.

BIBLIOGRAPHY

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

COMMENTARY ON

Art. 34 FADP

A commentary by Esther Zysset

SUGGESTED CITATION

Esther Zysset, Kommentierung zu Art. 34 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Zysset, N. XXX zu Art. 34 DSG.

Art. 34 Legal basis

[1] Federal bodies may only process personal data if there is a statutory basis for doing so.

[2] A statutory basis in a formal law is required in the following cases:

a. The matter involves the processing of sensitive personal data.

b. The matter involves profiling.

c. The purpose or manner of the data processing may lead to a serious violation of the data subject`s fundamental rights.

[3] A statutory basis in a substantive law is sufficient as the basis for processing personal data under paragraph 2 letters a and b provided the following requirements are satisfied:

a. Processing is essential for a task required by a formal law.

b. The purpose of processing poses no particular risks to the data subject's fundamental rights.

[4] In derogation from the paragraphs 1–3, federal bodies may process personal data if any one one of the following requirements is satisfied:

a. The Federal Council has authorised the processing because it considers that the data subject's rights are not at risk.

b. The data subject has consented to the processing in the specific case or has made their personal data generally accessible and has not explicitly prohibited any processing.

c. The processing is necessary in order to protect the life or physical integrity of the data subject or of a third party, and it is not possible to obtain the consent of the data subject within a reasonable time.

CONTENT

IN A NUTSHELL

As the cornerstone of data processing by state bodies, the requirement of a legal principle is of primary importance.

For data processing by federal bodies, Art. 34 FADP illustrates both Art. 5 FC, according to which all state action requires a basis in law, and Art. 36 FC, which sets out the requirements for fundamental rights interventions in general; the provision thus constitutes concretized constitutional law. The processing of personal data by public bodies constitutes an interference with the fundamental right to protection of informational self-determination under Article 13 para. 2 FC; depending on the context, a wide variety of other fundamental rights may also be affected. Art. 34 FADP schematically expresses the required norm level.

The new provision on the legal basis, which is unbundled compared to the previous version of the same norm, reflects the increased importance of the correct legal support of data processing by state bodies in the age of digital processing of large amounts of data.

I. GENERAL

A. preliminary remarks

1 A legal basis is a generally abstract norm issued by a competent state body. In detail, the applicable law determines which requirements a legal basis must meet. At the federal level, specifications in this regard can be found, for example, in the Federal Constitution (Art. 164 FC) or in parliamentary law (e.g. Art. 22 ParlG). The norm that serves as the legal basis in the individual case may originate from national or international law.

2 The terminology used in connection with the principle of legality shows a certain heterogeneity. In the following, for the requirement of a general-abstract regulation, referred to in Art. 34 FADP as "legal basis", the general term of the legal principle is also used. Furthermore, the law enacted by the legislature is described by the term "legal form" or "law in the formal sense". Lower-level enactments are considered "laws in the substantive sense" , as also expressed in Art. 34 para. 3 FADP.

B. purpose and background

Article 34 FADP specifies for data protection law what already applies to state action: in addition to the general principle of legality of Article 5 para. 1 FC, according to which the law forms the basis and barrier of state action, Article 36 para. 1 FC requires a legal basis for encroachments on fundamental rights. Art. 34 FADP provides schematic guidelines on the normative level for various types of data processing - and thus for various encroachments on fundamental rights, first and foremost encroachments on the fundamental right to informational self-determination (Art. 13 para. 2 FC). 3

C. history of origins

The Federal Council's draft of the first federal data protection law from 1988 already contained a provision that was similar to the one commented on here; in particular, a distinction was already made between the processing of ordinary personal data and data requiring a higher level of protection in the form of personal data requiring special protection and personality profiles. The predecessor provision Art. 17 aDSG, which has been modified in the meantime, provided for the basic principle of the legal basis and also stipulated exceptions, the scope of which was not very clear and accordingly gave rise to criticism. 4

The new provision makes a structural unbundling; in addition to the unchanged basic principle (para. 1), it clearly distinguishes between the requirement of legal form (para. 2), situations with a lowered normative level (para. 3) and situations in which the requirement of a legal principle can be completely deviated from (para. 4). 5

II. THE PRINCIPLE OF LEGALITY IN DATA PROTECTION

A. role and functions of the principle of legality in general

1. legal basis as a prerequisite for interference with fundamental rights and as a principle of state action

In the processing of personal data by state authorities, encroachments on positions protected by fundamental rights take place: First and foremost, this concerns Art. 13 FC and specifically its para. 2 (fundamental right to "informa- 6

tional self-determination") as well as Art. 8 ECHR and Art. 17 UN Covenant II. What is protected is not only, contrary to the wording of Art. 13 para. 2 FC, the protection against misuse of personal data, but the private sphere, insofar as it also includes data about the respective person. In addition, a wide variety of other fundamental rights may be affected, including the right to personal freedom (Art. 10 para. 2 FC) and freedom of expression (Art. 16 FC), especially with increasing digitization, in which every state activity is accompanied by data processing.

7 In Art. 36 para. 1, the Federal Constitution provides that restrictions of fundamental rights require a legal basis; serious restrictions must be provided for in law, unless there is a case of "serious, imminent danger that cannot be averted in any other way". Furthermore, restrictions on fundamental rights must serve the implementation of a public interest and be proportionate; the core content of the fundamental right must be preserved (cf. criteria of Art. 36 FC).

8 In its role as a principle of state action, Art. 5 para. 1 FC provides that state action requires a basis in law and, at the same time, it is law that sets limits to any state action ("barriers", in the words of the constitutional legislator). The administration - in the terminology of the FADP, the "federal body" - may therefore only act if there is a legal basis for it, and may only go as far as the action is covered by the relevant basis. This applies regardless of the legal nature of the state action, even if the requirements of the principle of legality take on different forms depending on the situation and the risk involved.

2. level and density of norms

9 Article 36 para. 1 FC already indicates that the required legal sentence must meet heightened requirements in the case of serious restrictions of fundamental rights. The more serious the encroachment on fundamental rights, the higher the requirements for the level and density of the norm. Serious restrictions must be provided for in the law itself, i.e. in a law in the formal sense (norm level) and must take sufficient account of the requirement of certainty (norm density). At a minimum, legal norms must be formulated in each case "so precisely that those subject to the law can direct their conduct accordingly and recognize the consequences of certain conduct with a degree of certainty appropriate to the circumstances". In which case which condition of the legal norm is sufficient is often not easy to answer and depends strongly on the individual case. In the words of Tschannen/Müller/Kern: the principle of legality

is "of unpleasant shorelessness". For federal law, Art. 164 FC at least provides an exemplary list of topics for which the basic provisions are considered important law-making provisions and must therefore be regulated in a law in the formal sense; these are:

- Exercise of political rights;
- Limitations of constitutional rights;
- Rights and obligations of persons;
- The group of persons liable to levies and the object and assessment of levies;
- Duties and services of the Confederation;
- Obligations of the Cantons in the implementation and enforcement of federal law;
- Organization and procedures of the federal authorities.

For its part, doctrine proposes the following criteria for circumscribing the importance of a regulatory object: 10

- Intensity of the interference;
- Number of persons affected by a regulation or the life circumstances regulated;
- financial importance;
- Significance for political decision-making, the organization of state institutions or the procedure and
- Explosiveness or acceptability of the issue.

The need for flexibility and rapid adaptation or special expertise, on the other hand, tend to speak in favor of regulations at a lower normative level. 11

These general requirements of the Federal Constitution must be taken into account when designing legal foundations in accordance with Art. 34 FADP. Art. 34 FADP specifies the required norm level for certain typified data protection situations, but not the norm density (see on norm density infra nos. 18-19). For the context of data protection that is of interest here, the focus from the catalogs cited above is on, among other things, the restriction of 12

constitutional rights or the intensity of encroachments on fundamental rights, as well as provisions on the "rights and obligations of persons". With increasing digitization, however, the explosive nature of the issues is also increasingly playing a role as a criterion for the form of legislation, which is currently evident, for example, in the use of artificial intelligence or, more specifically, facial recognition in public spaces.

13 If legislative powers are to be delegated from the legislative to the executive, the general requirements of legislative delegation developed by case law and doctrine also come into play in data protection. Thus, the delegation of legislative powers may not be excluded by the relevant law (cf. Art. 164 para. 1 FC); the delegation norm must be contained in an enactment at the legislative level; the delegation must be limited to a specific subject matter and the main features of this subject matter must already be listed in the law.

B. requirement of the legal principle pursuant to Art. 34 FADP

1. basic principle para. 1

14 With the fundamental requirement of a legal principle, data processing by federal bodies is subject to a prohibition with reservation of permission; this is in contrast to data processing by private persons. The requirement applies regardless of the type of data processing (see the legal definition of processing in Art. 5 lit. d FADP; for the special case of disclosure, see Art. 36 FADP). Art. 34 FADP merely provides the basic principle; it cannot itself be used as a direct legal basis. Furthermore, para. 1 makes no statement as to the normative level at which the legal sentence is to be located or what normative density it must have.

15 Moreover, it follows from the systematics of the FADP that the remaining general provisions of the law, in particular the data processing principles of Art. 6 FADP and the provisions on security pursuant to Art. 8 FADP, apply cumulatively. Thus, for example, the existence of a legal basis does not exempt from the obligation to observe the principle of proportionality and to process only the data effectively required for the performance of the public task.

16 The legal text of Art. 34 FADP refers to the processing of personal data by federal bodies. With regard to the definition of federal body, Art. 5 lit. i FADP expresses that this covers not only the organizationally assigned units of the

administration and public institutions of the Confederation, but also private individuals, provided they are entrusted with the performance of public tasks of the Confederation (see there).

Notwithstanding the indications on the normative level in para. 2-4, it is often not entirely clear in legislative practice what the normative density of the legal basis should be. This problem manifests itself, for example, in the question of whether a general ("indirect") legal basis is sufficient ("Office X fulfills the legal task Y") or whether a specific legal basis tailored to a certain data processing is required ("In order to process applications for subsidies, Office X processes the following personal data: ...", etc.). 17

On the question of the nature of the legal basis, the Federal Office of Justice has written a legislative guide that provides specific guidelines for legal bases in the area of data protection. Against the background of the functions of the principle of legality (see infra n. 43 ff.) and the postulate that the citizen should be able to direct her conduct in accordance with the relevant norm, the following elements must be regulated: 18

- Which authority (who)
- processes which categories of personal data (what),
- for what purpose (why) and
- in what way (how)?
- To whom, if anyone, is personal data disclosed (to whom) and
- in what way (how)?

In particular, it must be stated under what whether personal data requiring special protection are also processed and, if so, which categories (cf. Art. 5 lit. c FADP), whereas the precise attributes can be specified in an ordinance if the law is sufficiently dense. The more serious the encroachment on fundamental rights, the more detailed and precise the legal basis must be formulated, although in view of the rapid development of information and communication technologies, a certain flexibility in the formulation and an accompanying vagueness will sometimes have to be accepted. The processing also includes information on the retention period and deletion of the personal data. 19

20 To the extent that this provides the legal sentence with the transparency required by law vis-à-vis the data subjects, the obligation to provide information under Art. 19 FADP does not apply (cf. Art. 20 para. 1 lit. b FADP).

21 Special rules can be provided for in the respective substantive laws, which take precedence over the requirements of the FADP as lex specialis and, at least theoretically, can also deviate from them downwards. The Federal Supreme Court and doctrine assume, however, that the general principles of data protection law must still be observed in such cases.

2. legal form for cases under para. 2

22 The second paragraph requires the form of law (law in the formal sense) for cases in which the data processing may lead to a weighty encroachment on the fundamental rights of the persons concerned. Where the processing of personal data requiring special protection (lit. a) and profiling (lit. b) are concepts and terms defined in the FADP, para. 2 also provides a general clause that applies when either the purpose of the processing or the manner in which the data is processed may lead to a serious interference with the fundamental rights of the data subjects (lit. c). However, the requirement of the legal form for data processing with great relevance to fundamental rights already results from Art. 36 para. 1 FC, irrespective of which letter of para. 2 a matter is assigned to.

23 The two parameters of the objective and the manner of processing mentioned in lit. c are the main elements used to evaluate the encroachment on the corresponding fundamental right. In view of the fundamental rights context, they are not exhaustive.

24 If it is not possible to base data processing on a sufficiently precise, detailed legal basis, case law confirms that a particularly strict handling of the proportionality test, for example, can have a certain compensatory effect.

3. substantive legal basis for cases under para. 3

25 Para. 3 provides for the possibility of a reduced standard level for the processing of personal data requiring special protection and profiling, provided that two conditions are met cumulatively: The processing is indispensable for a task formally defined by law; and the purpose of the processing does not pose any particular risks to the fundamental rights of the data subject.

Due to the constitutional framework, it is again conceivable - even if the examples are likely to be rare - that deviations may arise that are not specifically enumerated by para. 3: For example, the social explosiveness of a topic could lead to the fact that the legal form must nevertheless be required for corresponding data processing; it is therefore the manner of data processing, instead of the purpose mentioned by para. 3, that gives rise to an increase in the norm level. 26

a. indispensability for a task described in the law (lit. a)

With regard to the wording of para. 3 lit. a, it is noticeable compared to the previous version (Art. 17 para. 2 lit. aDSG) that it should no longer be possible to refer to the reduced standard level merely "by way of exception". In the previous version, the position could be taken that it was only a matter of selective exceptional processing of data in situations in which no such processing would normally be necessary to fulfill the corresponding legal task. The current wording clearly deviates from this by dispensing with the requirement that an exceptional situation must exist. Accordingly, it must be assumed that the processing of particularly sensitive personal data and personality profiles on a permanent basis is also possible on an ordinance basis if the two requirements of para. 3 are met. 27

b. The purpose of the processing does not pose any particular risks to the fundamental rights of the data subject (lit. b).

para. 3 lit. b applies to those processing operations that fall into an intermediate category: Although these are types of processing that would typically lead to a serious encroachment on fundamental rights (which is why para. 2 normally requires a formal legal basis for them), in the specific case the purpose of the processing does not pose any particular risks to the fundamental rights of the data subjects. According to the Federal Council's dispatch, this refers in particular to data requiring special protection that is processed in the context of Federal Council, departmental and official business; mentioned are appeal decisions, state liability cases or federal personnel business. In addition, the formal legal basis must sufficiently specify the nature of the tasks for which the processing of personal data is necessary. 28

The wording in para. 3 lit b may be surprising, since it refers only to the "purpose of processing" without including the "manner of data processing" men- 29

tioned so far in para. 2 lit c. The wording in para. 3 lit b is not clear. It can be assumed that the legislator primarily wanted to remind people that data processing, which already appears to be sensitive from a fundamental rights point of view due to its purpose, requires a basis in the form of a law in any case, even if the type and manner of processing in the individual case entails few risks of its own.

4. Para. 4: Collection of Exceptions to the Requirements of Paras. 1-3

30 para. 4 exempts three ideal-typical situations (written as alternatives) from the requirement of a legal sentence:

- Authorization of processing by the executive branch (in this case, the Federal Council), where authorization must also be based on the requirement that the rights of the data subjects are not likely to be jeopardized (lit. a);
- Consent by the data subject in the individual case or the unconditional release of personal data by the same (lit. b) or
- The urgent, overriding interest in the form of the protection of the life or physical integrity of the data subject or a third party in a situation that makes it impossible to obtain consent (lit. c).

31 Where para. 3 merely reduces the requirements for the legal basis, para. 4 provides, according to the wording, that no legal principle, neither a law nor a legal principle of a substantive nature, is required for certain cases. Insofar as the requirement of a legal principle is now explicitly waived, this provision is formally the biggest innovation compared to previous versions of the same provision in the FADP. For the circumstances according to lit. a and b, both of which could already be found in the previous version, a welcome clarification is provided; it could not be read with certainty from the wording of the previous standard whether a complete waiver of a legal basis was intended or not.

a. federal council authorization (lit. a)

32 According to lit. a, the Federal Council authorizes processing because it "does not consider the rights of the data subject to be at risk". Whereas the previous version explicitly stated that this authorization was limited to the individual case, this addition is missing in the current wording. According to the dispatch, however, nothing is to change in the norm despite the difference in wording; this is also clear from the context on closer examination. In this con-

text, the authorization is to be seen as a form of decision in contrast to the general-abstract regulation. The latter takes the form of a Federal Council ordinance (Art. 182 para. 1 FC), i.e. a substantive legal basis that is either law-enforcing or law-representing (and in the second case requires authorization by a law). The case of action without a legal statute envisaged by para. 4 lit. a is therefore necessarily conceived for the individual case.

To the same extent as in the previous version, the wording according to which the "rights of the person concerned shall not be endangered" appears obscure. This formulation deviates from the wording in para. 3 lit. b, which states that the purpose of the processing "does not pose any particular risks to the fundamental rights of the data subject". Nevertheless, in view of the fact that any data processing by public bodies represents an encroachment on fundamental rights, it must be assumed that the formula used in para. 4 also means the same as in para. 3 lit. b, namely that a minor encroachment on fundamental rights must be assumed. 33

b. consent (lit. b)

In lit. b, consent substitutes the legal basis. In the case of unconditional release of data, consent is presumed; in this case, knowing and willing disclosure by the data subject is required. See on consent in general Art. 6 para. 6 and 7 FADP and on the question of consent as a valid substitute for a legal basis below infra n. 42 ff. 34

c. police clause under data protection law (lit. c)

Lit. c takes aim at the protection of urgent, overriding interests, concretized in the form of the protection of the life or physical integrity of the data subject or a third party. The prerequisite is that it is not possible to obtain the consent of the person concerned within a reasonable period of time, which is the case, for example, if the person is not in a responsive state (coma or similar) or cannot be found. This standard is a case of "police interests" specified under data protection law. In this respect, it fits easily into the scheme of Article 36 para. 1 FC, which exempts "cases of serious, imminent danger that cannot be averted in any other way" from the requirement of a legal basis. Not explicitly written down, but inherent in the nature of the police clause, is the requirement that it must be an individual case, which means, for example, that police 35

or intelligence service data processing in the context of recurring danger situations may not be carried out solely on the basis of para. 4 lit. c.

5. casuistry on the intensity of intervention and on the requirements of the norm

36 According to Art. 17 para. 2 aDSG, the processing of administrative assistance data relating to business relationships or bank details does not require a basis in law. The encroachment on constitutional rights in connection with the data to be collected in the case of administrative assistance does not, as a rule, weigh particularly heavily here, so that the requirements for the definiteness of the norm are also "not excessively high" (BGE 148 II 349 E. 5.3.3-5.3.4).

37 The legal basis that provides for the use of radio water meters by the municipal water supply must explicitly provide that the recorded hourly values are stored on the water meter for X days and sent out by radio at regular intervals (BGE 147 I 346 E. 5.4.1).

38 If, in addition to the license plate and thus the identity of the owner, the time, location, direction of travel and identity of other vehicle occupants are also obtained during the automated vehicle search, this data processing is within the scope of a "conventional determination of identity", which does not yet constitute a serious encroachment on fundamental rights. However, this changes significantly with the merging and automatic comparison of this data with other data records (there is talk of "serial and simultaneous processing of large and complex data records within fractions of a second") and the subsequent use by the authorities; the intensity of the interference increases "considerably", among other things because of the danger that persons may be wrongly suspected (BGE 146 I 11 E. 3.2).

39 The entry in a watchlist maintained by FINMA, which serves as a preliminary stage to possible restrictions on gainful employment in the area of the financial market and, in sum, leads to an actual personality profile, constitutes a serious encroachment on Article 13 para. 2 FC and requires a basis in the form of law (BGE 143 I 253 E. 4).

40 If a police law places the technical surveillance of generally accessible places under the catchphrase of "safeguarding public order and security", this statement of purpose is insufficient and, in particular, does not allow the legal basis

to be examined for its proportionality (in particular, the relationship between the ends and the means). (BGE 136 I 87 E. 8.3-8.4).

The sufficient definiteness of a norm can also result from the network of applicable norms: If it is objected that Art. 91 para. 5 SchKG has an insufficient density of norms for the disclosure of data containing personal data and/or personality profiles that are particularly worthy of protection, this must be countered by the fact that the provision is only applied within the framework of the execution of the attachment. Thus, the purpose and scope of the data processing are defined sufficiently precisely. (BGE 124 III 170 E. 3a)). 41

6. excursus: consent "in individual cases" (para. 4 lit. b)

In public data protection law, it is often not clear to what extent consent can replace the legal basis. The question of consent arises particularly acutely where serious encroachments on fundamental rights positions are involved; the focus here is on the waiver of fundamental rights or consent to particularly serious encroachments on fundamental rights. At the other end of the spectrum of interference, however, there may be just as many question marks, for example when it comes to the sending of a newsletter by a public authority or the obtaining of a reference in a recruitment procedure. Art. 34 FADP provides under para. 4 lit. b for consent as a substitute for the rule of law, and the same applies to Art. 36 para. 2 lit. b FADP with respect to the disclosure of personal data. In both cases, consent is linked to the individual case, but is otherwise not subject to the condition that the facts of the case are of little or no danger. In contrast to consent in private data protection law (see Art. 6 para. 6 and 7 FADP), it is not sufficient in public law for consent to be voluntary and informed. In addition, consent must be suitable in the specific case to take over the functions of the principle of legality at play. Beyond these substantive requirements, consent in public law is not bound by any form. 42

The Federal Supreme Court and doctrine agree that the principle of legality fulfills two types of functions. On the one hand, it pursues democratic concerns; these include securing the supremacy of the will of the people on the one hand and the separation of powers on the other. On the other hand, it fulfills the functions of the rule of law; in this context, it ensures the protection of the individual against arbitrary action by the state, equal treatment and the predictability of state action. 43

44 Under certain conditions, consent can certainly replace the constitutional functions of protection against arbitrariness and predictability of state action. For this to be the case, the scope of the consent must be recognizable at the time it is given, and the context must be one in which the voluntary nature of the consent can be assumed in good faith.

45 However, a first restriction arises from the constitutional function of equal treatment: as soon as it is a matter of granting rights or imposing duties, consent can only be operationalized as a substitute for a legal principle if only individual persons are affected. Where democratic concerns are in the foreground, consent is no longer able to provide any functional compensation.

46 Accordingly, depending on the facts of the case, it must be examined, with recourse to the concerns of the principle of legality and the criteria for the requirement of legal form (see supra nos. 9-10), whether a waiver of a legal basis and reliance on consent can be justified.

47 For data processing by federal bodies, Art. 34 para. 4 lit. b FADP delimits admissibility by limiting consent to the individual case. In view of what has been said, it can be assumed that the number of situations must be very limited, both in terms of subject matter and time, and furthermore for the introduction of rights and obligations also in personal terms.

48 Therefore, despite the schematic specification of the FADP with regard to encroachments on fundamental rights, the question can ultimately only be answered reliably in concrete terms, taking into account the concerns at issue. For example, the aforementioned newsletter of an authority can be sent on the basis of consent even in the case of a very large number of recipients and also with an unlimited periodicity, whereas the use of facial recognition systems even in an area that is narrowly defined in terms of location, time and personnel is unlikely to be permissible on the basis of consent in individual cases due to the intensity of the encroachment on the fundamental rights of the persons concerned and the social explosiveness of the technology used.

BIBLIOGRAPHY

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.

MATERIALS

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).

COMMENTARY ON

Art. 35 FADP

A commentary by Sandra Husi-Stämpfli

SUGGESTED CITATION

Sandra Husi-Stämpfli, Kommentierung zu Art. 35 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Husi-Stämpfli, N XXX zu Art. 35 DSG.

Art. 35 Automated data processing as part of pilot trials

[1] Before a formal enactment comes into force, the Federal Council may authorise the automated processing of sensitive personal data or other data processing under Article 34 paragraph 2 letters b and c if:

a. the tasks for which the processing is required are regulated in a formal law that is already in force;

b. adequate measures have been taken to limit any violation of the data subjects` fundamental rights to a minimum; and

c. a test phase before the enactment comes into force is essential for the practical implementation of the data processing, in particular for technical reasons.

[2] The Federal Council shall obtain the FDPIC`s opinion beforehand.

[3] The competent federal body shall submit an evaluation report to the Federal Council no later than two years after the start of the pilot trial. In the report, it shall propose the continuation or discontinuation of the processing.

[4] Automated data processing must in every case be discontinued if no formal enactment containing the required legal basis has come into force within five years of the start of the pilot trial.

CONTENT

IN A NUTSHELL

The provision for conducting pilot tests allows personal data requiring special protection to be processed, even if no formal legal basis exists yet. The aim of the provision is to allow experimental data processing for a limited period of time if this is indispensable in order to address certain technical innovations, organizational issues or further uncertainties.

I. GENERAL

A. Background

1 The need for powerful applications not only in the so-called "e-areas," i.e., eGovernment or eHealth, but more generally in the context of governmental task fulfillment is growing with the digitization of our lives and activities.

2 Since digitization projects generally entail high investment costs, but at the same time it is often impossible to assess whether the applications in question can be implemented technically as hoped, opportunities must be provided for evaluating the design and, in particular, the networking of applications as part of pilot trials. Pilot tests are to be understood as tests to gain knowledge about the feasibility or acceptance of a project.

B. Purpose of the standard

3 Pilot tests must not lead to the principles of the rule of law being undermined. Even if, due to the experimental nature of data processing and the complexity of the legislative process, it is not yet possible at the time of the pilot project to fall back on the legal bases provided by the Constitution (with an appropriate level and density of norms), minimum legal requirements must nevertheless be observed.

4 Art. 35 FADP therefore allows the Federal Council to conduct pilot tests for a limited period of time, based only on an ordinance (and not on a law in the formal sense, as would be required for particularly sensitive personal data, Art. 34 para. 2 FADP).

C. History

As early as 1999, the motion "Increased protection for personal data in online connections" was submitted. It formed the basis for the later Art. 17a aDSG and the regulation of data processing in the context of pilot tests, in which the personal rights of the persons concerned could be particularly endangered. The content of Art. 35 FADP was incorporated into the new Data Protection Act largely unchanged and uncontested in the parliamentary deliberations. 5

II. PREREQUISITES FOR A PERMISSIBLE PILOT TEST (PARA. 1)

Personal data requiring special protection or other data processing pursuant to Art. 34 (2) (b) and (c) FADP may only be processed as part of a pilot test and as an exception to the requirement of a legal basis if the following conditions are cumulatively met: 6

A. Task norm in a law in the formal sense (lit. a)

The tasks for the fulfillment of which the pilot project with the automated processing of personal data requiring special protection is to be required must already be regulated in a law in the formal sense at the time of the pilot project (see OK-Zysset on Art. 34 FADP), and the law must also already be in force. 7

It is not sufficient for the formal legal basis to merely regulate the tasks requiring processing. The requirement of norm density must be met, if not for the pilot project itself, then at least for the tasks underlying the project. The legal basis must thus describe the body that has access to the data, the specific purpose of the access, and the scope of the access authorization. 8

B. Limiting violations of privacy to a minimum (lit. b)

In order to minimize the risks posed by the pilot project to the data subjects, organizational, technical and legal measures must be taken, in particular to ensure data security. The protective measures must minimize the possible threat of personality violations. The new wording of Art. 35 (1) (b) FADP thus does justice to the fact that the risk of personality violations in the context of digitized data processing can de facto never be completely excluded. 9

C. Indispensability of the test phase (lit. c)

10 Pilot projects for the processing of personal data requiring special protection and the associated relativization of the principle of legality may not be initiated lightly: Art. 35 para. 1 lit. c FADP requires that the test phase is indispensable, in particular for technical reasons. At the same time, however, the legislator admits that there may well be other reasons, e.g. organizational reasons, which make a pilot test necessary for the processing of particularly sensitive personal data ("in particular").

11 Combinations of technical and organizational conditions are also conceivable, which would not justify recourse to Art. 35 FADP on their own, but together make a pilot test necessary, especially when it is a matter of testing information systems and checking interfaces across the federal levels, for example. And finally, the Covid pandemic has shown that there may also be unanticipated reasons to conduct a pilot test: Based on the then Art. 17a aDSG (in conjunction with Art. 78 para. 1 EpG), the Swiss Covid app was operated during a one-month trial phase to test the "newly developed solution approaches with regard to the decentralized nature of data processing and cryptographic methods, (the) stability of operation, (the) protection against unintentional or unauthorized manipulation, (the) user-friendliness (as well as the) comprehensibility of the information for the participants and for the professionals authorized to access it." In this case, and due to the urgency of the situation, the pilot phase lasted only from May 14, 2020 to June 25, 2020, after which the app was put into regular operation.

III. REGULATION OF THE PILOT PROJECT IN AN ORDINANCE.

12 Even though Art. 35 FADP, in contrast to its predecessor provision Art. 17a para. 3 aDSG, no longer explicitly provides that the Federal Council must precisely regulate the pilot project in an ordinance, this obligation not only remains pursuant to Art. 33 para. 2 lit. e FADP (obligation of the competent federal body to consult the FDPIC in the context of the licensing procedure and to submit a draft ordinance to it): It derives from the principle of legality enshrined in Article 5 para. 1 FC, from which it can be deduced that a minimum level of control under the rule of law must be maintained even during a pilot

project, or that serious encroachments on fundamental rights require at least a legal basis at the ordinance level, even in the case of pilot projects.

The ordinance must contain all those rules that would have to be adopted (outside of a pilot trial) at the level of laws and ordinances. It is important - especially with regard to the mandatory evaluation (n. 16) - that it is specified in advance as precisely as possible what exactly is to be tested. 13

IV. OBLIGATION TO OBTAIN THE OPINION OF THE FDPIC (PARA. 2)

The pilot project must be submitted to the FDPIC for its opinion. This provision establishes an essential control mechanism that takes into account the fact that pilot projects may deviate from the constitutional principle of the standard level. As an element of the "checks and balances", the FDPIC is responsible at least for the plausibility check of the pilot project, the control of the protective mechanisms adopted, the review of the ordinance as well as regular evaluations. For this purpose, according to Art. 33 para. 2 and para. 3 FADP, the FDPIC must be provided with detailed information, in particular on the pilot project as such, the organizational and technical (security) measures, a draft or at least a concept for the ordinance that is to regulate the pilot test, as well as a project plan. 14

Even if the FDPIC cannot issue a binding opinion, it can be assumed that the Federal Council will generally follow the FDPIC's assessment. 15

V. EVALUATION AND TIME LIMIT OF THE PILOT PHASE (PARA. 3 AND 4)

The pilot project must be evaluated at the latest within two years of going into operation (Art. 35 para. 3 FADP). In the evaluation report, the body responsible for the pilot test must explain to the Federal Council whether the project can already be transferred to a regular service, whether the pilot test should be continued (but note the maximum time limit of five years, n. 17) or whether the project should be discontinued. 16

Overall, the pilot phase may last a maximum of five years (Art. 35(4) FADP). This time limit cannot be extended, not even if the pilot is to be converted 17

into a regular service but no legal basis has yet been developed - "regular" operation based on a mere draft is not permissible for reasons of the rule of law.

VI. APPRAISAL

18 Although Art. 17a of the FADP has only been used very rarely to date and the Federal Council asserts that it will only make use of Art. 35 of the FADP in exceptional cases, it can be assumed that the digital transformation of the administration will also lead to more frequent use of the pilot test provision. This may well be in the interests of the digital further development of the federal administration, but it should not be forgotten that the application of Art. 17a aDSG or Art. 35 FADP is always accompanied by an undermining of the principle of legality. An overly generous recourse to Art. 35 FADP, without, for example, a task norm in the formal sense existing or the indispensability of the test phase having been seriously examined, should therefore be avoided. After all, it cannot be denied that pilot projects are always accompanied by high investment costs - the decision not to continue operating a system after the end of the test phase should therefore not only be difficult, but also rare.

The author gives her personal assessment in this commentary.

BIBLIOGRAPHY

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.

COMMENTARY ON

Art. 38 FADP

A commentary by Claudia Schreiber

SUGGESTED CITATION

Claudia Schreiber, Commentary art. 38 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Schreiber, art. 38 FADP N. XXX.

Art. 38 Offering documents to the Federal Archives

[1] In accordance with the Archiving Act of 26 June 1998, federal bodies shall offer to the Federal Archives all personal data that they no longer regularly require.

[2] They shall destroy personal data that the Federal Archives do not deem to be worth archiving unless:

a. the data are anonymised;

b. they must be preserved for evidentiary or security purposes or to safeguard the data subject's legitimate interests.

CONTENT

I. IN A NUTSHELL

Art. 38 FADP has an important bridging function between the Federal Act on Data Protection (FADP) and the Federal Act on Archiving (ArchA). 1

Today, Art. 38 FADP can give rise to misunderstandings, as archiving practice has changed at federal level, particularly in connection with the introduction of prospective evaluation in 2010. 2

II. GENERAL INFORMATION

A. History of origin

The fact that data protection, archiving and historical research, which relies on archived documents, have different interests has already been sufficiently discussed. In connection with the drafting of the first federal law on data protection at the end of the 1970s, fears arose in parts of the archiving world that data protection efforts could lead to an "increasing tendency towards destruction/deletion" and "restraint in the use and authorization practices of individual departments". These fears arose in particular because the first data protection law at federal level was drafted at a time when archiving at federal level was only regulated at the level of regulations and directives. 3

Initially, it appeared that the new Data Protection Act would address the issue of archiving personal data in detail, as the Working Group on Data Protection in the Federal Administration proposed drafting an Art. 20 entitled "Destruction and archiving of data" or "Archiving and destruction of data", which would contain detailed regulations on the archiving of (personal) data: A draft of the working group states: "Data carriers with permanently valuable data may be archived (Var.: preserved) in the Federal Archives beyond the time of the originally necessary processing; their further processing is only permitted within the framework of the regulations for the Federal Archives." 4

However, this proposal was not subsequently accepted. A special regulation regarding the archiving of data was dispensed with: The then Art. 18 para. 2 FADP as well as Art. 21 of the first FADP of 19 June 1992 deleted archiving from the title and stated under the title "Anonymization and destruction of personal data" that federal bodies must anonymize or destroy personal data 5

that they no longer need, unless "the data serve evidentiary or security purposes" or "are to be handed over to the Federal Archives". This laid the foundation for the character of today's Art. 38 FADP.

6 In a nutshell, after the first FADP came into force at federal level in 1992, the Federal Council instructed the Federal Department of Home Affairs (FDHA) to draw up a preliminary draft for the creation of a federal law on archiving in a resolution dated August 18, 1993. The work was subsequently undertaken by an interdepartmental working group. The need for a legal basis for archiving in a formal federal law arose from the obvious upheavals in the archiving sector (including the massive increase in the volume of files produced by federal agencies after the Second World War and the increased production of electronic documents in the last quarter of the 20th century) as well as from the demand for the "realization of appropriate data protection", as stated in the dispatch on the Federal Act on Archiving of 26 February 1997.

7 At the same time, the dispatch on the BGA stated that the right to inspect archive records does not mean the right to unchecked disclosure or uncritical forwarding of personal data. Rather, the right to inspect archival material "compels a critical review of the content of archived documents and their interpretation and presentation in keeping with the protection of personality rights"; this responsibility lies with the users of the archive. It should be noted here that in the case of documents that are still within the protection period and were not already publicly accessible prior to their delivery (cf. Art. 9 para. 2 BGA), the delivering authority will check in advance, in accordance with Art. 13 para. 1 lit. b, whether there are no overriding private interests that prevent access before the protection period expires and whether, if necessary, access should be granted subject to conditions and requirements, such as anonymization of personal data (Art. 13 para. 3 BGA).

8 With the entry into force of the BGA in 1999, the issues of data protection in the area of archiving were now also addressed from an archive perspective. With the introduction of the protection period regulation and the possibility thus created to extend the protection period for the inspection of documents in certain cases (Art. 11 and 12 BGA), the BGA explicitly aimed at "harmonization". As archive records may not be altered (Art. 14 para. 4 BGA), the denial note pursuant to Art. 15 para. 3 BGA supplements the protection period regulation. Furthermore, according to Art. 14 para. 2 BGA, the inspection of personal data by the authority creating or delivering the file is restricted during

the protection period, unless the exceptions according to Art. 14 para. 1 (lit. a-d) apply. According to the dispatch on the BGA, this ensures that "on the one hand, the interests of the persons concerned must be protected, but on the other hand, (historical) research in the public interest should not be hindered."

The new BGA therefore had an impact on the existing Data Protection Act. However, until 2006, Article 21 of the Data Protection Act only regulated the transfer of personal data to the Federal Archives as an exception for anonymization and destruction. 9

However, the current Article 38 FADP underwent a significant change in 2008 (version according to no. I of the Federal Act of March 24, 2006, in force since Jan. 1, 2008). Accordingly, the archiving of personal data was no longer an exceptional case of destruction or anonymization. Instead, reference was now made to the new Federal Act on Archiving, which has since come into force. This law now also introduces concepts from the archiving world into the Data Protection Act with the terms "offer" or "offering" and "archival value". 10

Since 2008, Article 21 of the aDSG, now Article 38 of the new FADP, which came into force on September 1, 2023, has remained essentially unchanged, but the enforcement of archiving legislation at federal level has developed significantly during this time, as the following explanations will show. 11

B. Scope of application

Art. 38 FADP is addressed to all federal bodies pursuant to Art. 2 para. 1 lit. b FADP. In Art. 1 para. 1, the FADP lists all bodies whose archiving is regulated by the FADP. The norm addressee is also the Federal Supreme Court, which in accordance with Art. 1 para. 3 regulates the archiving of its own documents, but does so in accordance with the principles of the ArchA and after consulting the Swiss Federal Archives (SFA). 12

Indirectly, Art. 38 FADP may also be relevant for record creators pursuant to Art. 17 para. 2 FGA, i.e. for persons under private or public law of national importance who voluntarily hand over their documents to the SFA for secure and appropriate storage and communication. As a rule, the corresponding donation and deposit agreements refer to the fact that the documents are subject to the same provisions for inspection as the documents of the federal state (Art. 9 ff. of the Federal Act on Archiving, ArchA). It can therefore be assumed 13

that, unless otherwise agreed between the file creator and the SFA, documents from private archives that constitute or contain personal data and are worthy of archiving can also be submitted to the SFA in accordance with Art. 38 FADP and, in particular, by applying the protection period regulation pursuant to Art. 9 et seq.

14 On the question of whether Art. 38 FADP can only apply to personal data that was obtained or processed lawfully, it should be pointed out with Epiney and others that the demand for the systematic destruction of documents that contain or represent personal data that was obtained and processed in a wholly or partially unlawful manner may, depending on the initial situation, be opposed by a public interest in the preservation of documents that were created by the administration in an unlawful manner. In addition, such a strict regulation would undermine the principles and objectives of the BGA as well as any requests for access by those affected, e.g. with regard to claims for compensation. The state security files, for example, which were handed over to the SFA, are valuable federal documents from a legal, political and historical perspective that document the business practices of the federal authorities, as postulated in Art. 2 para. 1 ArchA.

C. Terms

15 Where archive legislation and data protection legislation come into contact with each other - as in Art. 38 FADP - different perspectives and concepts collide. Archives legislation is based on the concept of "records". According to Art. 3 para. 1 FADP, documents are "all recorded information, regardless of the information carrier, which has been received or created in the performance of public tasks of the Confederation, as well as all aids and supplementary data necessary for the understanding of this information and its use." Data protection legislation, on the other hand, refers to personal data, which is defined in Art. 3 lit. a FADP as "any information relating to an identified or identifiable person". The question therefore arises as to the relationship between these two terms. For the following explanations, it is postulated that personal data is both a sub-category and a possible characteristic of recorded information (documents). In other words, personal data are always documents within the meaning of the BGA. Conversely, documents can contain personal data, but do not have to.

Article 38 FADP builds another bridge to the BGA with the use of the terms "offer" and "offer". However, the terms "offer" and "offering" are used differently in the FADP and the corresponding implementing legislation, and their meaning has changed to some extent over the last fifteen years. 16

On the one hand, the SFA refers to the "authorities obliged to offer" and thus, in conjunction with Art. 1 para. 1 SFA, outlines the relationship between the SFA and the federal authorities that are subject to the SFA's duty to issue instructions and are obliged to offer to the SFA. On the other hand, the terms "offer" and "offer" also describe work steps in the life cycle of documents. These steps are related to the appraisal of documents and are the subject of a significant change in practice, the shift from retrospective to prospective appraisal, which is described in the overall concept for appraisal in the Federal Archives in 2010. This change in practice is discussed in the following chapters. 17

III. OFFERING DOCUMENTS IN THE CONTEXT OF PROSPECTIVE APPRAISAL (PARA. 1)

The overall concept for appraisal in the Federal Archives, which was published in 2010, postulates in principle the abandonment of retrospective appraisal in favor of prospective appraisal. 18

While retrospective appraisal involves assessing the archival value of documents that have already been created, prospective appraisal involves appraising documents before they are created. This evaluation takes place during the development or revision of classification systems in accordance with Articles 7 and 8 of the GEVER Ordinance. Regulatory systems are drawn up by federal agencies and, in the case of agencies subject to the obligation to offer, are reviewed and approved by the SFA, provided they meet the requirements of the GAOA or the implementing provisions of the GAOA. In a classification system, series of documents are evaluated at the category level, i.e. it is determined whether the documents that will arise in the course of a federal agency's duties are fully, partially (selection or sampling) or not at all worthy of archiving. Only business-relevant documents are evaluated; non-business-relevant documents are not considered documents within the meaning of the BGA and are not subject to the obligation to offer. 19

20 The switch to prospective valuation has not been without consequences for the meaning of the term "offer" or "offer". In the case of retrospective appraisal in application of Art. 6 para. 1 ArchA, existing document series were offered to the SFA by the non-independently archiving agencies with a proposal for legal-administrative appraisal (offer for takeover) and the SFA also carried out a retrospective appraisal from a historical-social science perspective.

21 With the introduction of prospective appraisal, "offers" are made to the SFA at two different points in the life cycle of documents. The appraisal of documents takes place as part of the development or updating of a classification system and is to be understood as an offer for appraisal. The subsequently created archive-worthy documents are submitted to the SFA for submission at a later date (i.e. transmission of Submission Information Packages SIP containing files including metadata and indexing data for the submission of electronic documents or archive boxes containing paper dossiers for paper submissions). Since the introduction of prospective appraisal, the appraisal of documents in cooperation between file creators and the SFA and the transmission or submission of documents to the SFA no longer coincide.

22 As indicated above, both in the retrospective appraisal, which was the majority practice before 2010, and in the prospective appraisal after 2010, the federal agency concerned is involved in the appraisal alongside the SFA. The federal agency creating the file evaluates the documents per category from a legal-administrative perspective. This evaluation is the responsibility of the management/directorate of the federal offices concerned and ensures that the technical, legal and political aspects are taken into account. In a second step, the SFA reviews the legal-administrative evaluation of the authority creating the file and also carries out an evaluation according to historical-social science criteria. If one of the two evaluations is positive, the documents are deemed to be archivable (in full or in part in the form of sampling or selection). In exceptional cases, the prospective evaluation may be subject to a subsequent review.

IV. PERSONAL DATA THAT ARE NO LONGER PERMANENTLY REQUIRED (PARA. 1)

The literature often deals with the question of when personal data are no longer permanently required without reference to the document context. This approach can hardly be implemented in practice. This is because personal data are always documents within the meaning of the BGA, unless they are not relevant to business. Art. 6 of the FADP stipulates that documents must be submitted to the SFA when they are no longer permanently required. 23

If one were to assume that the question of when personal data is no longer permanently required would have to be answered differently from the question of when documents are no longer permanently required, then the conclusion would follow that documents worthy of archiving that contain or represent personal data may have to be submitted to the SFA at a different point in time than documents that do not contain or represent personal data. However, the SFA assumes that the business dossier is the relevant unit for archiving. In this respect, business files are often of a mixed nature: they consist of documents that contain personal data as well as documents that do not contain or represent personal data. It therefore makes sense for the federal authorities to consider the question of when personal data is no longer permanently required in the context of documents and to observe the implementing provisions of the FADP in this regard. 24

Pursuant to Art. 4 para. 1 OBGA, documents are deemed to be no longer permanently required if the body subject to the obligation to provide them no longer makes frequent, regular use of them, but no later than five years after the last addition to the file. Art. 3 para. 1 of the directives on the obligation to offer and the delivery of documents to the Swiss Federal Archives of September 28, 1999 also stipulates that the offices subject to the obligation to offer must regularly, but at least every five years, review their files and information repositories with regard to documents that they no longer need frequently and regularly. Art. 4 para. 2 VBGA and Art. 3 para. 2 of the directives regulate the extension of this period. Art. 4 para. 3 OBGA and Art. 3 para. 3 of the Directives also regulate cases of shortened deadlines. For certain categories of documents, more specific requirements apply in accordance with Art. 4 para. 3 OBGA and Art. 4 of the Directives. 25

26 Since the introduction of prospective evaluation in 2010, these time limits are to be understood as deadlines for the submission to the SFA of documents that have already been evaluated and are therefore worthy of archiving.

V. DESTRUCTION OF DOCUMENTS NOT WORTHY OF ARCHIVING (PARA. 2)

27 Reference is made to Art. 5 lit. d and Art. 6 para. 4 FADP regarding the processing procedure for destruction.

28 The wording "personal data designated by the Federal Archives as not worthy of archiving" used in paragraph 2 of Art. 21 is misleading because, as explained above, the appraisal of documents (and thus also of personal data) is not carried out by the SFA alone, but by the authority creating the file together with the SFA. Since the introduction of prospective appraisal in 2010, the moment documents are stored in the electronic records management system (GEVER), it is clear from the link between the corresponding business dossier (or a specialized application) and a category in the appraised classification system whether the documents containing or representing personal data are worthy of archiving (in part or in full) or not.

29 In this context, it should be noted that the destruction of documents must be recorded and that the resulting cassation records must be submitted to the SFA.

VI. ANONYMIZATION OF PERSONAL DATA (PARA. 2 LIT. A)

30 With regard to the term anonymization, reference is made to the commentary on Art. 2 para. 1 lit. a FADP and Art. 6 para. 4 FADP. Para. 2 lit. a FADP allows federal authorities to retain documents that are not worthy of archiving or documents that are only assessed as partially worthy of archiving (sampling or selection) that are no longer permanently required, or to retain them in their entirety, provided that they are anonymized. However, since the changeover to electronic business management, such storage can only be temporary storage and not archiving within the meaning of the ArchA, as the federal authorities only have the infrastructure required for long-term electronic archiving available to them within the scope of submission to the SFA.

VII. RETENTION FOR EVIDENTIARY OR SECURITY PURPOSES, SAFEGUARDING THE INTERESTS OF THE DATA SUBJECT WORTHY OF PROTECTION (PARA. 2 LIT. B)

As part of the administrative-legal assessment, the record-creating body shall check whether documents are to be stored permanently. The involvement of the file creators is intended to ensure that the "technical, legal and political aspects are carefully taken into account in the evaluation". From a legal-administrative perspective, documents are worthy of archiving in particular if they serve as evidence of business practice, have legal relevance or serve to ensure legal certainty. 31

If documents that contain personal data or constitute personal data must be retained for evidentiary or security purposes or to protect the legitimate interests of the persons concerned, they have generally already been assessed as archival value in the legal-administrative assessment. Accordingly, as in the cases of Art. 38 para. 2 lit. b FADP, only personal data that is contained in documents or constitutes documents that were assessed as not worthy of archiving in the prospective evaluation or, in the case of partial archival value, are not part of the sample to be archived or part of the selection to be archived, are to be expected as cases of application of Art. 38 para. 2 lit. b FADP. For example, accounting documents that are not worthy of archiving and are used as evidence in ongoing or impending proceedings are conceivable. 32

VIII. IMPLEMENTATION WITH MISUNDERSTANDINGS

In practice, however, Art. 38 FADP is not yet consistently understood in this sense, as can be seen in the literature and case law. In decision A-4236/2021 of the FAC of March 21, 2023, which refers to Art. 21 aDSG, for example, the FTA, which has an approved filing system, takes the position in connection with a request for data destruction that the FTA "can decide for itself" when the lawfully processed data should be offered to the Federal Archives. A party cannot request that the lawfully processed personal data be offered to the Federal Archives or destroyed. Therefore, it is not required to offer legally processed personal data from a dossier whose last addition to the file took place in 2020 to the Federal Archives at the request of the complainant or to destroy it." The FTA thus refers to the deadlines set out in the FNA and the 33

implementing legislation to the FNA, but at the same time fails to point out that the documents in question have already been assessed by the FTA and the SFA.

34 In its decision of March 21, 2023, the Federal Administrative Court also follows the evaluation practice prior to 2010 and writes: "It is not up to the Federal Administrative Court to clarify the question of the archival value of the data collected by the lower instance in the administrative assistance proceedings as the first instance in the appeal proceedings, especially since the responsibility for this decision does not lie with the lower instance, but with the Federal Archives, which has not yet been able to comment on this. [...] The lower instance must offer the data collected as part of the administrative assistance proceedings to the Federal Archives and, if the latter classifies the data as worthy of archiving, hand it over. If the data is not classified as worthy of archiving, the lower instance must destroy the data."

35 This recent decision of the Federal Administrative Court is an example of the misunderstandings that the current version of Art. 38 para. 1 FADP can lead to: Article 38 para. 1 FADP seems to suggest - at least according to the reading of the FTA and the FAC - that bodies subject to the obligation to provide personal data, in this case in the form of a business dossier on a tax case relating to a specific person, may only destroy such data if the SFA has made a specific statement on this individual dossier and its assessment. This is not compatible with the SFA's archiving practice for the following reasons:

a) In the present case, the FTA, which is obliged to offer, and the SFA already carried out a prospective evaluation when the FTA regulatory system was drawn up in 2015. Whether the documents resulting from this specific activity of the FTA (exchange of information in tax matters) are worthy of archiving or not can be seen from the FTA classification system or the linking of the business file in question to a section of the classification system. The SFA and the FTA have therefore already stated whether the series of documents to which the dossier or document in question belongs is worthy of archiving (in part or in full) or not.

b) The evaluation, both prospective and retrospective, relates to series of documents that arise in the performance of specific tasks and, where applicable, to specialized applications - but not to individual data records, individual personal data, individual documents or business dossiers. In other words: How

these series of documents are created and, in particular, the form in which the documents are filed in dossiers is a matter for the Federal Office of Justice to decide in accordance with Art. 2 para. 2 and Art. 5 para. 2 and 3 BGA in conjunction with Art. 3 VBGA. Art. 3 VBGA as well as Art. 6 GEVER Ordinance and Art. 22 RVOV fall within the area of responsibility of the bodies obliged to offer or create files. These are required to ensure the traceability and verifiability of their business activities in their records.

If, in the above-mentioned case, the corresponding series of documents had been assessed in the FTA classification system as worthy of archiving or as partially worthy of archiving (selection or sampling), the file-creating office would only have to decide, in application of the SFA and the implementing provisions to the SFA, when the dossier in question should be submitted to the SFA. Furthermore, in this case the file-creating office would decide whether the document in question was required for the traceability and verifiability of the business activities in this dossier. In the case of partial archival value, the authority creating the file would also implement the selection or sampling criteria set out in the OS. In this constellation, the SFA would also no longer have any decision-making authority after the prospective evaluation has been carried out. 36

If the corresponding series of documents had been assessed as not worthy of archiving, the authority creating the file would also decide what to do with the document or business file in question containing personal data. In other words, whether it should be stored temporarily in anonymized form in accordance with Art. 38 para. 2 lit. a FADP or in non-anonymized form in accordance with Art. 38 para. 2 lit. b FADP for evidence and security purposes or to protect the interests of the data subject worthy of protection. In this constellation, too, the SFA would no longer have the authority to make a decision after the prospective evaluation has been carried out. 37

Against this background, Art. 8 para. 1 ArchA is to be understood as meaning that only documents that have not been offered to the SFA for (prospective) evaluation may not be destroyed without the SFA's consent. In view of the comprehensive obligation to offer documents to the SFA, such documents are likely to be rare. 38

IX. APPRAISAL

39 Art. 38 FADP has its origins in the 1980s and was conceived as an instrument to prevent file creators from using the pretext of data protection to prevent the SFA from archiving documents that contain personal data or constitute personal data solely on the basis of this fact. Art. 38 FADP is still of practical relevance today, as the provision specifies the principle of proportionate data processing with regard to archiving: Not only the anonymization or destruction of documents that are not worthy of archiving and that contain or represent personal data is therefore proportionate once the necessary processing by the authorities creating the file has been completed, but also the (non-anonymized) submission of such documents to the SFA, provided they are worthy of archiving.

40 In its current version, Art. 38 para. 1 FADP is based on the practice of retrospective evaluation, which was standard practice at the SFA until the 2000s. Since the switch to prospective evaluation as the standard process, all federal agencies evaluate their documents in accordance with Art. 1 para. 1 FADP from a legal-administrative perspective and the SFA from a socio-scientific-historical perspective as part of the development of classification systems, i.e. before the documents are created.

41 Under the heading "Archiving of personal data", a revised Article 38 could in future limit itself to stating that documents pursuant to the ArchA may contain or constitute personal data and must be handled in accordance with the requirements of the ArchA (paragraph 1). A new para. 2 could stipulate that documents not worthy of archiving that contain or constitute personal data must be destroyed unless the conditions mentioned in the existing para. 2 lit. a and b apply.

The author would like to thank MAS ISc Barbara Kräuchi for the stimulating exchange of expertise in the course of the research for this article.

BIBLIOGRAPHY

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).

MATERIALS

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).

COMMENTARY ON

Art. 39 FADP

A commentary by Philipp do Canto

SUGGESTED CITATION

Philipp do Canto, Commentary art. 38 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-do Canto, art. 39 FADP N. XXX.

Art. 39 Data processing for purposes not related to specific persons

[1] Federal bodies may process personal data for purposes not related to specific persons, in particular for research, planning or statistics, provided:

a. the data are anonymised as soon as the purpose of processing permits;

b. the federal body only discloses sensitive personal data to private persons in such a manner that the data subjects are not identifiable;

c. the recipient only transmits the data to third parties with the consent of the federal body that disclosed the data; and

d. the results are only published in such a manner that the data subjects are not identifiable.

[2] Articles 6 paragraph 3, 34 paragraph 2 and 36 paragraph 1 do not apply.

CONTENT

IN A NUTSHELL

Art. 39 FADP allows federal bodies to process data for non-personal purposes under certain conditions. The rule grants facilitations within the meaning of the "research privilege" for research, statistics, planning and other areas. The rationale behind this is the great public interest in the activities concerned. The privilege only applies if the general conditions are met. Firstly, Art. 39 para. 1 FADP requires the earliest possible anonymization when processing personal data. Secondly, the consent of the federal body is required for the disclosure of data from the recipient to third parties. Thirdly, as in the case of private data processing in accordance with Art. 31 para. 2 lit. e FADP, federal bodies may only publish research or other results in such a way that data subjects cannot be identified.

As non-personal data processing does not involve the identity of the data subjects, Art. 39 para. 2 FADP declares that important principles are not applicable. For example, the requirement of purpose limitation and the requirement of a legal basis do not apply in certain constellations, e.g. for the disclosure of personal data. On the other hand, numerous special statutory provisions, namely in the area of statistics and research, which relativize the practical significance of Art. 39 FADP, must be taken into account.

I. GENERAL

1 Art. 39 FADP on the processing of data for non-personal purposes by federal bodies largely takes up the predecessor provision of Art. 22 aDSG with the so-called "**research privilege**". What is new is a specification regarding particularly sensitive personal data. According to Art. 39 FADP, federal bodies should (continue to) benefit from facilitations for processing for non-personal purposes if they comply with the framework conditions. This privilege is justified by the public interest in the relevant activities of the state. Research and statistics provide the basis for all aspects of public life.

2 The **conditions for facilitation** include, on the one hand, the obligation to anonymize at the earliest possible point in time (para. 1 lit. a). Secondly, conditions regarding the disclosure of particularly sensitive personal data to third parties must be observed (para. 1 lit. b). Secondly, a consent requirement applies to disclosure by the recipient (para. 1 lit. c) and finally the requirement of

non-identifiability when publishing the results (para. 1 lit. d). Art. 39 para. 2 declares that certain principles of the FADP are not applicable due to the reduced risks in the case of non-personal processing (para. 2).

The provision refers only to **data processing by federal bodies**. The provision mentions research, statistics and planning as privileged areas, although the list is not exhaustive. In addition to federal statistics, this includes research by federal institutions or on their behalf, national spatial and transport planning, the National Bank, migration management and public health. In contrast to the private sector, medical research, which is governed by human research law, tends to be in the background of the provision, as this area is mainly supported by the cantonal university hospitals and private pharmaceutical research. In contrast, research conducted by the ETH Domain as a decentralized federal unit is covered. 3

Due to the requirement of a legal basis for state data processing, the various activities are now extensively **regulated by special legislation** (below, IV). Art. 39 FADP therefore loses its independent meaning in numerous constellations or must be read in conjunction with the subject-specific provisions. 4

II. PARA. 1, REQUIREMENTS IN DETAIL

A. Basic facts: non-personal purpose

The central element of the provision is processing for non-personal purposes. Non-personal purposes are defined as purposes for which the **identity of the data subject is irrelevant**. In other words, the purpose of the activity is also fulfilled if anonymized or encrypted data is processed. The processing of data of large parts of the population as well as individual groups is covered, as long as it only concerns the characteristics and not the identity of the persons recorded. If only factual data or previously anonymized data is processed, the provision is not applicable. 5

The explicit mention of the areas does not mean that data processing in the areas of research, statistics and planning serves non-personal purposes. In particular, there are processing activities that **also serve personal purposes**. For such activities, Art. 35 FADP states that the exceptions under Art. 39 para. 2 FADP only apply to processing for non-personal purposes. 6

7 The introductory sentence to para. 1 contains the legal consequence, namely the simplified **authorization of data processing** if the requirements of the provision, which are explained below, are met.

B. Lit. a, Earliest possible anonymization

8 Federal bodies must (in principle) **anonymize** the data as soon as the purpose of the processing permits. The provision thus takes up the principle of Art. 6 para. 4 FADP. A deadline for anonymization is not specified. A general, abstract regulation would not meet the respective needs of statistics, research and planning.

9 In contrast to Art. 31 para. 2 lit. e FADP, no exception has been included that allows other measures to prevent the identifiability of the person if anonymization is impossible or disproportionate. Opinions differ on the question of whether **pseudonymization** or encryption of personal data is sufficient. If a code or key is available with which (partially) anonymized personal data can be re-identified, this is referred to as pseudonymization. Some scholars only want to allow encryption if the processing ultimately leads to anonymization. The opposing view is based on the widespread need in practice for the possibility of tracing the identity of the person concerned, which is opposed to anonymization, especially the required early anonymization. Furthermore, general anonymization is not in line with lit. b, according to which it is sufficient for particularly sensitive personal data if it cannot be identified when it is disclosed to private individuals, which also permits encryption. If encryption or "de facto anonymization" is sufficient for the disclosure of particularly sensitive data, this should also apply *a maiore minus* to less sensitive data. The dispatch on the aDSG mentions a need for pseudonymization. A decision by the Federal Supreme Court does not answer the question conclusively, but sees the solution in the purpose of the respective procedure: "There are, of course, limits to concealment. It must not lead to the judgment no longer being comprehensible. It can therefore not be completely ruled out that people who are familiar with the details of the case may be able to recognize who is involved despite the concealment." If anonymization therefore removes the purpose of the processing (which, however, does not always have to be personal), appropriate other measures to prevent the person from being identifiable must also be permissible.

C. Lit. b, Particularly sensitive data

The second requirement concerns the disclosure of particularly sensitive data to private individuals. The provision is a specific regulation in addition to the general provisions on the disclosure of data in Art. 36 FADP. In the case of particularly sensitive data, the principle applies that such data may only be disclosed to third parties in such a way that **the data subject cannot be identified**. In contrast to the wording of lit. a, anonymization is not required here; instead, prior encryption is also sufficient for the increased protection of the data. 10

In connection with measures to prevent identifiability, reference should be made to the extensive catalog of **technical and organizational measures** in Art. 3 GDPR, in particular the rules on confidentiality and integrity. There are also various guidelines on encryption, such as the binding scientific linking guidelines of the Federal Statistical Office or the guidelines of the European Cybersecurity Agency (Enisa). Among other things, the guidelines contain requirements for handling the codes and for de-pseudonymization. 11

Statutory confidentiality regulations also play a role. Where special legislation does not permit the disclosure of particularly sensitive data (to private parties) as an integral part, it takes precedence as a special regulation. Lit. b can therefore not be used as a justification for the disclosure of data that is protected by secrecy. 12

D. Lit. c, Consent requirement for disclosure

Thirdly, data may be disclosed for processing for non-personal purposes. However, according to lit. c, the consent of the federal body is required for the disclosure of the data. The consent of the federal body must be accompanied by the condition that the obligations regarding anonymization and publication are passed on to the third party. 13

For the **National Bank**, the special provision of Art. 16 para. ^{4bis} NBA applies, according to which the National Bank is authorized to disclose data to the FSO in non-aggregated form for statistical purposes. Notwithstanding Article 39 FADP, the FSO may not pass on data from the National Bank without its consent. 14

15 Art. 39 para. 1 lit. c leaves the **form of consent** open. According to the dispatch on the aDSG, consent may or must be given by contract or by order.

E. Lit. d, Publication of results

16 lit. d incorporates the previous provision according to which data subjects must not be identifiable when the results are published (Art. 22 para. 1 lit. c aDSG). Despite the same wording as Art. 31 para. 2 lit. e no. 3 FADP, (complete) **anonymization** is required for publication. Partial anonymization or pseudonymization, as is common in medical human research, is therefore not sufficient. Exceptions are conceivable, however, if the data relates to persons of contemporary history or if overriding interests in transparency require access to the file.

17 It is noted in the doctrine that the publication of studies with a small number of data subjects may give rise to a **risk of conclusions being drawn** about the individual, for example in the case of statistics for small geographical areas. However, this appears to be less of a problem when publishing results based on data from a large number of data subjects, as it is more difficult to identify the person by a human being. Technological systems, on the other hand, function independently of geographical or numerical restrictions, so that ultimately technical progress constantly increases the requirements for the publication of results.

III. PARA. 2, EXCEPTIONS

18 Art. 39 para. 2 FADP declares three provisions of the FADP inapplicable.

19 Firstly, the **requirement of purpose limitation** or prohibition of change of purpose pursuant to Art. 6 para. 3 FADP is not applicable. Because research, planning and statistical work has no direct impact on the data subjects in accordance with Art. 39 FADP, data may also be used in a different context than that for which it was collected. However, the limit of use is set by Art. 39 para. 1, according to which it may only ever be for non-personal purposes. Within this framework, data may be processed for any lawful purpose. In other words, the exception does not permit processing for other personal purposes.

20 The second exception is Art. 34 para. 2 FADP. Accordingly, the **requirement of a formal legal basis** does not apply to the processing of particularly sensitive personal data and profiles or to activities with a risk of serious interfer-

ence with fundamental rights. The principle of legality is therefore not completely eliminated. Art. 34 para. 1 FADP remains applicable. A legal basis at ordinance level is therefore still expected for such processing.

The third exception concerns Art. 36 para. 1 FADP on the disclosure of personal data. Consequently, **no specific legal basis** is **required** for the **disclosure of personal data**. Apart from the fact that Art. 39 para. 1 FADP contains requirements for the disclosure of personal data, special legislation will also regularly have to be complied with. If there are no regulations, a federal body can rely on this exception. However, this provision does not abolish the principle of legality for disclosure. 21

IV. SPECIAL LEGISLATION

Due to the above-mentioned **requirement of a legal basis** for state data processing, there is now extensive special legislation governing the activities of federal bodies. Depending on the level of detail, these can largely replace Art. 39 FADP, refer to it or supplement the provision. 22

A. Federal Statistics Act

Art. 19 para. 2 FStatA contains an almost identical provision on the disclosure of data for non-personal purposes to federal statistical producers. The provision is limited to disclosure because the FStatA contains relevant provisions on collection and processing (Art. 4 ff. FStatA). In addition to the requirements in Art. 39 para. 1 FADP, Art. 19 para. 2 lit. d FStatA requires compliance with **statistical confidentiality** and the other data protection provisions. Art. 16 para. 1 FStatA clarifies that the provisions on research, statistics and planning of the FADP apply "in addition", i.e. subsidiarily, to personal data. 23

B. Register Harmonization Act

The Register Harmonization Act (RHA) is then relevant in the area of **population statistics**. The purpose of register harmonization is to standardize and simplify the communal and cantonal registers in order to increase their statistical value and reduce the administrative burden. In addition, register harmonization makes things easier for the registers concerned. It enables the legally regulated electronic exchange of data between various official registers (cf. Art. 1 RHA). 24

C. Police information systems

25 The police and judicial authorities operate numerous registers and information systems. The systems are regulated by the Federal Act on Federal Police Information Systems (FPSI). Art. 6 para. 4 BPI allows those responsible to retain anonymized data that is intended for deletion, insofar as this is necessary for **statistical or criminal analysis purposes**. However, research with the corresponding anonymized data no longer falls under Art. 39 FADP, as it is no longer personal data.

D. Human research law and research at ETH

26 Human research law (currently under revision) with the HRA and related enactments such as the Cancer Registration Act, which contain their own provisions on pseudonymization and triage provisions regarding the application of the HRA and FADP (e.g. Art. 28 KRG), is also of importance. Of particular importance in the field of research is the development of **electronic consent** (so-called e-consent, Art. 8b E-HRA), which allows written consent to be dispensed with under certain conditions. Electronic consent plays a special role for future reuse in research, where projects often do not (or no longer) have a personal purpose (Art. 17 HRA).

27 Finally, the revised Art. 36c para. 1 **ETHG** states that personal data, including particularly sensitive personal data, may be processed in the context of research projects insofar as this is necessary for the corresponding project. According to para. 2, the FADP must be observed.

E. Archives of the Confederation

28 Finally, mention should be made of the Federal Archiving Act (ArchA), which contains the regulatory framework for the federal archives, in particular for the Federal Administration, Parliament and the federal courts. With regard to particularly sensitive personal data in non-anonymized archives, Art. 11 para. 1 ArchA provides for an **extended protection period of** 50 years.

BIBLIOGRAPHY

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).

MATERIALS

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).

COMMENTARY ON

Art. 40 FADP

A commentary by Anna Kuhn

SUGGESTED CITATION

Anna Kuhn, Kommentierung zu Art. 40 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Kuhn, N. XXX zu Art. 40 DSG.

Art. 40 Private law activities by federal bodies

If a federal body acts under private law, the provisions on data processing by private persons apply.

CONTENT

IN A NUTSHELL

Art. 40 FADP applies when federal bodies act under private law within the meaning of Art. 5 lit. i FADP. This is possible if an area is not conclusively regulated by public law and thus leaves room for private law actions. In order to determine this in individual cases, the existence of a special legal regulation must first be examined and then a distinction made between sovereign and private law actions. With administrative support activities, the administration of financial assets, private-sector state activities and parts of the administration of services, areas have emerged in which private-law action by the public sector is normally permissible and relevant. If there is private-law action, federal bodies are subject to the provisions for private individuals in the case of corresponding data processing.

However, even when applying Art. 40 FADP, public authorities acting under private law may never completely dispense with constitutional principles. For example, the obligation to respect fundamental rights or the principle of legality continue to apply.

I. GENERAL

A. Preliminary Remarks

Art. 40 FADP remains unchanged from the previous version (Art. 23 para. 1 aDSG) and has undergone only minor editorial changes. 1

The previous second paragraph, according to which supervision is governed by the provisions for federal bodies (Art. 23 para. 2 aDSG), has been deleted without replacement. The reason for this is that the version of the FADP commented on here already provides for the same supervisory system for private persons and federal bodies. 2

B. Purpose of the Norm and Background

The FADP is designed as a uniform law and regulates data processing by private persons and by federal bodies in only one decree. As part of the public sector, federal bodies are generally subject to stricter legal requirements, 3

which also applies to the processing of personal data and data protection obligations (see Art. 5 lit. i FADP).

4 Art. 40 FADP breaks this dichotomy. The provision stipulates that federal bodies acting under private law are subject to the less strict data protection provisions for private individuals (in particular Chapter 5 FADP). The provision is intended to ensure that federal bodies do not experience any disadvantages compared to private competitors when participating in economic competition. The legislator is thus addressing the fact that federal bodies, as subjects of private law, do not exercise sovereignty and that there is sometimes no relationship of subordination vis-à-vis private parties that could be compensated for by a stricter legal dress.

5 Art. 40 FADP is to a certain extent the counterpart to Art. 5 lit. i FADP, according to which private individuals who perform public duties are subject to the stricter provisions for federal bodies (cf. the commentary on Art. 5 lit. i FADP).

C. Genesis

6 The Federal Council's draft of the first Federal Data Protection Act of 1988 already provided for private-law activities by federal bodies to be subject to the provisions for private individuals. This principle is still valid and unchanged.

7 In the parliamentary deliberations on the 1988 draft, the Council of States argued that federal bodies should remain subject to the provisions for federal bodies even when acting under private law. This was subject to the proviso that the Federal Council be granted the authority to regulate exceptional situations. The Council of States was concerned that less restrictive data protection provisions should not make it unnecessarily attractive for the public sector to act under private law. And it should be ensured that private-law action by federal bodies - should it occur in exceptional cases - is based on a legal foundation. After the National Council supported the Federal Council's draft, the Council of States finally agreed to it. However, it imposed the condition that the requirements for the legal basis of federal bodies acting under private law be tightened.

8 The original version of the FADP 1988 stipulated that the supervision of federal bodies would not be relaxed in the area of private-law activities. Thus, the same supervisory possibilities were to remain in place. In the version

commented on here, however, this provision (Art. 23 para. 2 aDSG) was deleted without replacement. The reason for this is the standardization of the supervisory regime for private and federal bodies.

II. SCOPE OF APPLICATION

Art. 40 FADP ties in with the concept of a federal body. According to Art. 5 lit. i FADP, federal bodies are authorities and departments of the Confederation as well as private persons entrusted with public duties (for details, see the commentary on Art. 5 lit. i FADP). 9

In principle, the provisions specific to federal bodies are applicable to them (esp. Chapter 6 FADP). However, in the event that a federal body acts in a private capacity, it is subject to the provisions for private individuals pursuant to Art. 40 FADP (esp. Chapter 5 FADP). 10

III. SOVEREIGN AND PRIVATE-LAW ACTION BY THE STATE

A. Categorization of State Action

As diverse as the manifestations of state action itself are, so are the views on how state action should be subdivided and categorized. In the context of Art. 40 FADP, the division into "sovereign action" and "private action" is relevant because the provision conditions private action. The pair of terms acts as a counterpart to each other and describes the form of state action, not its object and content. 11

B. Sovereign Action as a Principle

In principle, the state acts in a sovereign manner in the performance of its duties. Sovereign action includes the power to unilaterally determine the rights and obligations of private parties and is accompanied by a superiority of the state over private parties (subordination relationship). An example of sovereign action is the issuance of decrees in return for the conclusion of contracts under private law. 12

The state acts in a sovereign manner, for example, in the area of intervention administration. This involves interfering with the rights and freedoms of private individuals, who must tolerate this. It directly serves the fulfillment of 13

public tasks. Examples include expropriation or police restrictions on land ownership. The state also acts in a sovereign manner in parts of the administration of services, i.e. when state services of an economic and social nature are provided to private individuals (e.g. the provision of state social security). It also directly serves the fulfillment of public tasks.

C. Private Law Action

1. Basic principles

14 It is undisputed that the public sector can also act under private law in certain constellations. However, whether there is room for the state to act under private law must be determined on a case-by-case basis. The starting point is that the state is always bound by the principle of legality in its actions (cf. Art. 5 para. 1 FC). In principle, it therefore has no autonomy in shaping its legal relations. If an area of law is conclusively regulated by public law, there is thus no room for maneuver for action under private law. This is only possible under the following conditions:

- There is no conclusive regulation under public law.
- Private law action is the appropriate form of action for the respective area of responsibility.

15 In the context of Art. 40 FADP, action under private law by a federal body is also decisive. Private-law action is characterized, as described, by the fact that no public-law norm applies to an activity, no subordination relationship exists as a result and the state and third parties deal on the same level (e.g. conclusion of a contract under private law). The existence of a competitive relationship with private parties, on the other hand, is not necessary under Art. 40 FADP.

16 In the area of data protection law, the legal nature of the basic relationship with the data subject is taken into account for the demarcation between private and public law actions. This distinction is often not trivial. The pluralism of methods can serve as an aid (see infra n. 18). In addition, certain case constellations have developed in which the state normally acts under private law (see infra n. 21 ff.).

2. Delimitation in accordance with methodological pluralism

In accordance with the principle of legality, in order to assign the basic relationship between the person concerned and the public body to public or private law, it must first be examined whether a solution exists under special law to regulate this question (see supra n. 14). 17

If this is not the case or if the interpretation of the regulation leaves doubts, the delimitation criteria developed in doctrine and practice can be consulted. According to this pluralism of methods, the following points are examined: 18

- Interest theory: Does the legal relationship predominantly serve the pursuit of private or public interests?
- Subordination theory: Does the acting state institution act in a sovereign and thus superior manner vis-à-vis the private parties?
- Functional theory: Does the legal relationship have as its object the fulfillment of a public task?
- Modal theory: Is a violation sanctioned by civil or public law?

According to practice, it must be examined separately for each individual case which theory is best suited for the delimitation. According to case law of the highest courts, for example, the functional theory is considered the most suitable for assessing the legal nature of contracts. 19

3. Cases of permissible private law action

In practice, certain areas of activity have emerged in which the public authority normally (permissibly) acts under private law. 20

In the case of administrative support activities (also known as demand management), the public authority procures the necessary material and personnel resources that it needs for the direct fulfillment of public tasks. The administrative support activity serves only indirectly to perform public tasks. For the implementation of these tasks, the public authority concludes contracts under private law. 21

The financial assets of the general government include all realizable assets. They serve the public authority only indirectly for the realization of the public task and in its management it acts under private law. Examples are the leasing 22

of real estate on the open market or trading in securities for investment purposes.

23 If the public sector acts under private law, it participates in economic life and is in a competitive relationship with the private sector. In the external relationship, i.e. in interaction with the competition, the public authority acts under private law. Examples are the operation of a municipal restaurant or certain business areas of the cantonal banks.

24 In the case of service administration, the public authority provides economic services for private individuals. It acts under private law if the provision of services only indirectly serves the pursuit of public interests, as in the case of transport contracts for public transport or contracts for the supply of energy. On the other hand, it acts in a sovereign manner when it provides IV pensions.

IV. LEGAL CONSEQUENCES

A. Applicable data protection provisions

25 If the matter concerns an area of permissible action under private law by the state, the data protection provisions for private individuals apply to federal bodies (Art. 40 FADP). Specifically, this means that in addition to the general provisions (Chapter 2), the special provisions for private individuals (Chapter 5) apply.

26 Federal bodies acting under private law are thus bound by less strict provisions. This is characterized, for example, by the lack of application of Art. 34 FADP, which requires the existence of a legal basis for data processing by federal bodies. A further consequence is the applicability of the mechanism under Art. 31 f. FADP, according to which certain violations of privacy can be cured by suitable grounds for justification (legal basis, overriding private or public interest, consent).

27 However, even within the framework of Art. 40 FADP, there is no complete decoupling from the legal regime for federal bodies. Certain constitutional principles must also be observed by federal bodies acting under private law (cf. infra n. 31 ff.).

B. Procedural

The provisions of private law also apply to the enforcement of rights if Art. 40 FADP is applicable. If a data subject wishes to take legal action to enforce data subject rights or other claims against a federal body acting under private law, the provisions of Chapter 5 of the FADP apply. 28

In the case of legal proceedings, the civil courts have jurisdiction in the action. The procedure is governed by the Code of Civil Procedure. 29

C. Further applicability of public law

1. Constitutional principles

Despite the application of Art. 40 FADP, the commitment to constitutional principles (see Art. 5 FC) may not be lightly abandoned. In the case of private-law actions by federal bodies, it must always be examined whether they comply with these overriding principles. 30

First and foremost, attention must be paid to the principle of legality (Art. 5 para. 1 FC). This fulfills both a democratic and a constitutional function. Under the private law regime of the FADP, the lawful implementation of the principle of transparency, the duty to inform or the obtaining of consent can compensate for the rule of law function in certain cases. The democratic function, on the other hand, cannot be replaced by the aforementioned obligations (cf. also Art. 34 of this Commentary, in particular the excursus on consent). 31

2. Commitment to fundamental rights

In the area of fundamental rights, too, there is no need for a complete alignment with private parties if the state acts under private law in accordance with Art. 40 FADP. The community as well as private individuals who perform public duties are always bound by fundamental rights in their actions and must contribute to their realization. After this principle was initially the subject of supreme court rulings, it was expressly laid down in the Federal Constitution of 1999 in Art. 35 para. 2 FC. For the fundamental rights obligation, it is also not private or sovereign action that is decisive, but - more broadly - whether a public task is performed (Art. 35 para. 2 FC speaks of "state task"). 32

3. Two-Tier Theory in the Submission Procedure

33 In order to distinguish between private and sovereign action, the two-stage theory is sometimes used in the submission procedure. It states that the award (formation of will) is made by means of a decree and is thus of a public-law nature, while the contract with the successful tenderer is of a private-law nature.

34 However, the two-stage theory has not been recognized by the supreme court case law. In any case, delimitation difficulties also arise in the context of data protection law: In light of Art. 40 FADP, application of the two-tier theory would mean that data processing up to and after the award would be subject to different legal regimes. However, such a strict separation of data processing entails considerable (technical) difficulties in practice.

35 In the sense of a solution that is not only pragmatic, but also constitutionally justifiable, it must therefore be assumed that the more restrictive data protection provisions for federal bodies will be applied globally to tender procedures. In this area, too, the state acting under private law must not be treated lightly and entirely on an equal footing with private parties.

V. CASUISTRY

36 The "SwissPass" ruling of the Federal Administrative Court provides an example of the procedure described above for examining the existence of private-sector action under Art. 40 FADP. In this case, the court had to assess whether the issuance of a SwissPass and the related data processing by SBB were subject to public or private law.

37 First of all, the special legal regulation for the area of passenger transport is relevant, according to which transport companies - irrespective of their legal form - are subject to the provisions for federal bodies for licensed and authorized activities and, in the case of private-law activities, to those for private persons (Art. 54 PBG). It follows that transport companies can also act under private law in the licensed area and must comply with the data protection regulations for private individuals.

38 According to the Federal Administrative Court, the issuance of the SwissPass does not directly serve the purpose of concessionary passenger transport, since it can also be issued without public transport services. However, since

the SwissPass is an aid for the conclusion of a passenger transport contract, the court nevertheless took into account its legal nature. Applying the pluralism of methods and, in particular, the theory of functions, the court qualified the passenger transport contract as civil law and deduced from this that SBB was subject to the data protection regulations for private individuals when issuing the SwissPass.

As a result, the judgment is correct and private-law action by SBB appears to be permitted and relevant in the specific case. Two points should then be noted: 39

- On the one hand, the court also included in its considerations the "fulfillment of a public task" as a criterion, which has no place in a strict interpretation of Art. 40 FADP. According to the wording, the norm is based solely on the legal form of the action. The two concepts of "public task" and "private-law or sovereign action" must be separated as a matter of principle.
- Despite this principle, it is argued here that a pure focus on the legal nature of the basic relationship between the person concerned and the public body can lead to a circumvention of overriding public law standards. The actions and, in the present context, the processing of personal data by federal bodies may not be measured solely by their choice of form of action. The action must be placed in a larger, constitutional context. Thus, Art. 40 FADP is not applicable at all if it does not concern a federal body, including private parties performing public tasks. In the present opinion, the Federal Administrative Court's assessment of the transport contract on the basis of the pluralism of methods and, sometimes, the theory of functions is therefore consistent and prevents any circumvention of principles of public law.

BIBLIOGRAPHY

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.

MATERIALS

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).

COMMENTARY ON

Art. 41 FADP

A commentary by Sarah Bischof

SUGGESTED CITATION

Sarah Bischof, Commentary to art. 41 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Bischof, art. 41 FADP N. XXX.

Art. 41 Rights and procedures

[1] Any person who has a legitimate interest may request the responsible federal body to:

a. stop the unlawful processing of the personal data concerned;

b. redress the consequences of unlawful processing;

c. declare the processing to be unlawful.

[2] The applicant may in particular request the federal body to:

a. correct, delete or destroy the personal data concerned;

b. communicate its decision, in particular about correcting, deleting or destroying personal data, the objection against the disclosure under

Article 37 or marking data as disputed under paragraph 4, to third parties or publish the decision.

[3] Instead of deleting or destroying the personal data, the federal body shall restrict the processing if:

a. the data subject disputes the accuracy of the personal data and neither its accuracy nor its inaccuracy can be established;

b. the overriding interests of third parties so require;

c. an overriding public interest, in particular Switzerland's internal or external security, so requires;

d. deleting or destroying the data may jeopardise an enquiry, an investigation or an administrative or judicial procedure.

[4] If neither the accuracy nor the inaccuracy of the relevant personal data can be established, the federal body shall mark the data as being disputed.

[5] The correction, deletion or destruction of personal data may not be requested in connection with the stocks held by publicly accessible libraries, education and training institutions, museums, archives or other public memory institutions. If the applicant credibly shows an overriding interest, he or she may request the institution to restrict access to the disputed data. Paragraphs 3 and 4 do not apply.

[6] The procedure is governed by the APA. The exceptions in Articles 2 and 3 APA do not apply.

CONTENT

IN A NUTSHELL

If a person is of the opinion that a federal body is violating the applicable provisions of the FADP when processing personal data, Art. 41 FADP (together with the right to information pursuant to Art. 25 FADP) provides them with the necessary rights to enforce lawful data processing against the responsible federal body. In particular, it can demand that the federal body **refrain** from unlawful data processing, **remedy** the consequences of unlawful processing or **establish** the unlawfulness of the processing (Art. 41 para. 1 FADP). The article provides for exceptions, such as in particular the restriction of processing (Art. 41 para. 3 FADP). The decision of the federal body to refuse or grant or reject these claims is issued in the form of an order, which in turn, if the necessary requirements are met, can be contested in accordance with the rules of general federal administration of justice.

I. GENERAL

A. Preliminary remarks

1 If a federal body processes personal data, this constitutes an interference with the fundamental right of informational self-determination of the person concerned in accordance with Art. 13 para. 2 FC and Art. 8 ECHR. For this reason, federal authorities may only process personal data to a limited extent in compliance with the processing principles pursuant to Art. 6 FADP and in particular Art. 34 et seq. FADP at all. In particular, they require a legal basis for this.

2 Data processing by a federal authority generally constitutes real acts. Art. 41 FADP grants the data subject (and possibly also third parties, see N. 8) a number of claims by means of which they can demand that the lawfulness of data processing be restored or that the unlawfulness at least be established. At least in the case of a (partially) dismissive decision, the data subject thus obtains a contestable order.

3 The individual legal protection under Art. 41 FADP, which only comes into effect in the event of an active claim by the data subject, must be distinguished from the supervisory rights of the Federal Data Protection and Information Commissioner (see the comments on Art. 49 et seq. FADP). Within the scope

of his supervisory powers, the FDPIC is authorized to conduct ex officio investigations and issue rulings, which also protects persons who cannot or do not wish to take legal action against an errant federal body (e.g. because they have no knowledge of the unlawfulness or of the data processing itself).

B. History of origin

According to the Federal Council's dispatch on the original FADP of 1992, the proposed legal system was to be based on the private-law actions of Art. 28a CC, but was also to be integrated into the administrative procedural law in force at the time. The Councils did not subsequently question this concept proposed by the Federal Council and only made a few changes. 4

The provision underwent some changes as a result of the revision, which came into force on September 1, 2023. In particular, an explicit right to erasure and the restriction of processing were included. These amendments and additions proposed by the Federal Council were adopted by the Councils without further ado. 5

II. CLAIM AND PROCEDURAL REQUIREMENTS

The addressee of the claim is the responsible **federal body** that processes the data or has it processed in order to fulfill its legal mandate. Not only the federal authorities are deemed to be a federal body, but also private individuals who perform public-law tasks for the Confederation (see explanations on Art. 5 lit. i FADP). This means, for example, that claims arising from unlawful data processing against a pension fund, which is organized as a foundation under private law but offers mandatory occupational pension provision in accordance with the BVG and is therefore considered a federal body, must be asserted in accordance with Art. 41 FADP (and not Art. 32 FADP). 6

It should be noted that the enforcement of a claim against a federal body has no binding effect on other federal bodies (see N. 21 on notification to third parties or publication); they must therefore be enforced individually against each responsible federal body that processes data. 7

Any person who has an **interest worthy of protection** is entitled to make a claim. Whether such an interest exists is assessed in accordance with the general principles of administrative procedure. The interest worthy of protection is also not limited to personal interests and does not have to coincide with the 8

interest protected by the infringed norm. The only requirement is that the applicant has a current legal or factual interest in the outcome of the proceedings he has initiated and that this can bring him a direct, practical benefit. They must have a special relationship to the subject matter of the dispute and therefore be more affected than the general public.

9 In the case of the person concerned, an interest worthy of protection will generally be given. However, exceptions are possible, e.g. if the federal body no longer processes the data at all, which would render the request irrelevant. In a few constellations, it is also conceivable that third parties whose data is not processed at all can demonstrate an interest worthy of protection. However, this is usually only the case if such a third party is a close relative or friend of the (deceased) person concerned and can invoke the protection of memory recognized by the Federal Supreme Court.

III. THE REQUESTS

A. Prerequisite of unlawfulness

10 Pursuant to Art. 41 para. 1 FADP, the applicant may request the **omission of** unlawful data processing, the **elimination of the consequences** of unlawful data processing or the **determination** of the unlawfulness of data processing.

11 What these claims have in common is that they presuppose that the data processing is **unlawful** . This is in contrast to the objection to the disclosure of personal data under Art. 37 FADP; here, only an interest of the data subject worthy of protection is decisive, but not the unlawfulness of the disclosure (see the commentary on Art. 37 FADP).

12 Unlawfulness may consist, among other things, in the fact that the federal body **does not have a sufficient legal basis** for the corresponding data processing. For example, the Federal Administrative Court ruled that a pension fund that sends unsealed pension certificates directly to the employer is acting unlawfully because such disclosure is not necessary for the implementation of occupational pension provision in accordance with the BVG and no other legal basis (in particular Art. 86a BVG, which regulates the disclosure of data within the framework of the BVG) would legitimize this. In addition, the **processing of incorrect data** is also unlawful if the responsible federal body

does not comply with its duty of verification in this regard (see commentary on Art. 6 para. 5 FADP).

B. Right to injunctive relief (para. 1 lit. a and para. 2 lit. a)

1. General

The claim for injunctive relief requires that at the time of assertion there is a **serious fear** that the responsible federal body will carry out certain unlawful data processing in the near future. Such a serious fear may exist if the federal body is already processing the data and this is continuing, or if there are concrete indications that the data will be processed unlawfully in a certain way in the near future. Only then, according to the case law of the Federal Supreme Court, can the current legal interest in injunctive relief be affirmed. 13

If these conditions are met, however, the data subject can not only demand that the federal body refrain from unlawful data processing. Rather, they can also request the **restoration of lawfulness**, in particular by requesting rectification, erasure or destruction of the data concerned on the basis of Art. 41 para. 2 lit. a FADP. 14

2. Rectification and confirmation (para. 4)

The processing of inaccurate personal data is only unlawful if the inaccuracy is due to a **breach of the duty of verification** pursuant to Art. 6 para. 5 FADP. A federal body processing data must therefore take appropriate measures ex officio to ensure the accuracy of the data at the time the data is collected or during the processing period (see commentary on Art. 6 para. 5 FADP). Even if it does so, data processing becomes unlawful at least at the moment the data subject approaches the federal body with a claim for rectification and the latter fails to sufficiently clarify the accuracy or inaccuracy again. 15

If the accuracy or inaccuracy of the data cannot be established or cannot be established without further ado despite the data subject's substantiated request for rectification, the federal body must restrict processing in accordance with Art. 41 para. 3 FADP for the duration of the necessary clarifications (see letter E below). This means that the federal body may only process the data during this period in order to establish its accuracy or inaccuracy. 16

17 If it is not possible for the federal body to prove the accuracy of the processed data, possibly despite further clarifications, but the data subject is also unable to prove the accuracy of the corrections he or she has requested, the federal body must attach a **note of dispute**. On the one hand, this serves the interests of the person concerned by demonstrating that they do not agree with the federal body's presentation of the facts. On the other hand, it ensures that the federal body does not have to refrain from processing data that it needs to fulfill its legal mandate.

18 The legislative materials on the new restriction introduced with the 2023 revision do not comment on the relationship between Art. 41 para. 3 and para. 4 FADP. However, as explained above, one of the purposes of the confirmation notice is to ensure that the federal body can continue to perform its statutory duties. If a clarification of the accuracy or inaccuracy of the data is unsuccessful, it must be possible for the federal body to lift a restriction on processing made for this purpose in accordance with Art. 41 para. 3 FADP, to attach a note of dispute and to process the data in question in full again, at least if it is not possible to completely refrain from processing and no other reason for restriction (see letter E) applies.

C. Right to erasure (para. 1 lit. b)

19 The data subject also has the right to have **the consequences** of unlawful data processing eliminated by means of suitable and proportionate measures. This relates to the actual elimination of adverse consequences that are attributable to unlawful data processing, for example the subsequent granting of statutory benefits. If a health insurance company in the area of compulsory health insurance (OKP) were to use a health questionnaire to clarify the general state of health of an insured person and not offer them certain OKP benefits based on this, there would be no legal basis for this (and it would contradict the obligation to accept data under the KVG); the data collection would be unlawful and the health insurance company would have to grant the insured person the benefits under health insurance law.

20 However, the entitlement does not allow the persons concerned to remove formally legally binding decrees. This is still only possible with the statutory grounds for revision in accordance with Art. 66 APA. It is also not possible for data subjects to claim compensation or satisfaction based on Art. 41 para. 1 lit. b FADP, as these claims must be asserted via the Federal Liability Act.

In practice, the claim for removal will regularly play a role in the event of unlawful data disclosure. In this case, the data subject can request, among other things, the publication of the decision on the unlawful data processing (namely on the rectification, erasure or destruction, the notice of objection but also on the objection to the disclosure pursuant to Art. 37 FADP) or its notification to any data recipients (Art. 41 para. 2 lit. b FADP). The purpose of this is that a data recipient can voluntarily accept the decision and delete or correct the data, but cannot be forced to do so. In this case, the data subject still has no choice but to assert any claims against the data recipient. 21

D. Right to a declaratory judgment (para. 1 lit. c)

The applicant may also request a declaration that the data processing **is unlawful**. This claim **is** only **subsidiary** to the claim for injunctive relief and removal. As long as it is possible to demand the cessation of unlawful processing or the elimination of the associated consequences, there is no legitimate interest in the determination of unlawfulness. 22

According to the case law of the Federal Supreme Court, there is an interest in a declaratory judgment if (past) unlawful data processing or the associated violation of personality rights continues to have a disruptive effect and the determination of unlawfulness is suitable for eliminating this ongoing effect. 23

E. Restriction of processing (para. 3)

With the revision of 2023, Art. 41 para. 3 FADP was newly inserted. According to this, instead of deleting or destroying the data, the federal body must restrict processing if one of the following cases applies 24

- The data subject disputes the accuracy of the personal data, but neither the accuracy nor the inaccuracy can be established (see n. 18 above);
- Overriding interests of third parties or overriding public interests require that the data continue to exist;
- the deletion or destruction of the data would jeopardize an investigation, an inquiry or official or judicial proceedings.

It should be noted that Art. 18 DSGVO also provides for the "restriction of processing". In contrast to the provision of the FADP, where it is a claim of the data subject against the controller, Art. 41 para. 3 FADP is designed as an ex- 25

ception to erasure/destruction or rectification. When processing a request for erasure/destruction, but also for rectification (although not explicitly mentioned, the restriction of processing to check the accuracy or inaccuracy of the data makes sense from a legal point of view), the federal body must check ex officio whether one of the reasons for a restriction exists. If the request is granted and the restriction is affirmed, the federal body must reduce the processing to the purpose that conflicts with the erasure/destruction or rectification.

26 The decision on the restriction must be issued as an order or as an interim order if the proceedings are not concluded as a result.

27 The dispatch stipulates that the restriction must be implemented in such a way that the disputed data must be clearly marked, which in practice could mean that it is temporarily moved to another processing system or that access rights are restricted. In this argument, the legislator has not taken into account the fact that this will regularly lead to implementation problems in practice, as it cannot be assumed that all systems enable such precautions for individual data, i.e. "field-based", so to speak, and cannot be implemented without further ado. If the technical implementation options are not available, the restriction must at least be ensured with organizational measures, e.g. by means of instructions in the system, directives or separate lists.

IV. EXEMPTION PROVISION (PARA. 5)

28 The rectification, erasure or destruction of personal data cannot be requested in relation to the holdings of so-called public repositories, such as in particular publicly accessible libraries, educational institutions, museums or archives. In these constellations, it is also not possible to issue a notice of dispute. The purpose of these institutions is to depict a moment in the past, which can only be achieved if the holdings are faithful to the original and unchanged.

29 However, the data subject can at least request that access to disputed data be restricted. In principle, the public interest in free and unaltered access to documents takes precedence. However, an overriding interest of the person concerned in restricting access is to be assumed if he or she would suffer considerable personal disadvantages as a result of free access, for example because his or her professional advancement would be restricted and the archival value of the data in question appears to be lower in comparison. According to

the dispatch, this exception must be taken into account in particular with regard to the increasing publication of archive records on the Internet.

V. ADMINISTRATIVE PROCEDURAL LAW (PARA. 6)

The procedure for asserting claims under Art. 41 para. 1-2 FADP is governed by the APA. This applies even if the APA does not actually apply to the respective subject area (the exceptions in Art. 2 and 3 of the APA do not apply). 30

This means in particular that the federal body must clarify the facts of the case ex officio (principle of investigation, Art. 12 APA). However, the applicant is subject to a duty to cooperate (Art. 13 APA); for example, as part of an application for rectification, the applicant must submit evidence that proves the correctness of the changes requested. 31

The federal body can also decide to reject, approve or reject the application. The decision is issued in the form of a ruling, which in turn can be appealed to the Federal Administrative Court. 32

BIBLIOGRAPHY

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.

MATERIALS

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).

COMMENTARY ON

Art. 42 FADP

A commentary by Sarah Bischof

SUGGESTED CITATION

Sarah Bischof, Commentary to art. 42 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Bischof, art. 42 FADP N. XXX.

Art. 42 Procedure for disclosing official documents that contain personal data

Where proceedings relating to access to official documents that contain personal data in accordance with the Freedom of Information Act of 17 December 2004 are pending, the data subject may claim those rights in the proceedings that they would have under Article 41 of this Act in relation to the documents that are the subject matter of the access proceedings.

CONTENT

IN A NUTSHELL

According to Art. 42 FADP, the claims under Art. 41 FADP can be asserted in the context of an access procedure under the Public Access Act, provided that the documents in question contain personal data. The provision thus takes account of the fact that the protective purposes of the FADP and the FoIA, namely informational self-determination as part of the protection of privacy on the one hand and the principle of transparency of the administration on the other, can be in tension.

I. PRELIMINARY REMARKS

The former Art. 25bis aDSG was introduced with the entry into force of the Federal Act on the Publicity of the Administration (Publicity Act, FoIA). This established the principles of coordination between the FADP and the FoIA. In the revised version of the FADP of 2023, the content of the provision was not changed; it can now be found in Art. 42 FADP. 1

The provision ensures that a data subject can assert their data protection claims as part of the access procedure under the Public Access Act. This means that the access procedure is extended to include these data protection issues. 2

II. ASSERTION OF CLAIMS PURSUANT TO ART. 41 FADP IN THE ACCESS PROCEDURE

The FoIA provides that every person has the right to inspect official documents and to obtain information from the authorities about the content of official documents (**principle of public access**, Art. 6 para. 1 FoIA). However, access may be restricted, postponed or denied if the granting of access may adversely affect the privacy of third parties, provided that the public interest in access does not outweigh this (Art. 7 para. 2 FoIA). 3

In order to protect the privacy of third parties in the access procedure, official documents containing personal data must in principle be **anonymized** (Art. 9 FoIA). However, if anonymization is not possible, for example because the content and context of the official document would no longer be comprehensible or because it would involve a disproportionate effort (which requires a 4

comprehensive weighing of interests by the federal body), access may only be granted under the condition of Art. 36 FADP, which regulates the disclosure of data by federal bodies (see commentary). If the authority is considering granting access, it must first give the data subject whose personal data is contained in the documents in question and whose privacy may be affected by this the **opportunity to comment** within 10 days. As part of this statement, the data subject may not only request that their data not be disclosed to the applicant. Rather, Art. 42 FADP allows them to assert their claim for the **omission of** unlawful data processing, the **elimination** of the consequences of unlawful data processing or the **determination of** the unlawfulness of data processing (see commentary on Art. 41 FADP). The claims must relate to the documents that are the subject of the access procedure.

5 If the authority wishes to grant access contrary to the opinion of the data subject, it must inform the data subject accordingly (Art. 11 para. 2 FoIA). The data subject may then request **mediation** from the FDPIC within 20 days. If the mediation fails, the FDPIC will issue a recommendation. The authority must then issue an order if it either does not follow the recommendation or if the person concerned (or the applicant) requests such an order (Art. 15 para. 1 and para. 2 lit. b FoIA). An appeal against this decision may be lodged with the Federal Administrative Court (Art. 16 para. 1 FoIA).

6 Art. 42 FADP is thus intended, among other things, to ensure procedural economy, as the person concerned may only become aware that their personal data is contained in the official documents in question when they are invited to comment. Accordingly, it may make sense for the data protection aspects to be assessed as part of the access procedure. One criticism of this solution is that it makes the access procedure cumbersome and lengthy.

BIBLIOGRAPHY

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.

MATERIALS

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).

COMMENTARY ON

Art. 43 FADP

A commentary by Carl Jauslin / Danielle Schneider

SUGGESTED CITATION

Carl Jauslin/Danielle Schneider, Kommentierung zu Art. 43 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Jauslin/Schneider, N. XXX zu Art. 43 DSG.

Chapter 7 Federal Data Protection and Information Commissioner

Section 1 Organisation

Art. 43 Election and status

[1] The United Federal Assembly shall elect the head of the FDPIC (the Commissioner).

[2] Any person with the right to vote on federal matters is eligible for election.

[3] The Commissioner‘s employment relationship is governed, unless this Act provides otherwise, by the Federal Personnel Act of 24 March 2000[12] (FPA). The Commissioner shall be insured against the financial consequences of retirement, invalidity and death with PUBLICA, the

Federal Pension Fund. If the Commissioner remains in the position after reaching the age of 65 and so requests, pension cover shall be extended until the end of the employment contract, but no later than the end of the year in which the Commissioner attains the age of 68. The FDPIC shall finance the employer's contributions.[13]

[3bis] The Federal Assembly shall issue the implementing provisions relating to the Commissioner's employment contract in an ordinance.[14]

[4] The Commissioner shall exercise his or her duties independently, without seeking or accepting instructions from any authority or third party. He or she is assigned for administrative purposes to the Federal Chancellery.

[5] He or she shall have a permanent secretariat and his or her own budget. He or she shall appoint his or her staff.

[6] He or she is is not subject to the system of assessment under Article 4 paragraph 3 FPA.

CONTENT

IN A NUTSHELL

The election and position of the head of the FDPIC (the Commissioner) is crucial for the independence and legitimacy of the supervisory activity. The Commissioner is elected by the United Federal Assembly and exercises his or her function independently: The commissioner does not accept instructions, is not subject to the evaluation system in the BPG, and is only administratively assigned to the Federal Chancellery. He or she has a permanent secretariat and his or her own budget.

The election and removal from office of the appointee is the responsibility of the United Federal Assembly. The Judicial Commission is responsible for other employer decisions concerning the appointee. Federal personnel law applies to the employment relationship of the Commissioner only insofar as the FADP and its implementing provisions do not provide otherwise.

I. GENERAL

1 Art. 43 governs the election and position of the head of the FDPIC, who supervises the application of federal data protection regulations (Art. 4 para. 1 FADP).

2 Terminologically, the head of the FDPIC as a person must be distinguished from the FDPIC as an authority: If the person in question is the head of the Federal Data Protection and Information Commissioner, the term "the Commissioner" is used; if, on the other hand, the authority of the Federal Data Protection and Information Commissioner in the institutional sense is meant, the abbreviation "FDPIC" is used. In terms of personnel, the institution FDPIC includes not only the Commissioner but also, in particular, the Secretariat.

3 Whereas under the previous law the Commissioner was elected by the Federal Council and the election had to be approved by the United Federal Assembly (Art. 26 para. 1 aDSG), under the current law the United Federal Assembly is responsible for electing the Commissioner (Art. 43 para. 1 FADP). Election by the United Federal Assembly is intended to strengthen the independence of the Commissioner and his or her democratic legitimacy.

4 The focus of this provision on election and position is to guarantee the independence of the Commissioner as a person and of the FDPIC as an authority.

The concept of independence includes institutional independence, functional independence and substantive independence.

- Institutional independence means that the FDPIC is not organizationally subordinate to any other authority. However, this does not exclude an administrative assignment, as in the case of the FDPIC to the Federal Chancellery (BK) (see Art. 43 para. 4 second sentence FADP).
- Functional independence requires that the FDPIC exercise his or her duties and powers independently, without receiving instructions from any body (see Art. 43 para. 4 first sentence FADP) and that the appointee is not subject to any system of evaluation pursuant to Art. 4 para. 3 BPG (see Art. 43 para. 6 FADP). The functional independence of the FDPIC is also ensured by the fact that the Commissioner is employed on a 100% basis (Art. 8 of the Ordinance on the Employment Relationship of the Commissioner), secondary employment is only possible to a very limited extent (Art. 46 and 47 FADP) and the Commissioner can only be removed from office in very restrictive exceptional cases (Art. 44 para. 3 FADP).
- Material independence requires that the conditions and framework be created so that the FDPIC can exercise his or her duties and powers independently, i.e. not only on paper, but also actually have the possibility to fulfill his or her legal mandate independently. This material independence includes, in particular, that the FDPIC has a permanent secretariat and budget and is allowed to hire its staff independently (see Art. 43 para. 5 FADP).

The revision of this provision on the election, position and employment relationship of the Commissioner took place in three steps: 5

- In a first step, Parliament strengthened the independence of the FDPIC by adopting the Federal Law of September 28, 2018, on the implementation of EU Directive 2016/680, which is part of the further development of the Schengen acquis.
- In a second step, as part of the total revision of the Data Protection Act of September 25, 2020, Parliament further strengthened the independence of the FDPIC and stipulated that the Commissioner will now be elected by the United Federal Assembly. The change in the electoral body was only introduced during the parliamentary debate, contrary to the view of the Federal Council, which stuck to the previous solution. The parliamentary

initiative Leutenegger Oberholzer 16.409 already demanded that the Commissioner be elected by the United Federal Assembly. In the parliamentary debate, the strengthening of the independence and position of the FDPIC and the increased democratic legitimacy were cited to argue for a change in the election procedure in favor of the United Federal Assembly. The Federal Council and the supporters of the previous solution feared a politicization of the election, which could be influenced by various interest groups in parliament, and emphasized that even under the previous solution, the United Federal Assembly must approve the election by the Federal Council and is thus involved.

- In a third step, individual aspects of the employment relationship were specified at the legislative level and the Federal Assembly was given the authority to issue implementing provisions on the employment relationship of the commissioner (Parliamentary Initiative SPK-N 21.443). The amendments to the totally revised FADP associated with the parliamentary initiative SPK-N 21.443 as well as the newly created implementing provisions were adopted on June 17, 2022 and will enter into force at the same time as the total revision of the FADP (Sept. 1, 2023). They resulted in the independence of the commissioner also being reflected in the employment relationship.

6 Art. 43 para. 4 and 5 FADP remain unchanged in relation to the old law (Art. 26 para. 4 and 5 FADP), with Art. 43 para. 5 FADP being supplemented by Art. 45 FADP on the budget process. Art. 43 para. 3 first sentence corresponds to Art. 26 para. 2 FADP and was extended and by three sentences on the pension fund of the commissioner.

7 Art. 43 FADP adheres to the requirements of European law in Art. 15 of the modernized 108+ Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data, Art. 41 et seq. of the Schengen-relevant EU Directive 2016/680 and the standard for effective data protection supervision provided for in Art. 51 et seq. of the EU General Data Protection Regulation 2016/679 in connection with the EU Commission's adequacy decision (Art. 45 para. 2 lit. b EU General Data Protection Regulation).

II. ELECTORAL BODY (PARA. 1).

The United Federal Assembly shall elect the Commissioner. The Judicial Commission is responsible for advertising the position and preparing the election (Art. 40a para. 1 lit. d and para. 2 first sentence ParlA; see also Art. 2 of the Ordinance on the Employment Relationship of the Commissioner). The deputy of the Commissioner is not covered by the provision and is not elected by Parliament. The general provisions of federal personnel law apply to the deputy. 8

Art. 43 para. 1 FADP is based on Art. 168 para. 2 FC, according to which a law may authorize the Federal Assembly to elect persons other than those referred to in Art. 168 para. 1 FC (the members of the Federal Council, the Federal Chancellor, the judges of the Federal Supreme Court and the General). Examples are the Federal Prosecutor and the Deputy Federal Prosecutors as well as the members of the supervisory authority over the Office of the Attorney General (see Arts. 20 and 23 StBOG). 9

European law does not prescribe the procedure for electing the members of the data protection authority (see Art. 43 para. 1 of Directive (EU) 2016/680; also Art. 53 para. 1 of Regulation (EU) 2016/679). According to these legal acts, it is up to the Member States to ensure that the appointment is made in a transparent procedure and to provide for an appointment by the Parliament, the Government, the Head of State or an independent body entrusted with it under the law of the Member State. 10

III. ELIGIBILITY (PARA. 2)

According to para. 2, anyone who is entitled to vote in federal matters is eligible to be elected as a commissioner. Pursuant to Art. 136 para. 1 FC, all Swiss citizens who have reached the age of 18 and who are not incapacitated by reason of mental illness or infirmity are entitled to vote in federal matters. In particular, Swiss citizenship is consequently required for the office of commissioner. 11

This provision on eligibility, which is based on the right to vote, is found by analogy in other federal laws. It corresponds, for example, to Art. 20 para. 1bis StBOG for the election of the Federal Prosecutor and the Deputy Federal 12

Prosecutors or Art. 5 para. 2 VGG for the election of judges of the Federal Administrative Court.

13 Requirements for the factual and personal suitability of the appointee are not explicitly stated in the FADP. However, they are derived from federal personnel law, which remains subsidiarily applicable to the appointee pursuant to Art. 43 para. 3 FADP, namely from the obligation to advertise the position publicly (cf. Art. 7 FADP in conjunction with Art. 22 BPV). Thus, the appointee must be a proven expert in the area of the FADP as well as the FoIA, who has personal integrity. However, the factual and personal suitability is not a prerequisite for eligibility, but is rather the responsibility of the electoral authority. The judicial commission responsible for preparing the election of the appointee shall already take into account the professional and personal suitability when advertising the position. The business audit commissions and the finance delegation shall be obliged to examine the professional and personal suitability of the appointee and to bring their findings to the attention of the court commission (Art. 40a para. 6 ParlA).

14 The appointee is not subject to a personal security check by the federal administration (Art. 29 para. 4 lit. e^{bis} ISG), which means that the examination of security aspects is also the responsibility of the electoral body.

IV. EMPLOYMENT RELATIONSHIP (PARA. 3)

15 The employment relationship of the appointee is governed by the BPG, unless the FADP provides otherwise. Consequently, the BPG applies subsidiarily, in the event that the FADP does not provide for any special provisions. In the FADP, deviating or clarifying provisions can be found in the following places:

- Art. 43 para. 1 and 2 FADP (election).
- Art. 43 para. 3 FADP (pension fund)
- Art. 43 para. 3bis FADP (legal basis for implementing provisions)
- Art. 43 para. 4 first sentence FADP (independence and freedom to issue instructions)
- Art. 43 para. 6 FADP (appraisal system)
- Art. 44 para. 1 and 2 FADP (term of office and termination)
- Art. 44 para. 3 FADP (removal from office)

- Art. 44a FADP (warning)
- Art. 46 FADP (incompatibility)
- Art. 47 FADP (secondary employment)
- Art. 47a FADP (recusal)
- Art. 72 FADP (transitional provision)
- Art. 72a FADP (transitional provision)

Deviations from federal personnel law are necessary in particular if the independence of the appointee or the special election procedure (election by the United Federal Assembly) so requires.

Art. 43 para. 3 then contains, in sentences 2-4, a clarifying provision for the appointee with regard to the occupational benefit scheme. Such a provision is necessary because, according to the SPK-N report, the BPG is not directly applicable here. Art. 43 para. 3 states that the appointee is insured with the Federal Pension Fund PUBLICA against the economic consequences of old age, disability and death until the age of 65. In addition, the appointee has the option of continuing to be insured against the economic consequences of old age until the end of the year in which he or she reaches the age of 68 (cf. also Art. 4 para. 2 of the Ordinance on the Employment Relationship of the Appointee), provided that the employment relationship is continued. This provision corresponds in substance to Art. 8 para. 2 and 3 of the Ordinance of the Federal Assembly of 1 October 2010 on the Employment Relationship and Salary of the Federal Prosecutor and the Deputy Federal Prosecutors (hereinafter: Ordinance on the Employment Relationship of the Federal Prosecutor, SR 173.712.23). The FDPIC finances the employer's savings contributions. 16

V. IMPLEMENTING PROVISIONS ON THE EMPLOYMENT RELATIONSHIP (PARA. 3BIS)

Parliament, and not the Federal Council, is responsible for issuing the implementing provisions on the employment relationship of the Commissioner on the basis of his or her position as electoral body. The fact that the implementing provisions are issued by the electoral body is to be welcomed for reasons of coherence and preservation of independence. Parliament has taken this work in hand as part of the parliamentary initiative SPK-N 21.443 and adopt- 17

ed the "Ordinance on the Employment Relationship of the Head of the Federal Data Protection and Information Commissioner" on 17 June 2020.

18 The Ordinance of the Federal Assembly on the Employment Relationship of the Commissioner is based on Art. 43 para. 3bis FADP. Among other things, it states that

- the most important employer decisions concerning the election of the appointee and the removal from office fall within the competence of the United Federal Assembly (purely declaratory reference in Art. 2 para. 1), while the Judicial Commission is responsible for the other employer decisions (e.g. job advertisement) concerning the appointee (Art. 2 para. 3).
- the employment relationship of the appointee is established by an electoral decree of the Federal Assembly requiring approval (Art. 3 para. 1) and, unlike other magistrates, the appointee does not have to take an oath or a vow of conscientious obedience (Art. 3 para. 4).
- the appointee shall retire from office at the latest at the end of the year in which he or she reaches the age of 68 (Art. 4 para. 2).
- the appointee is classified in salary class 34 in accordance with Article 36 BPV (Art. 5 para. 1) and neither performance bonuses in accordance with Article 49 BPV nor spontaneous bonuses in accordance with Article 49a BPV can be paid (Art. 6 para. 1).
- the appointee is insured for occupational benefits under the Federal Pension Plan (Art. 7).
- the degree of employment of the appointee is 100 percent (Art. 8) and he or she must be domiciled in Switzerland (Art. 9).
- the judicial commission is responsible for the release from official secrecy in accordance with Art. 320 no. 2 StGB (Art. 10).
- a provisional suspension of the commissioner in office is only possible under the conditions of Art. 14 para. 5 VG and the provisions of federal personnel law (Art. 103 and 103a BPV) are excluded (Art. 11)).
- the Judicial Commission may in principle award the appointee compensation amounting to a maximum of one year's salary in the event of termination of the employment relationship if the individual case justifies this (Art. 12; for the exceptions see Art. 12 para. 3 and for the reimbursement obligation see Art. 12 para. 5).

- the data processing of personal data of the appointee within the scope of his or her employment is governed by the Ordinance on the Protection of Personal Data of Federal Personnel (BPDV), subject to the provisions of the Parliamentary Administration Ordinance (ParlVV) (Art. 13).

VI. INDEPENDENCE AND ASSIGNMENT (PARA. 4)

Pursuant to the first sentence of Art. 43 para. 4 FADP, the Commissioner shall exercise his or her function independently, without seeking or accepting instructions from any authority or third party. The freedom from instructions includes two elements: The appointee may neither actively seek nor passively accept instructions. This applies to instructions from other public authorities as well as from private third parties. 19

The FDPIC's freedom from instructions takes into account, in particular, the European law requirements for the independence of the data protection supervisory authority in Article 12bis para. 4 in the modernized 108+ Convention of the Council of Europe and Article 42 paras. 1 and 2 of the Schengen-relevant Directive (EU) 2016/680 as well as Article 52 paras. 1 and 2 of Regulation (EU) 2016/679 in connection with the EU Commission's adequacy decision (cf. Article 45 para. 2 lit. b of the EU General Data Protection Regulation 2016/679). 20

Even after the total revision of the FADP, the Commissioner or Commissioner and the permanent secretariat of the FDPIC constitute a decentralized administrative unit without legal personality (Art. 2 para. 3 GAOA in conjunction with. Art. 8 para. 1 lit. b RVOG in conjunction with. Annex 1 lit. A no. 2.1.1). Administratively, the FDPIC remains assigned to the Federal Chancellery (FC) as an authority (Art. 43 para. 4, second sentence), but is not institutionally subordinate to it. The FDPIC's task is to facilitate and support the FDPIC administratively, without affecting its independence. On the basis of a service agreement, the BK provides the FDPIC with a number of services in the areas of personnel administration, finances and office automation. Examples include the allocation of office space, the provision of appropriate ICT infrastructure and organizational support for the website. Despite its organizational integration into the federal administration, the FDPIC is not to be regarded as an actual administrative authority, but as a sui generis institution. The sui generis status is shaped by the FADP and other decrees. By ensuring the FD- 21

PIC's freedom from instructions, its institutional and functional independence is guaranteed.

22 The institutional and functional independence of the FDPIC, while at the same time being administratively assigned to the BK, is also reflected in the prescribed communication channel. Article 37 para. 1 FDPIC provides that the FDPIC communicates with the Federal Council through the Federal Chancellor. In this context, the Federal Chancellor is obliged to forward the proposals, opinions and reports unchanged to the Federal Council. However, the FDPIC does not submit reports for the attention of the Federal Assembly via the BK, but directly via the parliamentary services (Art. 37 para. 2 FADP).

23 The question arises as to whether there are more suitable solutions under administrative organization law for the FDPIC instead of the administrative assignment to the BK. However, an administrative assignment of the FDPIC to the parliamentary services would appear artificial, since there is no connection whatsoever between the tasks of the FDPIC and those of the parliamentary services. The complete abandonment of an administrative assignment, as is the case for the Federal Supreme Court, for example, would have the consequence that the cooperation between the FDPIC and the federal bodies would no longer be equally close if the Commissioner as a person or the FDPIC as an authority were no longer part of the federal administration.

VII. SECRETARIAT, BUDGET AND PERSONNEL (PARA. 5)

24 Human and financial resources are crucial to the material independence of the FDPIC. Art. 43 para. 5 FADP therefore provides that the Commissioner shall have his or her own budget and a permanent secretariat. The budget process is regulated in Art. 45 FADP.

25 The FDPIC must have sufficient human and IT resources to fulfill his or her legal duties. For this purpose, the secretariat requires, in particular, legal, organizational, (security) technical and communication knowledge. As far as Switzerland's relations with the European Union are concerned, the provision of sufficient resources is also important, and in two respects: it constitutes an important element both with regard to the adequacy decision and with regard to the implementation of the Schengen acquis. Thus, the obligation to provide supervisory authorities with sufficient human, technical and financial resources, premises and infrastructures is enshrined in the European decrees

(Article 12bis para. 5 of 108+ of the modernized Council of Europe Convention, Article 42 para. 4 of EU Directive 2016/680 and Article 52 para. 4 of EU Regulation 2016/679).

Article 43 para. 5, second sentence, FADP provides, as before, that the Commissioner hires his or her own staff and has certain competences in doing so. She or he signs the employment contracts, for example. However, the appointee is still not regarded as an employer under personnel or pension law within the meaning of the BPG for the employees of the Secretariat. According to Art. 3 para. 1 lit. a BPG, the employer is the Federal Council. Whether or not the commissioner is to have employer status in the future is to be clarified at the earliest opportunity at the formal legal level. According to Art. 36 para. 2 FDPIC, therefore, federal personnel law continues to apply to the employment relationship of the employees of the permanent secretariat of the FDPIC. The BPV, the VBPV and the BPDV therefore continue to apply to the employees of the secretariat. 26

VIII. ASSESSMENT (PARA. 6)

The appointee is not subject to the appraisal system under Art. 4 para. 3 BPG. This appraisal system under the BPG forms the basis for performance-related remuneration and goal-oriented development of employees. Since the FDPIC performs his or her function independently and is not subject to any directives, he or she must be exempt from the appraisal system under the BPG. The fact that the performance of the appointee is not evaluated according to the appraisal system of the BPG is therefore the logical consequence of not being bound by instructions and corresponds to the other side of the coin. Those who are not bound by directives cannot be evaluated accordingly without compromising their independence. 27

Instead of performance-related remuneration with bonuses, a performance-independent salary development was provided for the head of the FDPIC according to the model of the Federal Prosecutor. According to Art. 5 para. 3 of the Ordinance on the Employment Relationship, the salary increases on 1 January of each year by three percent of the maximum amount of the salary category until it reaches this maximum amount (cf. Art. 6 para. 3 of the Ordinance on the Employment Relationship of the Federal Prosecutor). 28

29 The FDPIC's duty to report on its activities (Art. 57 FADP) is of central importance against the background of the lack of an evaluation system. In the case of breaches of official duty, there is also the possibility of a warning (Art. 44a FADP). In the event of a serious breach of official duties, removal from office (ultima ratio) (Art. 44 para. 3 FADP) or non-re-election by the Federal Assembly may be considered.

30 The Commissioner and the institution of the FDPIC are not free from any form of supervision. The activities of the FDPIC are subject to judicial review, as its rulings may be appealed all the way to the Federal Supreme Court. In addition, the FDPIC is subject to financial supervision by the Swiss Federal Audit Office (Art. 8 para. 1 lit. a FKG; cf. on Schengen-related requirements: Art. 42 para. 6 of EU Directive 2016/680). The manner of financial control must take into account the independence of the FDPIC. Finally, the FDPIC also remains subject to the supervision of the Federal Assembly (Art. 169 para. 1 FC). According to Art. 8 para. 2 FCA, the federal courts, the Federal Financial Market Supervisory Authority, the Federal Audit Oversight Authority, the supervisory authority over the Office of the Attorney General of Switzerland and the Office of the Attorney General of Switzerland are subject to financial supervision by the Federal Audit Office only to the extent that it serves the exercise of overall supervision by the Federal Assembly. In our opinion, a corresponding addition to Art. 8 para. 2 FKG to include the commissioner is at least worth considering for the purpose of strengthening his or her independence.

The view expressed reflects the personal opinion of the authors and does not bind the Federal Office of Justice.

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 44 FADP

A commentary by Danielle Schneider / Carl Jauslin

SUGGESTED CITATION

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 44 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Schneider/Jauslin, N. XXX zu Art. 44 DSG.

Art. 44 Term of office, re-election and termination of office

[1] The Commissioner‘s term of office amounts to four years and may be extended twice. It begins on the first day of January following the start the National Council‘s legislature period.

[2] The Commissioner may terminate his or her employment contract at the end of any month subject to a period of six months‘ notice. The Judiciary Committee may in an individual case allow the Commissioner a shorter period of notice if there are no substantial interests that preclude this.

[3] The United Federal Assembly may remove the Commissioner from office before the end of the term of office if he or she:

a. has wilfully or through gross negligence committed a serious violation of his or her official duties; or

b. has permanently lost the capacity to carry out his or her official duties.

CONTENT

IN A NUTSHELL

The provisions on the term of office, re-election and termination of the employment relationship are important for the independence of the appointee in various respects. In particular, the limitation of the term of office and the restrictive possibilities for terminating the employment relationship must be mentioned. The United Federal Assembly, and not the Judicial Commission, is declared responsible for any removal from office of the commissioner due to its drastic effects.

I. GENERAL

A. Purpose of the Norm

1 Art. 44 FADP regulates the commencement and term of office (para. 1; n. 6 ff.) as well as the termination of the Commissioner‘s employment (paras. 2 and 3; n. 10 ff.). For the independence of the appointee, the reasons and the procedure for the termination of the employment relationship are of particular importance. In this sense, Art. 44 FADP contributes to independent data protection supervision with the limited term of office of the Commissioner and the restrictive possibilities of removal from office.

B. Background and History

2 The limitation to two terms of re-election (Art. 44 para. 1 first sentence FADP; cf. n. 6) was already introduced during the first stage of the total revision of the FADP (data protection provisions for Schengen cooperation in criminal matters) in Art. 26a para. 1 aDSG. This took into account Art. 44 para. 1 lit. e of the Schengen-relevant Directive (EU) 2016/680. According to this provision, the Schengen states must regulate whether and - if so - how often the members of the data protection supervisory authority can be reappointed. The amendment to Art. 26a para. 1 aDSG entered into force on March 1, 2019.

3 In the second stage of the total revision of the FADP, the United Federal Assembly was designated as the electoral body of the Commissioner (see Art. 43 para. 1 FADP). As a result, the regulations on the term of office, re-election and termination of the term of office also had to be adapted. Among other things, it was specified that the term of office begins on January 1 following

the start of the legislative period of the National Council (Art. 44 para. 1, second sentence FADP; cf. n. 8). In addition, the United Federal Assembly was declared competent to remove the Commissioner from office (Art. 44 para. 3 FADP; cf. n. 18). By contrast, the grounds for removal from office remain materially unchanged compared to the previous law (Art. 26a para. 3 aDSG) (cf. n. 13 ff.).

Finally, as part of the parliamentary initiative SPK-N 21.443, the termination of the employment relationship at the initiative of the Commissioner was revised in Art. 44 para. 2 FADP: Instead of the previous request for dismissal, a (unilateral) right of termination was enshrined (cf. n. 10 f.). 4

The parliament has controversially discussed whether the appointee should receive severance pay upon termination of his or her employment. In the draft of the SPK-N for the implementation of the parliamentary initiative 21.443, a new Art. 44 para. 4 FADP was envisaged, which - in deviation from the provisions of the federal personnel law - expressly excluded a severance payment. The justification for this provision was that the appointee was less politically exposed than other persons elected by the Federal Assembly (such as the Federal Prosecutor) or other high-ranking functions of the federal administration. Furthermore, the potential for conflict in the event of termination of the employment relationship was not so high as to justify severance pay. After the Federal Council, in its statement on parliamentary initiative 21.443, had come out in favor of severance pay in view of the equality of rights and the independence of the appointee, the SPK-N amended its draft decree and proposed severance pay analogous to the regulation for the Federal Public Prosecutor and the Federal Public Prosecutor and the Federal Public Prosecutor. the Federal Prosecutor and the first-instance federal judges (today: Art. 12 of the Ordinance of the Federal Assembly of 17 June 2022 on the Employment Relationship of the Head of the Federal Data Protection and Information Commissioner [hereinafter "Ordinance on the Employment Relationship of the Commissioner"]). The concerns regarding severance pay, on the other hand, should be examined in a general framework (i.e. not only for the Commissioner). The National Council and the Council of States agreed to this solution. 5

II. TERM OF OFFICE AND RE-ELECTION (PARA. 1)

6 According to Art. 44 para. 1, first sentence, FADP, the term of office of the Commissioner is four years and may be renewed twice. The Commissioner may thus remain in office for a maximum of twelve years. According to the Federal Council's dispatch, this limitation on the term of office is intended to strengthen the independence of the commissioner.

7 After the expiry of the four-year term of office, the commissioner must be re-elected by the United Federal Assembly if he or she wishes to continue to exercise the office. In contrast to the previous law (Art. 26a para. 1bis aDSG) and in deviation from Art. 14 para. 2 lit. c BPG, there is no longer a tacit or automatic extension of the term of office. This promotes the democratic legitimacy of the appointee.

8 Article 44 para. 1, second sentence, FADP sets the start of the term of office of the Commissioner at 1 January following the start of the legislative period of the National Council. In this way, the election is transferred to the newly composed parliament in each case. Art. 72 para. 2 FADP provides for a (one-time) exception in the event that, when the Commissioner is elected for the first time by the United Federal Assembly, the previous incumbent is elected. In this constellation, the new term of office of the Commissioner already begins on the day after the election (cf. Art. 72 n. 6 f.).

9 The appointee shall automatically leave office at the latest at the end of the year in which he or she reaches the age of 68 (Art. 4 para. 2 of the Ordinance on the Employment Relationship of the Appointee). By raising the age limit to 68, the Commissioner is treated in the same way as the federal judges and the Federal Prosecutor, who are also elected by the Federal Assembly.

III. TERMINATION OF EMPLOYMENT BY THE COMMISSIONER (PARA. 2)

10 The Commissioner may terminate the employment relationship at the end of any month by giving six months' notice (Art. 44 para. 2, first sentence, FADP). Whereas the previous law only gave him or her the option of requesting dismissal (Art. 26a para. 2 aDSG), the appointee can now unilaterally terminate the employment relationship by giving notice. Thus, an analogous provision to that of the Federal Prosecutor applies to the Commissioner.

The judicial commission may grant the commissioner a shorter notice period in individual cases if no substantial interests are opposed (Art. 44 para. 2 second sentence FADP). In doing so, it shall take into account the circumstances of the specific individual case, such as the transitional period until a new appointee or appointees may take office. A shortened notice period may be considered in particular in the case of health reasons. 11

IV. REMOVAL FROM OFFICE (PARA. 3)

Art. 44 para. 3 FADP regulates the removal from office procedure. In terms of content, the provision corresponds to the previous regulation in Art. 26a para. 3 aDSG (cf. n. 13 ff.). However, it is now the United Federal Assembly, rather than the Federal Council, that is responsible for removing the Commissioner from office (cf. n. 18 ff.). 12

A. Requirements

In view of the high demands on the independence of the Commissioner, removal from office is only permissible in serious cases. The grounds are listed exhaustively in Art. 44 para. 3 FADP: The Commissioner may be removed from office if he or she has seriously violated official duties intentionally or through gross negligence (lit. a; n. 14 et seq.) or has permanently lost the ability to exercise the office (lit. b; n. 17). 13

1. Serious breach of official duties

The main duty of the Commissioner consists in the lawful and diligent performance of the duties assigned by law in the area of data protection and the principle of publicity. This includes, in particular, investigating breaches of data protection regulations (Art. 49 ff. FADP), but also advising private data processors or federal bodies and data subjects (Art. 58 para. 1 lit. a, c and d FADP), as well as numerous other duties, for example in connection with data disclosure abroad (Art. 16 para. 2 FADP), data protection impact assessment (Art. 23 FADP) or reporting breaches of data security (Art. 24 FADP). Other official duties include the duty of confidentiality (Art. 320 SCC, but cf. also Art. 20 para. 2 FoIA), the restriction of secondary employment (Art. 46 and 47 FADP) or the duty of residence (Art. 9 of the Ordinance on the Employment Relationship of the Commissioner). 14

15 Removal from office is not permissible for every breach of official duty. The breach must be serious and committed intentionally or through gross negligence (Art. 44 para. 3 lit. a FADP). In the case of a less serious breach of official duty, a warning by the judicial commission may be considered (cf. Art. 44a FADP).

16 In the doctrine, the obviously unjustified non-performance of statutory duties or (as a rule) a breach of official secrecy are qualified as serious breaches of official duty. Mere criticism of the manner in which the office is performed, on the other hand, cannot constitute grounds for removal from office. The breach of official duty must be of such a nature that it irrevocably damages confidence in the person and makes continuation in office appear unacceptable.

2. Permanent incapacity for office

17 Removal from office is permissible if the capacity to hold office has been permanently lost (Art. 44 para. 3 lit. b FADP). This is likely to apply only in exceptional cases. In particular, medical or illness-related reasons should be considered. However, family reasons are also possible. Finally, the official capacity may also be permanently lacking if the appointee is missing or has disappeared.

B. Procedure

18 The removal of a commissioner from office falls - along with his or her election - as one of the most important employer decisions within the competence of the United Federal Assembly. This is stated not only in Art. 44 para. 3 FADP, but also declaratorily in Art. 2 para. 1 of the Ordinance on the Employment Relationship of the Commissioner.

19 The Judicial Commission prepares a possible removal from office and submits the necessary motions to the United Federal Assembly (Art. 40a para. 1 lit. d ParlG and Art. 2 para. 2 of the Ordinance on the Employment Relationship of the Commissioner). As a rule, however, the Judicial Commission will first issue a warning for reasons of proportionality (Art. 44a FADP) before initiating proceedings for the removal from office.

20 Within the framework of the impeachment proceedings, the commissioner must be granted the right to be heard. In its principles of action on the proce-

dure for impeachment or non-re-election, the Judicial Commission provides, among other things, that the person affected by the impeachment proceedings has the right, after completion of the investigation and before reporting to the United Federal Assembly, to comment in writing or orally on the results of the investigation and the reasons for the decision (Art. 7 para. 4 of the principles of action). Subsequently, the application of the Judicial Committee to the United Federal Assembly must contain a statement of the opinion of the person concerned (Art. 14 para. 2 lit. d of the Principles of Action).

If the United Federal Assembly decides to remove the Commissioner from of- 21
fice, the question arises as to whether this decision can be challenged in court. In principle, no legal remedy is available against decisions of the United Federal Assembly (Art. 189 para. 4 of the Federal Constitution). However, in its report on parliamentary initiative 21.443, the SPK-N refers to the more recent practice of the ECtHR, according to which the guarantee of legal recourse pursuant to Art. 6 para. 1 ECHR applies in the case of the dismissal of judges. The SPK-N considers it conceivable - rightly in our view - that this case law could be transferred to the commissioner, who also has a strong independence. In this case, the commissioner would have to be able to challenge a removal from office by the United Federal Assembly before a court (Federal Administrative Court, Federal Supreme Court, ECHR).

The opinion expressed reflects the personal opinion of the authorship and does not bind the Federal Office of Justice.

BIBLIOGRAPHY

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.

MATERIALS

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).

COMMENTARY ON

Art. 44a FADP

A commentary by Danielle Schneider / Carl Jauslin

SUGGESTED CITATION

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 44a DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Schneider/Jauslin, N. XXX zu Art. 44a DSG.

Art. 44*a* Reprimand

The Judiciary Committee may issue a reprimand if it establishes that the Commissioner has failed to comply with official duties.

CONTENT

IN A NUTSHELL

Disciplinary law is governed by special legislation in Art. 44a FADP. The provision restricts the range of disciplinary measures possible under federal personnel law and makes only the measure of a warning available to the appointee. This takes into account the independence of the appointee. At the same time, the disciplinary measure of a warning provides the judicial commission with an instrument for objecting to conduct by the appointee that is in breach of duty and for protecting the reputation and trustworthiness of the FDPIC's authority.

I. GENERAL

A. Genesis

Article 44a FADP was inserted into the totally revised FADP as part of the parliamentary initiative SPK-N 21.443. During this work on the implementing law on the employment relationship of the Commissioner, it became apparent that individual additions to the totally revised FADP were necessary. In this context, the legislator considered - among other things - the disciplinary law as an important provision to be clarified at the formal-legal level. 1

B. Purpose of the Norm

Art. 44a FADP provides for a deviation from federal personnel law for the employment relationship of the Commissioner in the area of disciplinary law (cf. Art. 43 para. 3 first sentence FADP). Most of the disciplinary measures listed in Art. 99 para. 2 and 3 BPV (in conjunction with Art. 25 para. 2 lit. b and c BPG), which can be taken in the event of a breach of duties under employment law, are in fact incompatible with the office of the appointee or could jeopardize the independence of the appointee. This applies in particular to salary reductions and fines as well as changes in the scope of duties, working hours or place of work. However, the legislator did not want to completely dispense with disciplinary measures against the appointee, as such measures can help to ensure that the appointee performs his or her duties in accordance with the law. 2

3 Art. 44a FADP must be understood in light of this tension between the preservation of independence and the interest in the lawful execution of official duties. The provision restricts the range of disciplinary measures possible under federal personnel law and makes only the measure of a warning available to the appointee.

II. DISCIPLINARY MEASURE OF WARNING

4 Pursuant to Art. 44a FADP, the Judicial Commission may issue a warning if it finds that the appointee has violated official duties. This provides it with an instrument which it should use to ensure the reputation and trustworthiness of the FDPIC. With a warning, "the employer gives the employee to understand that he or she is not willing to continue to tolerate the reprimanded conduct and that he or she intends to take harsher measures in case of repetition or continuation of the reprimanded conduct."

5 In contrast to the removal from office pursuant to Art. 44 para. 3 lit. a FADP, a warning does not have to be based on a serious breach of official duty. The wording of the law seems to allow a warning for any kind of breach of official duty. However, in view of the principle of proportionality, a warning must be suitable and necessary to restore the proper performance of official duties by the commissioner. According to the explanations of the SPK-N on parliamentary initiative 21.443, a warning could, for example, be considered if the appointee violates the provisions on secondary employment (Art. 47 FADP) or the acceptance of gifts or other benefits (Art. 1 para. 2 of the Ordinance of the Federal Assembly of 17 June 2022 on the Employment Relationship of the Head of the Federal Data Protection and Information Commissioner [hereinafter "Ordinance on the Employment Relationship of the Appointee"] in conjunction with Art. 93 f. FADP). Art. 93 f. BPV) is violated. On the other hand, the Judicial Commission may not issue a warning if it is of the opinion that the Commissioner is setting the wrong priorities in the performance of his or her duties. This would be incompatible with the independence of the commissioner and would interfere with the performance of his or her duties.

6 As a disciplinary measure, a warning always presupposes fault. The appointee must therefore have acted intentionally or at least negligently.

III. DISCIPLINARY PROCEEDINGS

The Judicial Commission is responsible for imposing the warning on the appointee. This corresponds to Art. 2 para. 3 of the Ordinance on the Employment Relationship of the Commissioner, according to which the Judicial Commission makes those employer decisions that are not assigned to the United Federal Assembly. If the Judicial Commission comes to the conclusion that the conduct complained of constitutes a serious breach of official duty in accordance with Art. 44 para. 3 letter a FADP, it may request the United Federal Assembly to remove the appointee from office. 7

Disciplinary proceedings against the appointee shall be governed by the (subsidiary applicable) provisions of federal personnel law (Art. 1 para. 2 of the Ordinance on the Employment Relationship of the Appointee). 8

The warning may only be issued following a disciplinary investigation (Art. 99 para. 1 BPV). Art. 98 BPV applies to the disciplinary investigation: according to this, the judicial commission opens the disciplinary investigation and designates the person who will be entrusted with the investigation. This may also be an external person (Art. 98 para. 1 BPV). 9

The Administrative Procedure Act is applicable to the disciplinary proceedings (Art. 98 para. 2 BPV). This means in particular that the determination of the facts by the judicial commission is also governed by the provisions of the APA, namely with regard to the right to abstain (Art. 10 APA), the principle of investigation and the evidence (Art. 12 and Art. 14 ff. APA), the duties of the commissioner to cooperate (Art. 13 APA) and the procedural rights of the commissioner (in particular the right to inspect the files and to be heard; Art. 26 ff. APA). APA). 10

The warning must be issued as an order within the meaning of Art. 5 APA (Art. 34 APA). The commissioner may appeal the court commission's warning to the Federal Administrative Court (Art. 36 para. 1 BPG). 11

The opinion expressed reflects the personal opinion of the authorship and does not bind the Federal Office of Justice.

BIBLIOGRAPHY

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.

MATERIALS

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).

COMMENTARY ON

Art. 45 FADP

A commentary by Carl Jauslin / Danielle Schneider

SUGGESTED CITATION

Carl Jauslin/Danielle Schneider, Kommentierung zu Art. 45 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Jauslin/Schneider, N. XXX zu Art. 45 DSG.

Art. 45 Budget

The FDPIC shall submit the draft of his or her budget each year via the Federal Chancellery to the Federal Council. The Federal Council shall submit the budget unchanged to the Federal Assembly.

CONTENT

IN A NUTSHELL

The FDPIC drafts its budget independently and submits it to the Federal Council via the Federal Chancellery (FC). The latter submits it unchanged to the Federal Assembly for approval. This budget process, in which the FC and the Federal Council forward the FDPIC's budget unchanged and may not amend it, strengthens the independence of the FDPIC as a supervisory authority.

I. GENERAL

Budget sovereignty, the budget process and the budget decision are fundamental to the independence of the FDPIC as a supervisory authority (Art. 43 n. 4). Only those who independently decide on their budget are free to perform their tasks within the framework of the legal mandate. Indeed, functional independence presupposes a certain degree of financial or material independence. 1

Art. 45 describes the process through which the FDPIC's budget passes. The FDPIC's budget includes staff salaries, which make up by far the largest part of the budget, room rent, non-personnel IT expenses, consulting expenses, and other operating expenses. The provision is linked to Art. 43 para. 5 FADP, which already provides in connection with the position of the FDPIC that the Commissioner has his or her own budget. 2

Art. 45 FADP was included in the Federal Data Protection Act with the total revision of 25 September 2020 (entry into force 1.9.2023). The provision was proposed by Parliament and is not yet in the Federal Council's draft. In particular, the Commissioner felt that the regulation of his budget should be aligned with the regulation for the Federal Audit Office. The old data protection law of 19 June 1992 provided in Art. 26 para. 4 aDSG (now Art. 43 para. 5 FADP) only that the Commissioner had his or her own budget. Under the old law, the Federal Council was not yet obliged to adopt the FDPIC's draft budget unchanged. Moreover, the FDPIC did not yet have the possibility to present his or her budget to the Federal Assembly itself (see the new Art. 142 para. 2 and 3 third sentence ParlA). 3

II. BUDGET SOVEREIGNTY

4 Budget sovereignty means that the FDPIC draws up its budget independently. Budgetary sovereignty forms an essential part of the independence of the FDPIC. The FDPIC should independently determine what resources it needs to carry out its statutory tasks. In the area of data protection, this concerns the investigation of violations of data protection regulations (Art. 49 ff. FADP), administrative assistance (Art. 54 f. FADP), tasks related to data disclosure abroad (Art. 16 FADP), consultation on data protection impact assessments (Art. 23 FADP), as well as register management, information, awareness-raising and cooperation (Art. 56 ff. FADP). The administrative assignment of the FDPIC to the Federal Chancellery only affects the budget process and does not affect the budgetary sovereignty of the FDPIC (Art. 43 N. 19 ff).

III. BUDGET PROCESS

5 After the FDPIC has prepared its draft budget independently, it submits it to the Federal Council via the Federal Chancellery, to which it is administratively assigned (Art. 43 para. 4 second sentence FADP). Pursuant to Art. 142 para. 2 of the Parliament Act (ParlA), the Federal Council must include the draft budget and the FDPIC's accounts unchanged in its draft budget and accounts of the Confederation. The same applies to the estimates and accounts of the Federal Assembly, the federal courts, the Federal Audit Office, the Office of the Attorney General of Switzerland and the supervisory authority over the Office of the Attorney General of Switzerland. The common feature of the institutions mentioned is their independence from the Federal Council. In their actions, the aforementioned institutions are bound only by the law and not by the instructions of the Federal Council. The Constitution itself (in the case of the Federal Assembly and the Federal Supreme Court) or a federal law (in the case of the Swiss Federal Audit Office, the Office of the Attorney General of Switzerland as well as its supervisory authority) explicitly state the independence of the organizational units mentioned.

6 Art. 45 FADP is based on the solution adopted for the supervisory authority over intelligence activities when submitted via the department (cf. Art. 4 of the Ordinance of 16 August 2017 on the Supervision of Intelligence Activities, VAND). The Swiss Federal Audit Office, SFAO, on the other hand, submits its annual estimate directly to the Federal Council (cf. Art. 2 para. 3 FKG) - with-

out going through the Federal Department of Finance, to which the SFAO is attached (Art. 1 para. 3 FKG).

In addition, according to Art. 142 para. 3, third sentence, ParlA, the FDPIC itself represents the draft of its estimates and accounts before the Federal Assembly. In principle, this should be done by the Commissioner. By comparison, for the SFAO, the financial delegation of the two federal chambers (Art. 51 ParlA) performs this task, whereas the Federal Supreme Court and the supervisory authority over the Office of the Attorney General of Switzerland also represent their estimates before Parliament, as does the FDPIC itself before the Federal Assembly (Art. 142 para. 3 ParlA). 7

The budget process can be summarized as follows: 8

- The FDPIC prepares a draft budget that includes all necessary resources to conscientiously and dutifully fulfill its legally assigned duties as data protection and public information commissioner.
- The FDPIC submits his draft budget to the Federal Chancellery, to which he is administratively assigned (Art. 43 para. 4 second sentence FADP).
- The Federal Chancellery forwards the FDPIC's draft budget to the Federal Council.
- The Federal Council forwards the FDPIC's draft budget unchanged to the Federal Assembly for approval (Art. 45 FADP). In concrete terms, this means that the Federal Council includes the FDPIC's draft budget and accounts unchanged in the federal budget and accounts (Art. 142 para. 2 ParlA) and submits the draft federal budget to the Federal Assembly. It does so in the form of a simple federal decree (Art. 143 para. 3 ParlA).
- The Finance Committees of the two Councils discuss the estimates in advance (Art. 50 para. 1 ParlA). The councils are obliged to approve the budget (Art. 73 para. 3 ParlA).
- The FDPIC presents its draft budget to the Federal Assembly (Art. 142 para. 3, third sentence).
- The Federal Assembly is responsible for approving the FDPIC's draft budget. If, in the procedure for settling differences between the two Councils, a motion for agreement on the federal resolution on the federal budget is rejected, the resolution of the third deliberation providing for the lower amount is deemed to have been adopted (Art. 94 ParlA).

IV. BUDGET RESOLUTION

9 Parliament is responsible for deciding on the budget. In order for Parliament to be able to deliberate meaningfully on the FDPIC's budget request, the FDPIC must justify its budget.

10 The parliament may not attach any conditions or requirements to the approval of the budget; specifications on the use of funds or the setting of priorities are not permitted. The FDPIC may freely dispose of the funds granted within the scope of its legal mandate.

11 Article 15 para. 6 of the modernized 108+ Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data requires that the supervisory authority have the necessary means to effectively carry out its functions and exercise its powers. The Schengen-relevant EU Directive 2016/680 also provides in Art. 42 para. 4 that each supervisory authority must be provided with the resources it needs to effectively carry out its functions and exercise its powers, including in the context of mutual assistance, cooperation and participation. Furthermore, sufficient resources of the data protection supervisory authority are an essential criterion when assessing the adequacy of the level of data protection from the perspective of the EU Data Protection Regulation 2016/679 (cf. in this regard Art. 52 para. 4 in conjunction with Art. 45 para. 2 lit. b). Finally, the effectiveness of supervision depends on the available resources.

12 A budget that is insufficient to fulfill the tasks conferred by law calls into question the independence of supervision. Legal mechanisms to review the adequacy of the budget are lacking. At the same time, budget overruns owed to the fulfillment of statutory tasks are not considered a breach of official duty (Art. 44 para. 3 lit. a FADP).

The view expressed reflects the personal opinion of the authors and does not bind the Federal Office of Justice.

BIBLIOGRAPHY

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.

MATERIALS

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).

COMMENTARY ON

Art. 46 FADP

A commentary by Carl Jauslin / Danielle Schneider

SUGGESTED CITATION

Carl Jauslin/Danielle Schneider, Kommentierung zu Art. 46 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Jauslin/Schneider, N. XXX zu Art. 46 DSG.

Art. 46 Incompatibility

The Commissioner may not be a member of the Federal Assembly or the Federal Council and may not have any other employment relationship with the Confederation.

CONTENT

IN A NUTSHELL

The commissioner may not be in any other employment relationship with the Confederation. In particular, simultaneous membership of the Federal Assembly or the Federal Council is incompatible with the commissioner's supervisory function. This is intended to avoid conflicts of interest and to strengthen the independence of the FDPIC.

I. GENERAL

The Commissioner may not be a member of the Federal Assembly or the Federal Council and may not have any other employment relationship with the Confederation. This is intended to exclude conflicts of interest arising from different and simultaneously exercised functions. 1

Art. 144 FC regulates incompatibilities between functions of members of the legislative, executive and judicial branches and is an expression of the separation of powers at federal level. Members of the National Council, the Council of States, the Federal Council and judges of the Federal Supreme Court cannot simultaneously belong to another of these authorities. Incompatibility rules are intended to prevent concentrations of power in one person, to prevent conflicts of interest, to safeguard the independence of office holders and to prevent impairments in the performance of their duties. Paragraph 3 of Art. 144 FC states that the law may provide for further incompatibilities. For members of Parliament, the incompatibility provisions are found in Art. 14 f. ParlA; for the members of the Federal Council and the Federal Chancellor, the professional incompatibilities are specified in Art. 60 GAOA. 2

Art. 46 FADP also constitutes a statutory incompatibility within the meaning of Art. 144 para. 3 FC. The provision on the incompatibility of the appointee on the basis of function corresponds to that for federal judges (Art. 6 para. 1 BGG, Art. 6 para. 1 VGG, Art. 44 para. 1 StBOG, similarly also Art. 10 para. 1 PatGG) and that for members of the supervisory authority over the Office of the Attorney General of Switzerland (Art. 24 para. 1 StBOG). 3

Art. 46 FADP was added to the Federal Data Protection Act by the total revision of 25 September 2020 (entry into force 1.9.2023). The provision was proposed by Parliament and is not yet in the Federal Council's draft. Under the 4

old Data Protection Act of June 19, 1992, questions of functional incompatibility had to be assessed from the perspective of secondary employment.

5 Functional incompatibility is a sine qua non for guaranteeing the independence of the Commissioner and therefore an outgrowth of the provisions of European law in Art. 15 para. 5 of the modernized 108+ Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data, Art. 42 para. 3 of the Schengen-related Directive (EU) 2016/680 and Art. 52 para. 3 of the European Union's General Data Protection Regulation 2016/679.

6 Art. 46 FADP provides for three incompatibilities for the Commissioner, which will be briefly discussed below. However, the incompatibilities apply solely to the Commissioner and not to his or her employees.

II. NO MEMBER OF THE FEDERAL ASSEMBLY

7 The appointee may not at the same time be a member of the Federal Assembly, i.e. of the National Council or the Council of States. Thus, in the event of election as a commissioner, the person elected must terminate any existing functions or employment before taking office.

8 Members of the Federal Assembly may be elected as commissioners, but must resign from Parliament by the time they take office at the latest. This has already been done in two out of three elections by the Federal Council. Conversely, pursuant to Art. 44 para. 2 FADP, the appointee may terminate his or her employment at the end of any month, subject to six months' notice, and subsequently take up a new position as a member of Parliament (or the Federal Council; see n. 9 below). Pursuant to Art. 44 para. 2 FADP, the Judicial Commission may grant the appointee a shorter notice period in such cases if no substantial interests are opposed.

III. NO MEMBER OF THE FEDERAL COUNCIL

9 The Commissioner may not at the same time be a member of the Federal Council. Even though, on the one hand, the Federal Council has no authority to issue instructions to the FDPIC (Art. 43 para. 4 FADP) and, on the other hand, the FDPIC may not exercise its supervisory function through the Federal Council (Art. 4 para. 2 lit. b FADP), conflicts of interest cannot be avoided

and the independence of the FDPIC would not be guaranteed by such a personal union.

IV. NO OTHER EMPLOYMENT RELATIONSHIP WITH THE CONFEDERATION

The function of the Commissioner is also not compatible with other employment relationships that exist at the same time with the Confederation. Other employment relationships with the Confederation must therefore be terminated by the time the appointee takes office (cf. n. 8). This incompatibility constitutes a kind of subsidiary general clause in relation to the two specific incompatibilities relating to Parliament and the Federal Council. Against the background of the central importance of the independence of the Commissioner, such a broadly defined incompatibility rule is to be welcomed. 10

For reasons of constitutional competence, Art. 46 makes no statements on incompatibility with functions and employment at the cantonal or municipal level. Whether such offices and employment at the cantonal or communal level are compatible with the function of the head of the FDPIC must be examined in the case of secondary employment within the meaning of Art. 47 FADP. Conversely, secondary employment connected with an employment relationship with the Confederation is already inadmissible due to the incompatibility provision in Art. 46 FADP. 11

The view expressed reflects the personal opinion of the authors and does not bind the Federal Office of Justice.

BIBLIOGRAPHY

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.

COMMENTARY ON

Art. 47 FADP

A commentary by Danielle Schneider / Carl Jauslin

SUGGESTED CITATION

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 47 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Schneider/Jauslin, N. XXX zu Art. 47 DSG.

Art. 47 Additional occupation

[1] The Commissioner may not have any additional occupations.

[2] The Judicial Committee may permit the Commissioner to carry out an additional occupation provided this does not adversely affect the exercise of his or her duties or the independence and the reputation of the FDPIC.The decision shall be published.

CONTENT

IN A NUTSHELL

As a matter of principle, the commissioner may not engage in any secondary employment (Art. 47 Para. 1 FADP). This prohibition helps to strengthen independence. In order for an activity to qualify as secondary employment, it must be of a certain quality and intensity. It does not matter whether the activity is remunerated or not. By way of exception, the Federal Judicial Commission may allow the Commissioner to exercise a secondary activity, provided that neither the exercise of the function, nor the independence, nor the reputation of the FDPIC are impaired (Art. 47 para. 2 FADP). In view of the high demands on the independence of the commissioner, a strict standard is appropriate. Any secondary employment of the officer must be published in order to take account of the need for transparency.

I. GENERAL

A. Norm Purpose

Art. 47 FADP provides that the Commissioner may not, in principle, engage in any secondary employment (Art. 47 para. 1; n. 4 f.). This special legal regulation, which is stricter than the general federal personnel law (Art. 23 BPG in conjunction with Art. 91 BPV), takes into account the independence of the appointee. In the performance of his or her duties, the appointee should not have any conflict of interest that could compromise his or her independence and cast doubt on the credibility of the office. 1

B. History of origins

The fundamental prohibition of secondary employment for the Commissioner was already introduced in the first stage of the total revision of the FADP in Art. 26b aFADP (data protection provisions for Schengen cooperation in criminal matters). Regarding the secondary employment, the requirements of Art. 42 (3) of Directive (EU) 2016/680 were authoritative. The provisions entered into force on March 1, 2019. 2

In terms of content, Art. 47 FADP has not changed since then. However, the responsibility for authorizing secondary employment of the appointee has been adjusted twice: In the version of the totally revised FADP of September 3

15, 2020, the task was transferred to the United Federal Assembly. Subsequently, concerns arose that the allocation of tasks was not appropriate to the levels and that the procedure could prove too cumbersome in practice. Therefore, within the framework of the parliamentary initiative SPK-N 21.443, the Judicial Commission was declared responsible (Art. 47 para. 2; cf. n. 11 et seq.).

II. PRINCIPLE: PROHIBITION OF SECONDARY EMPLOYMENT (PARA. 1)

4 Art. 47 para. 1 FADP prohibits the Commissioner from engaging in secondary employment. This applies regardless of whether such activity is remunerated or not. The fundamental prohibition of secondary employment thus goes further than the incompatibility rule enshrined in Art. 46 FADP and includes, in particular, cantonal and municipal offices or employment.

5 The FADP does not define the term secondary employment. However, it is clear from the materials that not every activity that the Commissioner performs in addition to his or her office is to be considered inadmissible. Instead, the secondary employment must be of a certain quality and intensity. In particular, leisure activities or hobbies are not considered to be secondary employment.

III. EXCEPTION: AUTHORIZATION OF SECONDARY EMPLOYMENT (PARA. 2)

6 Exceptions to the prohibition of secondary employment are possible under the conditions of Art. 47 Para. 2 FADP: The Judicial Commission may permit the Commissioner to engage in secondary employment (cf. N. 11 ff.), provided that neither the exercise of the function, nor the independence, nor the reputation of the FDPIC are impaired (cf. N. 7 ff.). The aforementioned requirements are to be understood cumulatively. When granting approval, the judicial commission takes into account in particular the content of the secondary employment, the time required and the amount of any compensation.

A. Content-related requirements

First, the secondary employment must not interfere with the commissioner's performance of his or her duties. The performance of duties should not be restricted by the absence or unavailability of the appointee. It should be noted that the office of the Commissioner - unlike under previous law, in which no specific degree of employment was prescribed - may now only be exercised on a full-time basis (Art. 8 of the Ordinance of the Federal Assembly of 17 June 2022 on the Employment Relationship of the Head of the Federal Data Protection and Information Commissioner). This is related to the demands on the office, which have increased in particular due to digitalization, as well as the new tasks and competences that the FDPIC will receive as part of the total revision of the FADP (e.g. new powers of investigation and disposition under Art. 49 ff. FADP). 7

Secondly, the secondary employment must not impair the independence of the FDPIC. A conflict of interest or the mere appearance of a conflict of interest must be legally and factually excluded. 8

Thirdly, the secondary employment must not impair the reputation of the FDPIC. This is all the more true since the function of the FDPIC is highly personalized and a negative perception of the appointee or appointees may also have an impact on the authority of the FDPIC. 9

Examples: 10

- Serving as a member of a company's executive board, board of directors, or auditing body is likely to impair the appointee's independence as a general rule (and, depending on the scope of the activity, may also limit the appointee's availability for the office).
- Furthermore, activities for associations whose objectives call into question data protection or supervision by the FDPIC would be inadmissible, as this would jeopardize the reputation of the FDPIC.
- Whether a teaching activity (e.g. as a lecturer at a university) could be approved depends on the circumstances of the individual case. In any case, only a smaller workload would be possible.

B. Responsibility

11 The judicial commission is responsible for approving secondary employment (for the history of the development of Art. 47 para. 2 FADP, cf. n. 2 f.).

12 On the basis of the information submitted by the appointee, the Judicial Commission examines in each individual case whether the criteria for an exception to the fundamental prohibition of secondary employment are met. In view of the high requirements for the independence of the commissioner, a strict standard is appropriate. However, if the requirements of Art. 47 Para. 2 FADP are clearly met, it would be arbitrary for the Judicial Commission to refuse to grant the appointee an exemption.

13 The decision of the court commission is published (Art. 47 para. 2 second sentence FADP). This contributes to transparency regarding the office of the commissioner.

The opinion expressed reflects the personal opinion of the authorship and does not bind the Federal Office of Justice.

BIBLIOGRAPHY

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.

MATERIALS

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).

COMMENTARY ON

Art. 47a FADP

A commentary by Danielle Schneider / Carl Jauslin

SUGGESTED CITATION

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 47a DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Schneider/Jauslin, N. XXX zu Art. 47a DSG.

Art. 47a Recusal

In the event of any dispute with regard to the Commissioner's recusal, the decision shall be taken by the president of the division of the Federal Administrative Court that is competent in data protection matters.

CONTENT

IN A NUTSHELL

Art. 47a FADP clarifies the question of who decides on the recusal of the commissioner in the event of a dispute. The task is assigned to the president of the department of the Federal Administrative Court responsible for data protection. This solution preserves the independence of the commissioner and the fact that he or she is not bound by instructions.

I. HISTORY OF ORIGINS

Art. 47a FADP was inserted into the totally revised FADP as part of the parliamentary initiative SPK-N 21.443. When drafting the implementing regulations on the employment relationship of the appointee, Parliament found that it was unclear who would decide on the appointee's recusal in the event of a dispute. 1

The usual responsibilities under federal personnel law (supervisor pursuant to Art. 94a para. 3 FOPI) and administrative procedural law (supervisory authority or collegiate authority to the exclusion of the member concerned pursuant to Art. 10 para. 2 APA) were out of the question due to the special position of the appointee. The United Federal Assembly or the Judicial Commission, which are in principle responsible for employer decisions vis-à-vis the Commissioner (cf. Art. 2 of the Ordinance of the Federal Assembly of 17 June 2022 on the Employment Relationship of the Head of the Federal Data Protection and Information Commissioner; hereinafter "Ordinance on the Employment Relationship of the Commissioner"), were also out of the question as decision-making bodies due to the independence of the Commissioner or the fact that he or she is not bound by instructions. 2

Parliament filled this gap by entrusting the president of the department of the Federal Administrative Court responsible for data protection with the decision on a disputed recusal of the Commissioner. This competence is obvious, since the president of Division I of the Federal Administrative Court already performed special duties in the area of data protection under the previous law (cf. Art. 30 para. 2 and Art. 33 para. 2 aFADP). 3

II. GROUNDS FOR RECUSAL OF THE COMMISSIONER

4 The grounds for recusal of the Commissioner are generally governed by federal personnel law (Art. 43 para. 3 first sentence FADP in conjunction with. Art. 1 para. 2 of the Ordinance on the Employment Relationship of the Commissioner). Pursuant to Art. 94a para. 1 FOPI, the appointee shall recuse himself or herself if he or she could be biased in a matter due to a personal interest or for other reasons. The appearance of bias is sufficient (Art. 94a para. 1 FOPI). Art. 94a para. 2 FOPI lists (not exhaustively) the following grounds for partiality:

- the special closeness of relationship or personal friendship or enmity with natural and legal persons involved in or affected by a transaction or decision-making process (lit. a) and
- the existence of a job offer from a natural or legal person involved in or affected by a transaction or decision-making process (lit. b).

5 In contrast, in the context of an investigation into violations of data protection regulations, the provisions of administrative procedural law and thus the grounds for recusal under Art. 10 para. 1 FADP apply (Art. 94a para. 4 FOPI and Art. 52 para. 1 FADP). These include, among others:

- a personal interest in the matter (Art. 10 para. 1 lit. a APA),
- marriage, registered partnership or de facto cohabitation with a party (Art. 10 para. 1 lit. b APA),
- relationship or affinity with a party (Art. 10 para. 1 lit. bbis APA), and
- representation of a party or acting for a party in the same matter (Art. 10 para. 1 lit. c APA).

III. DECISION ON RECUSAL

6 The grounds for recusal are of a mandatory nature. The commissioner must therefore take them into account on his or her own initiative and bring them to the attention of the persons involved. If the appointee withdraws, his or her deputy shall take over the business.

7 If, on the other hand, the Commissioner's recusal is disputed, the president of the department of the Federal Administrative Court responsible for data pro-

tection shall decide on the matter (Art. 47a FADP). This decision may be appealed to the Federal Supreme Court in public law matters (Art. 82 ff. and Art. 92 BGG).

The opinion expressed reflects the personal opinion of the authorship and does not bind the Federal Office of Justice.

BIBLIOGRAPHY

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.

MATERIALS

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).

COMMENTARY ON

Art. 48 FADP

A commentary by Carl Jauslin / Danielle Schneider

SUGGESTED CITATION

Carl Jauslin/Danielle Schneider, Kommentierung zu Art. 48 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Jauslin/Schneider, N. XXX zu Art. 48 DSG.

Art. 48 Self-regulation of the FDPIC

The FDPIC shall ensure by means of suitable control measures, in particular in relation to data security, that the legally compliant implementation of data protection regulations under federal law is guaranteed within his or her office.

CONTENT

IN A NUTSHELL

Compliance with data protection regulations by the FDPIC is a legal obligation that already arises from the FDPIC's capacity as a federal body. Since no external data protection supervision is provided for the FDPIC, the legislator obliges the FDPIC to self-monitor: according to Art. 48 FADP, the FDPIC must ensure that legally compliant enforcement is guaranteed by means of appropriate control measures. Art. 40 FADP specifies that the FDPIC must draw up processing regulations for all of its automated data processing operations - regardless of whether it processes sensitive personal data or carries out profiling. This ensures that compliance with data protection regulations is also monitored within the FDPIC, which strengthens the credibility of the FDPIC as a supervisory authority vis-à-vis third parties.

I. GENERAL

Article 48 of the FADP is addressed to the FDPIC - but not in its capacity as a supervisory authority, but as a federal body that processes personal data. It obliges the FDPIC to ensure appropriate control measures to guarantee data security in particular and the legally compliant enforcement of federal data protection regulations in general, also within its institution. Since no external data protection supervision is provided for the FDPIC as a supervisory authority, the legislator obliges the FDPIC with this provision to self-monitor the processing of personal data. 1

The FDPIC processes personal data, including particularly sensitive personal data, for the following purposes (Art. 39 FADP): 2

- to carry out its supervisory activities (lit. a),
- to carry out its advisory activities (lit. b),
- for cooperation with other authorities (lit. c),
- for the performance of its duties under the penal provisions of the FADP (lit. d),
- to fulfill its duties under the Public Information Act (lit. e-g),
- to inform parliamentary supervision (lit. h), to inform the public (lit. i) and to carry out its training activities (lit. j).

The FDPIC processes personal data both in his function as data protection commissioner and as public information commissioner. Specifically, he maintains in particular a business administration system (Art. 57h GAOA), a personnel administration system, a list of data protection advisors (Art. 10 para. 3 lit. d FADP; Art. 10 para. 4 FADP in conjunction with Art. 27 para. 2 FADP), the directory of processing activities of federal bodies (Art. 12 para. 4 FADP), and a data breach notification portal (Art. 24 FADP). In particular, within the scope of its legal duties, the FDPIC may process personal data of its employees, personal data of other federal employees, as well as data of third parties, including data of legal entities (Art. 57r GAOA).

3 The FDPIC itself is not subject to any external data protection supervision, which is why it is required to carry out self-monitoring. The provision in Art. 48 FADP makes it clear that even the FDPIC, as a supervisory authority in the area of data protection, is not above data protection law and must also ensure compliance within its own authority. External control of the FDPIC would disproportionately limit its independence measured against the rather low risk of data misuse.

4 As a federal body, the FDPIC is bound not only by the general provisions in Arts. 5-13 and 16-29, but also by the special provisions on data processing by federal bodies under Arts. 33 ff. FADP. Art. 48 FADP provides that the FDPIC must provide for appropriate control measures to ensure compliance with these obligations. This obligation to self-monitor is due to the fact that there is no corresponding external data protection supervision for the FDPIC. The primary obligations are thus no different from those of other federal bodies; Art. 48 FADP concerns only the obligations of the FDPIC to control with regard to compliance with these primary obligations. In particular, the FDPIC must take all those control measures that it usually carries out in the context of its supervisory activities vis-à-vis other federal bodies, insofar as these also prove to be appropriate in the case of self-monitoring. This strengthens the credibility of the FDPIC in its supervisory activities vis-à-vis federal bodies and private individuals.

5 The provision in Art. 48 FADP on self-monitoring by the FDPIC was incorporated into the Federal Data Protection Act with the total revision of 25 September 2020 (entry into force on 1 September 2023).

II. CONTROL MEASURES

A. Data security in particular

Article 48 FADP requires the FDPIC to establish appropriate control measures to guarantee data security within its own institution. According to Art. 5 lit. h FADP, a data security breach is "a breach of security that results in personal data being inadvertently or unlawfully lost, deleted, destroyed or altered, or disclosed or made accessible to unauthorized persons." 6

The obligation to ensure data security for the FDPIC already arises in a general way from Art. 8 FADP. In accordance with this provision, data controllers and processors must ensure data security appropriate to the risk by means of suitable technical and organizational measures. The measures put in place must make it possible not only to detect breaches of data security retrospectively, but also to prevent them. Data security is specified in more detail in the DPO. In particular, Art. 3 DPO lists a number of technical and organizational measures to achieve the data security goals set forth in Art. 2 DPO, such as access, user, input and disclosure controls. The processing regulations for federal bodies pursuant to Art. 6 FADP also serve as a means of ensuring data security. 7

Against this background, the Federal Council has specified the FDPIC's obligation for self-monitoring in Art. 40 FDPIC. The FDPIC must draw up processing regulations for all automated processing - irrespective of whether, for example, sensitive personal data are being processed, profiling is being carried out or the purpose of the processing or the manner in which the data are processed may lead to a serious interference with the fundamental rights of the data subject. Indeed, Art. 40 DPA declares Art. 6 para. 1 DPA and the requirements therein for the establishment of a processing regulation not applicable in the case of the FDPIC. 8

Apart from the obligation to draw up processing regulations, Art. 40 FDPIC does not mention any further measures within the framework of self-monitoring by the FDPIC. In the explanatory notes to Art. 40 DPA, the Federal Office of Justice states that the FDPIC, like the other federal bodies, must also provide for appropriate internal processes that implement the processing regulations and verify compliance. The legal provision in Art. 48 FADP, however, speaks in a more general manner of "appropriate control measures, in particu- 9

lar with regard to data security" The creation, implementation, review as well as regular adaptation of the processing regulations pursuant to Art. 40 FADP consequently does not release the FDPIC from its more general obligation pursuant to Art. 48 FADP to provide for more extensive control measures, provided that these are judged to be appropriate and adequate.

B. Legally compliant enforcement of data protection regulations in general

10 Art. 48 FADP obliges the FDPIC to establish control measures that ensure the legally compliant enforcement of federal data protection regulations. This obligation goes beyond the creation and implementation of processing regulations as defined in Art. 40 FADP. In particular, it requires that the planned data processing operations be regularly checked for their conformity with the federal data protection provisions. It is precisely within the framework of the internal control system (ICS) that the FDPIC should provide for further measures to ensure compliance with the FADP requirements.

11 In contrast to the obligation to draw up processing regulations, however, control measures going beyond this are only required if, on the one hand, they are suitable for ensuring compliance with the data protection provisions and, on the other hand, they are proportionate to the risk of data misuse and the threat to the fundamental rights of the data subject. Specifically, the FDPIC's obligation must not result in making its statutory supervisory and advisory duties impossible or disproportionately difficult. This said, the FDPIC may take into account the necessary human resources incurred in the context of self-regulation in its budget request.

The view expressed reflects the personal opinion of the authors and does not bind the Federal Office of Justice.

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 49 FADP

A commentary by Michael Reinle

SUGGESTED CITATION

Michael Reinle, Kommentierung zu Art. 49 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Reinle, N. XXX zu Art. 49 DSG.

Section 2 Investigation of Violations of Data Protection Regulations

Art. 49 Investigation

[1] The FDPIC shall open an investigation into a federal body or a private person ex officio or in response to a report if there are sufficient indications that a data processing activity could violate data protection regulations.

[2] It may refrain from opening an investigation if the violation of data protection regulations is of minor importance.

[3] The federal body or the private person shall provide the FDPIC with all the information and documents that is needed for the investigation. The right to refuse to provide information is governed by the Articles 16

and 17 of the APA, unless Article 50 paragraph 2 of this Act provides otherwise.

[4] If the data subject has filed a report, the FDPIC shall inform them about the steps taken in response and the result of any investigation.

CONTENT

IN BRIEF

This provision is crucial in terms of strengthening the competences of the FDPIC. In particular, the obligations of federal bodies and private persons to cooperate in the investigation are important. What is new and also significant is that the FDPIC can open an investigation against private persons if there are sufficient indications of a breach of data protection regulations. Under the previous FADP, the authority to investigate private persons was more limited.

I. GENERAL

A. Normative Purpose and Background

1 While Art. 4 FADP states in general terms that the FDPIC is responsible for supervising the application of federal data protection legislation, Art. 49 FADP regulates one of the most important powers of the FDPIC in connection with this supervision, namely the investigation of possible data protection violations by federal bodies and private persons.

2 One of the most important objectives of the revision of the FADP was to strengthen the supervisory competences of the FDPIC. This was also because the previous FADP was considered toothless with regard to the supervision of data processing by private persons (Art. 29 aFADP).

3 In addition, the previous investigative powers of the FDPIC were below international standards, which is why it was feared that without a strengthening of the investigative powers of the FDPIC, a positive adequacy decision of the EU could be in danger.

B. History of origins

4 In the normative concept for the revision of the Data Protection Act, the strengthening of the competences of the FDPIC was stated as one of the core demands in the revision of the DPA and, among other things, the introduction of a preliminary investigation procedure and the strengthening of the investigative powers were discussed.

5 In Art. 41 FDPA, various measures from the norm concept were implemented: Thus, the investigative powers vis-à-vis federal bodies and private persons,

which had previously been contained in Art. 27 and Art. 29 aFADP, were combined in one provision, and the informal preliminary clarification procedure was regulated. While Art. 29 aFADP only permitted the opening of investigations against private persons under limited conditions, these restrictions were to be deleted in the future. This was also justified by the fact that the previous restrictions in Art. 29 aFADP would not meet the requirements of E-SEV 108. The new investigative powers of the FDPIC were also said to be a crucial element with regard to Art. 45 of Regulation (EU) 2016/679 to ensure that the European Commission renews or maintains the adequacy decision vis-à-vis Switzerland. Art. 41 VE-DSG was the subject of lively discussion in the consultation. While certain participants in the consultation welcomed the strengthening of investigative powers, others thought it went much too far.

The content of Art. 43 of the Draft Data Protection Act was based on Art. 41 of the Draft Data Protection Act. However, the preliminary investigation procedure was not mentioned. Also, the investigative measures explicitly mentioned in Art. 41 para. 3 VE-DSG were omitted or copied into another provision. In turn, the message on the DPA revision emphasized that the new regulation of the investigative powers of the FDPIC was important because its monitoring powers vis-à-vis the private sector would not currently meet the requirements of the E-SEV 108. 6

Art. 43 E-DSG was the subject of parliamentary deliberations. In the National Council, the discussion focused primarily on the requirements for opening an investigation. The "Romano" minority wanted to raise the minimum requirements for opening an investigation. The reason given for this was that mere indications of a violation of data protection regulations would not satisfy the requirements of a procedure based on the rule of law. It was also feared that the FDPIC could be overburdened if the requirements were too low. The majority, on the other hand, did not want to "handcuff" the FDPIC. The responsible Federal Councillor Keller-Sutter pointed out that the proposal of the majority - there must be sufficient indications and not merely signs of a data protection breach - would not represent a material change compared to Art. 43 E-DSG. However, it is critical of a further increase in the requirements. The "Romano" minority amendment would lead to a certain degree of legal uncertainty in the procedures of the FDPIC. In addition, the increased requirements for the opening of proceedings would jeopardize the adequacy of the Swiss level of data protection in an area of particular importance to the 7

EU. Neither Convention 108+ nor the EU legal acts would provide for such a limitation of the investigative powers of data protection supervisory authorities. The National Council followed the majority opinion.

8 The Council of States concurred with the decision of the National Council regarding Art. 43(1) E-DSG. The Council of States primarily discussed Art. 43 (3) E-DSG. The debate was about the protection of professional secrecy. Although Art. 43 (3) E-DSG would already protect the professional secrecy of lawyers and doctors, for example, the Council of States committee requested that the reservation of professional secrecy be explicitly mentioned again. BR Keller-Sutter defended the proposal of the Federal Council. She emphasized that professional secrecy was already sufficiently protected in the applicable procedural laws. In the view of the Federal Council, the renewed emphasis on professional secrecy would rather lead to legal uncertainties. The question would arise why other important grounds for refusal under general procedural law were not also expressly mentioned again. However, the Council of States followed its commission. The National Council followed this decision of the Council of States.

II. INVESTIGATION

A. Difference from previous law

9 Until now, investigations against federal bodies as well as private persons were governed by different provisions (Arts. 27 and 29 aFADP). The requirements for opening an investigation were also different. Art. 27 para. 2 aFADP did not provide for a specific threshold for opening investigations against federal bodies. According to Art. 29 para. 1 aFADP, on the other hand, the FDPIC was only allowed to open investigations against private persons if the processing methods were likely to infringe the personality of a larger number of persons (system error), data collections had to be registered or there was a duty to inform according to Art. 6 para. 3 aFADP. However, these requirements in Art. 29 para. 1 aFADP did not meet the international standards.

10 Now, the former requirements for opening an investigation against private persons are deleted. In addition, uniform rules apply to the opening of investigations against federal bodies and private persons. This leads to a strengthening of the FDPIC.

B. Opening of the investigation (para. 1)

Pursuant to Art. 49 para. 1 FADP, the FDPIC shall open an investigation ex officio or upon notification if there are sufficient indications that a data processing operation may violate data protection provisions. 11

The report may be made by a third party or by the data subject, i.e. in principle by anyone. However, the person making the report does not have party status in the proceedings (Art. 52 para. 2 FADP e contrario). The report can also be made anonymously. Since the FDPIC now only has to initiate an investigation if there are sufficient indications of a data protection violation, an anonymous report may have a negative impact on this decision. Whether or not a report is made, for example, by a person with a close connection to the reported data processing, is thus certainly relevant in this assessment. 12

The FDPIC can also become active if press releases report on possible data protection violations, which already corresponds to current practice. 13

Data protection regulations within the meaning of Art. 4 para. 1 FADP do not only refer to the regulations of the FADP, but also to the sector-specific data protection regulations of the Confederation. This includes data protection-related provisions in other federal decrees as well as international treaties specific to data protection law. This extension beyond the DPA is primarily relevant for federal bodies. 14

An investigation may only be opened if there are sufficient indications of a breach of data protection regulations. This requirement was introduced by Parliament (see n. 7 above). Based on the parliamentary deliberations, it is not possible to find any overly clear guidelines as to what is to be considered a sufficient indication. A minority of the National Council wanted Art. 43 E-DSG to be worded as follows: "In the event of well-founded suspicion, the Commissioner shall open an investigation ex officio or upon well-founded complaint against a federal body or a private person if there are clear indications that a data processing operation could violate data protection regulations." However, these stricter requirements - in particular the requirement that there must be clear indications - were rejected. Sufficient indications do not have to be clear indications or reasonable suspicion in the sense of criminal procedure law. According to BR Keller-Sutter, sufficient indications should not be a material change compared to the Federal Council's proposal, which simply spoke of indications. In the end, the Federal Council also did not want 15

the FDPIC to exhaust its resources with blanket investigations. It must be a matter of indications that justify the use of the FDPIC's resources. The parliamentary deliberations and in particular the votes of the majority show that one wanted to grant the FDPIC discretionary powers in this regard.

C. Waiver of investigation (para. 2)

16 According to Art. 49 para. 2 DPA, the FDPIC may waive a formal investigation if the violation of data protection rules is of minor importance. According to the dispatch, this would be the case, for example, if a sports or cultural association sends an e-mail message to all its members without concealing the identity of the recipients. Paragraph 2 can also be applied, according to the message, if the FDPIC is of the opinion that the advice given to the person responsible is sufficient to eliminate a situation that is hardly problematic in itself.

17 According to Rosenthal, a waiver should also be possible if, in the case of data breach notifications, it is clear that the breach is not serious or that the responsible party has the matter under control.

18 On the other hand, there are arguments against a waiver if the data processing in question affects a large number of individuals and there is therefore a general interest on the part of the public.

19 The FDPIC should act if in his view there is sufficient public interest for an investigation. On the other hand, it should refrain from an investigation if only the privacy of an individual is affected. In the latter case, the person concerned has the option of bringing an action against the private individual before a civil court or of challenging the decision of the federal body before the competent complaints body.

20 Art. 49 para. 1 in conjunction with. para. 2 FADP is an "optional" provision, which leaves the FDPIC some room for maneuver in deciding whether to open or refrain from an investigation. Parliament has left this leeway to the FDPIC (see n. 7 above). It is up to the FDPIC to decide on the appropriateness of such an investigation. Thus, there is still no entitlement of the whistleblower to conduct a formal investigation.

21 The FDPIC has already made it clear that he will continue to carry out informal contacts, i.e. preliminary investigations. If these informal contacts show

that the person responsible acknowledges deficiencies that have been brought to his attention and remedies them within a reasonable period of time, the FDPIC will refrain from opening a formal investigation. Due to the limited resources of the FDPIC, it can generally be assumed that he will continue to prioritize the handling of complaints in accordance with the principle of opportunity even after the new FADP enters into force.

D. Obligation to cooperate (para. 3)

Art. 49 para. 3 FADP regulates the duties of cooperation of the private person and the federal body in the event of a formal investigation by the FDPIC, with the majority of the provisions under Arts. 27 para. 3 and 29 para. 2 aFADP having been adopted. 22

The party to the proceedings must provide the FDPIC with all the information and documents that the FDPIC requires for the investigation. According to Art. 49 Para. 3 FADP, a party is not obliged to do more than provide information and hand over documents. Cooperation may be requested informally. Further measures in the investigation are regulated in Art. 50 and 52 FADP. 23

According to Art. 49 para. 3 FADP, the federal bodies and the private person must cooperate. As under the previous law, the FDPIC may also require the data processors with primary responsibility at the federal body concerned or the private person concerned, as well as other employees, contract processors, auxiliary persons and third parties who are involved in the data processing to be investigated or who can provide relevant information about it, to cooperate. 24

The obligations to cooperate under Art. 49 para. 3 FADP may relate to information on a specific case, but may also be of a fundamental nature. They relate to all documents that may be relevant for the evaluation by the FDPIC. 25

So that the persons obliged to cooperate do not have to incriminate themselves, there are also rights to refuse information in the investigation by the FDPIC. The rights to refuse information are based on Art. 16 and 17 APA. 26

Art. 16 para. 1 APA refers to Art. 42 paras. 1 and 3 of the Federal Act of 4 December 1947 on Federal Civil Procedure with regard to the right to refuse to give evidence. According to Art. 42 paras. 1 and 3 of the Federal Act on Civil Procedure, persons questioned may refuse to testify if answering the question 27

may expose them to the risk of criminal prosecution. This concerns persons who are subject to a legal obligation of secrecy according to Art. 321, 321bis and 321ter StGB. This means that doctors can refuse to provide the FDPIC with personal data about their patients if the patients do not consent to this disclosure. The same applies to lawyers and their clients. Art. 90 GDPR also provides for the possibility of establishing such rights of refusal in national law.

28 A deviating provision in Art. 50 para. 2 FADP remains reserved. This only states that professional secrecy is reserved. This reservation was inserted during the parliamentary deliberations (see n. 8 above). This is an emphasis which in itself would not have been necessary, since legal professional secrets are already taken into account via the APA. The reservation of professional secrets already applied under previous law. However, professional secrecy can only be held against the FDPIC if the person protected by professional secrecy does not release the person obliged to cooperate from the obligation of secrecy.

29 Official secrets may not be held against the FDPIC.

30 The persons obliged to cooperate may also not invoke business and trade secrets or contractual secrecy obligations.

31 In the case of informal preliminary investigations prior to the opening of a formal investigation, private persons do not have to provide the FDPIC with any information. Art. 49 para. 3 FADP applies only after formal proceedings have been opened. However, it may make sense for data controllers to cooperate with the FDPIC voluntarily if there is a possibility that the matter can thereby be clarified without the need for formal proceedings.

32 It should be noted that documents provided to the FDPIC in connection with an informal preliminary investigation are subject to the Public Information Act. The informal preliminary investigation does not fall under Art. 3 FoIA. According to its own statement, the FDPIC also cannot guarantee any restriction or refusal of access by third parties under Art. 7 FoIA. Particularly confidential information as well as, for example, personal data of third parties must therefore be processed prior to release. In addition, in the case of particularly confidential information, e.g. information on data security measures, it may be advisable not to provide the information to the FDPIC in writing, but to

present the information to him orally on site during a visual inspection or to show it to him, e.g. on the occasion of a video conference with a split screen.

E. Information of the person concerned (para. 4)

The data subject is not a party to the proceedings (Art. 52 para. 2 FADP e contrario). This also applies if the data subject has filed a complaint. The data subject is therefore not entitled to inspect the files. 33

According to Art. 49 para. 4 FADP, if the data subject has filed a complaint, the FDPIC must at least inform the data subject of his or her further course of action and the outcome of any investigation. 34

The data subject may then assert his or her rights through the applicable legal remedies, i.e., he or she may file a complaint with a civil court if the responsible party is a private person, or he or she may file a complaint against the decision of the responsible federal body. 35

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 50 FADP

A commentary by Reto Fanger / Isabelle Oehri

SUGGESTED CITATION

Reto Fanger/Isabelle Oehri, Kommentierung zu Art. 50 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Fanger/Oehri, N. XXX zu Art. 50 DSG.

Art. 50 Powers

[1] If the federal body or the private person fails to fulfil the duties to cooperate, the FDPIC may as part of the investigation order the following in particular:

a. access to all information, documents, records of processing activities and personal data that are required for the investigation;

b. access to premises and installations;

c. questioning of witnesses;

d. appraisals by experts.

[2] Professional secrecy remains reserved.

[3] In order to enforce the measures under paragraph 1 the FDPIC may request support from other federal authorities and from the cantonal or communal police.

CONTENT

I. PURPOSE OF THE NORM AND HISTORY OF ITS ORIGINS

1 If the FDPIC conducts an investigation into suspected data protection violations by a federal body or a private person, he must in principle provide all the information and documents necessary for the investigation in accordance with Art. 49 para. 3 FADP. In order to ensure that the supervisory activities can be carried out effectively even if the persons responsible do not comply with their obligations to cooperate, Art. 50 FADP grants the FDPIC certain powers of investigation and intervention in order to clarify the facts comprehensively, quickly and precisely.

2 The purpose of Art. 50 FADP is to meet the current and expected future requirements of international law, which Switzerland must comply with as a member state of Convention ETS 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data and as a Schengen state. Article 15 para. 2 lit. a of the Protocol of Amendment of 18 May 2018 to the ETS 108 Convention requires that Member States provide their data protection supervisory authorities with powers of investigation and intervention. Similarly, Art. 47(1) of Directive (EU) 2016/680 provides that EU and Schengen States shall provide for effective investigatory powers for their supervisory authorities, namely the power to obtain access to all personal data processed and to all information necessary for the performance of their tasks.

3 In view of Article 45 of Regulation (EU) 2016/679 (the General Data Protection Regulation, GDPR), according to which a transfer of personal data from the EU to third countries may only be carried out if the third country in question provides an adequate level of protection in accordance with a decision of the European Commission, the Swiss legislator considers the new investigative powers of the FDPIC to be a crucial element in ensuring that the EU upholds its adequacy decision vis-à-vis Switzerland.

4 Compared to the 1992 Data Protection Act (aDSG), Art. 50 FADP clarifies and strengthens the position of the FDPIC. Thus, Art. 27 para. 3 aDSG (in the area of supervision of federal bodies) and Art. 29 para. 3 aDSG (in the private sector) already provided for the possibility of requesting files, obtaining information and having data processing performed within the scope of fact-finding investigations. The persons responsible were obliged to cooperate, subject to

the right to refuse to testify that applies mutatis mutandis under Art. 16 APA (cf. Art. 27 para. 3 aDSG and Art. 34 para. 2 lit. b aDSG). However, if the persons responsible did not cooperate of their own accord, the FDPIC had no direct coercive measures at its disposal to obtain information (e.g. the possibility of seizing information or gaining access to localities, installations or systems even against the will of the person entitled). In the event of a refusal to cooperate by a federal body, the FDPIC could only turn to a higher-level unit with the right to issue instructions to the same; in the private sector, the only option open to him was in fact to file criminal charges for violation of the obligations to cooperate (Art. 34 para. 2 lit. b aDSG). In serious cases of refusal to cooperate by a federal body or a private person, he could also inform the public pursuant to Art. 30 para. 2 aDSG.

The limited investigative powers of the FDPIC under the aDSG have sometimes met with criticism from academics and data protection practitioners. Suggestions to expand the FDPIC's information-gathering powers were also made, for example, by the FADP Revision Support Group in 2014. Accordingly, the strengthening of the position of the FDPIC in its investigative activities is a response to the international requirements (cf. n. 2 f. above) as well as the weaknesses identified by doctrine and practice. 5

Practice will show whether the newly designed regime of the FDPIC's investigative powers, together with its cautiously expanded remedial powers (cf. OK-Fanger/Oehri on Art. 51 FADP), will ensure effective supervisory activity. In addition to the corresponding order of competences, effective supervision in fact also requires that the FDPIC be adequately resourced. In this regard, there has been some criticism in the literature about the resources, which are considered to be too scarce and which, despite an increase that has already taken place, will probably continue to force the FDPIC to proceed according to the principle of opportunity in its supervisory activities in the future. In this regard, the 2018 Schengen evaluators were also critical and recommended that the FDPIC be allocated sufficient financial and human resources to fulfill all of its tasks in the Schengen context. 6

II. RIGHT TO INFORMATION OF THE FDPIC

A. Ordering investigative measures

7 If the FDPIC opens an investigation against a federal body or a private person pursuant to Art. 49 para. 1 FADP because of a suspected data protection violation, it is in principle up to the federal body or the private person concerned to provide the FDPIC with all the information and documents necessary for the investigation (Art. 49 para. 3 FADP). If the person responsible does not comply with the obligations to cooperate under Art. 49 para. 3 FADP, Art. 50 para. 1 FADP grants the FDPIC the authority to order measures to obtain information. The ordering of such measures is subsidiary to the cooperation of the person responsible and thus presupposes that the FDPIC has opened an investigation and has tried in vain to obtain the necessary information and documents.

8 The catalog of possible measures for obtaining information in Art. 50(1) FADP is based on that of Art. 12 APA and is not exhaustive. In particular, the FDPIC may request access to all information, documents, lists of processing activities and personal data required for the investigation (lit. a) as well as to premises and installations (lit. b), and may order the examination of witnesses (lit. c) and expert assessments (lit. d).

9 In order to enable a targeted investigation, the concept of access (Art. 50 para. 1 lit. a and lit. b FADP) must be understood broadly. Thus, access to documents includes not only their inspection, but also their seizure, if necessary. With regard to the access measures in Art. 50 Para. 1 lit. a and lit. b FADP, the regulation is essentially based on the relevant provisions of the FADP (Art. 58 para. 1 lit. e and lit. f FADP). In this context, the information is usually collected by means of a questionnaire and all documents relevant to the investigation are recorded with the records. Pursuant to Art. 12 para. 1 FADP, the directory of processing activities - except in the exceptional cases of Art. 12 para. 5 FADP, which are, however, very extensive in Switzerland as a country of SMEs and therefore probably represent the rule - must be created and maintained by the controller and the processor independently of any data protection investigation. Here, too, the order pursuant to Art. 50 para. 1 FADP thus relates to the inspection and, if necessary, seizure, but not to the proper maintenance. The latter can, if necessary, be the subject of an order under Art. 51 FADP based on the results of the investigation. If necessary, the disclo-

sure of the personal data required for the investigation may also be ordered under Art. 50 para. 1 lit. a FADP. Access to premises and facilities may be necessary if technical and organizational measures (TOM) are the subject of the investigation. By mentioning the examination of witnesses and expert opinions, Art. 50 para. 1 FADP goes further than the GDPR, which does not contain any explicit rules in this regard.

Compared to the aDSG, the exemplary list of possible investigative measures in Art. 50 para. 1 FADP means a selective expansion of the information powers (cf. n. 4 above). However, the essential expansion of the position of the FDPIC with regard to the procurement of information lies primarily in the strengthening of the enforcement mechanisms (cf. below n. 18 ff.). 10

B. Personal and material scope of application

In order for the FDPIC to be able to fulfill his legal supervisory duties, the information gathering rights to which he is entitled must be comprehensively structured. 11

In personal terms, information is primarily obtained from the federal body or private person concerned, but may also include other bodies or persons involved in the data processing in question (e.g. employees, auxiliary persons, agents, outsourcing partners) or third parties who can provide relevant information (e.g. data subjects, authorities, former employees, business partners). Under the aDSG, the group of persons from whom the FDPIC can obtain information in the course of its investigations was already broadly defined. The explicit inclusion of witness hearings and expert opinions in Art. 50 para. 1 FADP now also makes the possible involvement of third parties clear in the text of the law. While the duty of the responsible party to cooperate as a party is based on Art. 49 para. 3 FADP and Art. 13 para. 1 lit. c APA, that of third parties is based on Art. 15 and Art. 17 APA. Rights of refusal applicable in individual cases remain reserved (cf. n. 14 ff. below). 12

The FDPIC's right to information must also be interpreted broadly from a factual point of view. Article 50 para. 1 lit. a FADP specifically mentions all information, documents, lists of processing activities and personal data that are necessary for the investigation. Consequently, the right to information extends to all information in connection with a specific case or of a general nature that is relevant and necessary for a legal assessment of the alleged data 13

protection violation. This includes all documents and information that could possibly say something about whether, when and how the responsible bodies comply with the requirements of data protection law, in particular those that can be used to assess the accuracy of the data, the permissibility of its processing and the observance of the rights of the data subjects. Also covered are, for example, documents and information on personnel, technical and organizational precautions, process, program and system documentation as well as all legal bases (e.g. directives, guidelines, leaflets, contracts) that have to do with the enforcement of data protection provisions.

C. Limits, in particular reservation of professional secrecy

14 The FDPIC's right to information and the corresponding duties to cooperate on the part of federal bodies and private persons against whom an investigation is directed, as well as third parties where applicable, are of course not unlimited. They find their limits in the relevant rights of refusal. In this regard, Art. 49 para. 3 FADP provides that the right to refuse information of federal bodies and private persons is governed by Art. 16 and Art. 17 FADP, unless Art. 50 para. 2 FADP provides otherwise. Art. 16 and Art. 17 APA also apply to third parties.

15 According to the applicable order, which results from the interplay of the FADP and the APA and the partial reference therein to the BZP and the StGB, information and also other cooperation, for example in the form of the surrender of documents, can be refused in any case:

- if the contributor would expose himself or a close person to the risk of criminal prosecution or a serious disadvantage to the honor or would cause a direct pecuniary damage for himself or for the latter (Art. 16 para. 1 APA in conjunction with Art. 42 para. 1 lit. a BZP);
- if the contributor can invoke the protection of sources for media professionals (Art. 16 para. 1 APA in conjunction with. Art. 42 para. 1 lit. abis BZP in conjunction with. Art. 28a StGB);
- if the contributor can invoke a professional secret pursuant to Art. 321 no. 1 SCC and the person entitled to the secret has not consented to the disclo-

sure of the secret (Art. 16 para. 1 APA i.V.m. Art. 42 para. 1 lit. b BZP in conjunction with. Art. 321 no. 1 StGB);

- if it concerns attorney correspondence (Art. 17 APA in conjunction with Art. 51a BZP).

In contrast, invoking manufacturing or trade secrets, contractual confidentiality obligations or official secrecy does not exempt a person from participating in an investigation by the FDPIC. The FDPIC, for his part, is bound by the applicable legal provisions - namely on data protection and the protection of industrial and commercial secrets - and is subject to official secrecy under Article 22 of the Federal Act on Civil Procedure, which, according to the legislator, guarantees the confidential treatment of the information obtained in the course of his investigations. 16

According to the practice under the aDSG, holders of other professional secrets, i.e., for example, persons subject to banking secrecy (Art. 47 BankG), professional secrecy in medical research (Art. 321bis SCC) or postal and telecommunications secrecy (Art. 321ter SCC), could not invoke a right to refuse to cooperate in investigations under data protection law pursuant to Art. 16 para. 2 APA in conjunction with Art. 42 para. 2 BZG. Art. 42 para. 2 BZP. It is questionable whether the explicit reservation of professional secrecy in the new Art. 50 para. 2 FADP changes anything in this regard. This was only inserted during the parliamentary debate. However, according to the view expressed here, the relevant parliamentary debate suggests that the explicit mention of professional secrecy is merely a clarification and does not imply any change in the legal situation and practice. 17

III. PROCEDURAL MATTERS

A. Overview

While the content of the FDPIC's right to information under Art. 50 para. 1 FADP has probably only been expanded in certain respects compared to the old law (cf. n. 7 ff. above), the position of the FDPIC with regard to its enforcement has been significantly strengthened. Under the aDSG, the FDPIC could provide for investigative measures, but could not compulsorily enforce 18

them in the case of an uncooperative counterpart (cf. n. 4 above). The FDPIC's information gathering is now regulated in three stages:

- Primarily, it takes place through an informal request by the FDPIC to the federal body or the private person against whom an investigation has been opened. Pursuant to Art. 49 (3) FADP, the person responsible is obliged to provide information and hand over documents, insofar as this is necessary for the investigation, if he or she cannot assert a right to refuse to cooperate.
- Subsidiarily, i.e. if obtaining information solely by means of providing information and handing over documents by the federal body concerned or the private person concerned is either unsuccessful or insufficient, the FDPIC may "order" investigative measures pursuant to Art. 50 para. 1 FADP (cf. on this point n. 19 ff. below).
- Finally, the FDPIC may involve other federal authorities as well as the cantonal or communal police authorities in the enforcement of the measures ordered under Art. 50 para. 1 FADP pursuant to Art. 50 para. 3 FADP.

B. Term "order"

19 The law and also the materials do not explicitly comment on what is meant by the term "order" or in what form this order must be made. Whereas in the context of the administrative measures that the FDPIC can issue on the basis of Art. 51 FADP after the conclusion of an investigation, both the dispatch and the reception of the new provision in the literature prominently address the FDPIC's authority to issue orders (cf. OK-Fanger/Oehri on Art. 51 FADP, n. 1 ff.), with regard to the investigative measures under Art. 50 FADP, there is no discussion of the question of whether their order also has the character of an order or whether it is to be qualified as an official act.

20 The provisions of the FADP applicable to the investigation procedure under Article 50 FADP by virtue of the reference in Article 52 para. 1 FADP, in particular Articles 12-19 FADP, as well as Articles 37, 39-41 and 43-61 FADP, which are also applicable by virtue of the further reference in Article 19 FADP and which are all relevant to the determination of the facts in administrative proceedings, do not expressly determine the form in which investigative measures are to be ordered.

According to the view expressed here and explained in detail below, the ordering of investigative measures must take the form of a procedural (interim) order. 21

Unlike in the area of civil procedure, actual evidence orders are not common in administrative proceedings, in which the investigative maxim prevails. However, evidentiary or investigative measures are generally ordered in the form of injunctions in many administrative areas. Although the case law hardly deals in detail with the legal nature of the orders in question, in most of these decisions the ruling court assumes an order without further ado in the considerations on the object of challenge. 22

In decisions in which the Federal Supreme Court had to deal specifically with the question of whether the order of an investigative measure in a specific case qualifies as a (contestable) order or not, the picture is not uniform: sometimes a corresponding order is classified as a procedural interim order, sometimes as a real act of the authorities. In its more recent case law, the Federal Supreme Court seems to increasingly assume the character of an injunction. However, no general statements for all administrative areas can be derived from this. 23

With reference to the fact that the ordering of evidence measures under the duty to cooperate always creates a legal obligation, the doctrine argues - rightly in the view represented here - for a qualification as an order. In some cases, a distinction is made as to whether the fulfillment of the duty to cooperate can be enforced by sanctions (direct coercion, fines, etc.). Insofar as this is provided for by law and thus a genuine legal obligation is to be assumed, an order to cooperate in this regard is to be structured as an interim order if the threat to cease and desist is so specific that it can be enforced. 24

If an administrative act strongly interferes with the legal position of the addressee, an injunction is appropriate so that the addressee can, if necessary, arrange for a review by an appellate body. The federal body or the private person as a party to an investigation under data protection law is likely to disagree with the ordering of investigative measures on a regular basis: After the responsible party was unwilling or unable to provide the FADP with the necessary information basis for the assessment of a possible data protection violation in the context of the informal inquiry by the FDPIC, it can be assumed that he will not suddenly be able or willing to cooperate sufficiently of his own 25

accord, even in response to an order pursuant to Art. 50 para. 1 FADP. In view of the right to be heard, it is all the more important for him to have the possibility of having the disputed order reviewed by the courts under the conditions of Art. 52 para. 1 FADP in conjunction with 46 APA. In addition, the FDPIC can enforce the ordered investigative measures, insofar as they can be compulsorily enforced, with the help of other federal authorities and the cantonal and municipal police authorities in accordance with Art. 50 para. 3 FADP. Failure to cooperate is punishable under Art. 60 FADP. In other words, investigative measures under Art. 50 para. 1 FADP regularly give rise to real legal obligations for the party to the proceedings, which is why they must be ordered by decree.

26 The same applies analogously to the obligation of third parties to cooperate, which can be enforced (Art. 50 para. 3 FADP) and non-compliance with which may also result in penalties (Art. 52 para. 1 FADP in conjunction with Art. 60 APA). If they are summoned as witnesses or requested to edit documents or grant access to premises and installations, this constitutes a substantial interference against which a legal remedy must be available before compulsory enforcement or sanctioning of non-cooperation.

27 From the perspective of procedural economy, it can admittedly be objected that, depending on the circumstances of the individual case, the ordering of investigative measures by decree can lead to very lengthy and costly investigative proceedings. However, this is acceptable for reasons of the rule of law. No excessive requirements are to be placed on the justification of investigative measures by the FDPIC, so that an order in the form of a decree does not lead to a significant additional expense compared to a purely real act. There is a risk of delay in the procedure if an independent appeal is possible (Art. 52 para. 1 FADP in conjunction with Art. 46 para. 1 APA), which in the present context will only be the case in exceptional cases (see in detail below n. 28). In addition, the FDPIC may withdraw the suspensive effect of an appeal if necessary (Art. 52 para. 1 FADP in conjunction with Art. 55 para. 2 APA). Finally, especially in the case of complex investigations with a long duration of proceedings, the precautionary ordering of administrative measures pursuant to Art. 51 FADP may sometimes be necessary (cf. OK-Fanger/Oehri on Art. 51 FADP, n. 22 ff.).

C. Legal remedy

If the order for investigative measures is deemed to be of an injunctive nature, it may be appealed under the conditions of Art. 52 para. 1 FADP in conjunction with Art. 46 para. 1 VwG. Art. 46 para. 1 APA, it can be challenged independently by appeal to the Federal Administrative Court. 28

Primarily, a challenge is likely to exist if the order may cause irreparable disadvantage within the meaning of Art. 46 para. 1 lit. a APA. This is the case if objections are raised against the ordered evidence measures which cannot be raised without disadvantage by challenging the final decision. Art. 46 para. 1 lit. b APA, according to which the appeal is also admissible if its approval would immediately bring about a final decision and thus save a significant amount of time or costs for extensive evidentiary proceedings, will hardly be relevant with regard to investigative measures under data protection law. 29

Where an appeal is admissible, the decision of the Federal Administrative Court can subsequently be appealed to the Federal Supreme Court by means of an appeal in public law matters (Art. 82 lit. a in conjunction with Art. 86 para. 1 lit. a BGG). In addition to the addressee of the order, the FDPIC also has the right of appeal (Art. 52 para. 3 FADP). 30

D. Enforcement

Art. 50 para. 3 FADP provides that the FDPIC may involve other federal authorities as well as the cantonal or municipal police authorities in the enforcement of the measures under Art. 50 para. 1 FADP. Art. 54 para. 2 lit. c FADP also states in this regard that the FDPIC may disclose to the authorities consulted the information and personal data necessary for the performance of their legal duties. 31

Article 50 (3) FADP was amended during the legislative process. Still in the FADP of 2017, the provision in question explicitly granted the FDPIC the power to order precautionary measures for the duration of the investigation and to have them enforced by a federal authority or the cantonal or municipal police bodies (Art. 44 para. 2 FADP [2017]). The final version of the provision no longer contains any direct mention of precautionary measures (cf. on the possibility of ordering precautionary measures during the duration of a data protection investigation, OK-Fanger/Oehri on Art. 51 FADP, n. 22 ff.). 32

33 With regard to enforcement, the rules of the FADP, in particular Art. 39-43 of the APA, also apply in addition, in accordance with the reference in Art. 52 para. 1 FADP, unless Art. 50 FADP provides otherwise. Consequently, enforcement requires that no legal remedy with suspensive effect is available against the order (Art. 52 para. 1 FADP in conjunction with Art. 39 APA). With regard to the possible means of coercion (cf. Art. 52 para. 1 FADP in conjunction with Art. 41 APA), coercive access and searches of premises and installations as well as the seizure of installations, documents, lists of processing activities and personal data will primarily play a role in practice. A threat of punishment may also come into consideration (cf. Art. 60 FADP and Art. 52 para. 1 FADP in conjunction with Art. 60 APA). In contrast, the compulsory production of parties to provide information or of witnesses should hardly ever be considered, especially since the principle of proportionality always applies with regard to the means of compulsion used (Art. 52 para. 1 FADP in conjunction with Art. 42 APA).

E. No fee

34 Art. 59 para. 1 lit. d FADP stipulates that the FDPIC shall charge a fee to private persons for the issuance of precautionary measures and (administrative) measures under Art. 51 FADP. With regard to the investigation procedure, this means e contrario that no fees are to be imposed on a federal body in any case in the absence of a corresponding legal basis. Moreover, according to the dispatch on the FADP (2017), it should be concluded that no fees are charged for investigations against private persons that are concluded without ordering precautionary measures or administrative measures.

35 The envisaged exemption from fees is convincing for investigation proceedings in which the clarification of the facts is formally simple, i.e. can be carried out without a formal order of investigative measures solely through the cooperation of a fully cooperating responsible party, and on the other hand has an exculpatory effect, i.e. does not lead to administrative measures. Likewise, it can be argued that the ordering of investigative measures on third parties, insofar as these were not first made necessary by a lack of cooperation on the part of the data controller, should not entail any financial consequences for the latter. However, Art. 50 FADP is not only tailored to such case constellations, but also applies in particular if the data controller does not sufficiently cooperate in the investigation procedure (cf. Art. 50 para. 1 FADP). According

to the opinion expressed here, the ordering of investigative measures, which became necessary solely because the responsible party unjustifiably failed to comply with his or her duties to cooperate, should in any case have cost consequences in the private sector, even if, after the investigation has been fully conducted and opened in response to sufficient indications pursuant to Art. 49 para. 1 FADP, it turns out that there has been no violation of data protection provisions and thus no administrative measures need to be ordered pursuant to Art. 51 FADP.

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 51 FADP

A commentary by Reto Fanger / Isabelle Oehri

SUGGESTED CITATION

Reto Fanger/Isabelle Oehri, Kommentierung zu Art. 51 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Fanger/Oehri, N. XXX zu Art. 51 DSG.

Art. 51 Administrative measures

[1] If data protection regulations have been violated, the FDPIC may order that the processing be modified, suspended or terminated, wholly or in part, and the personal data deleted or destroyed, wholly or in part.

[2] It may delay or prohibit disclosure abroad if this violates the requirements of Article 16 or 17 or provisions relating to the disclosure of personal data abroad in other federal acts.

[3] It may in particular order that the federal body or the private person:

a. provide him or her with information in accordance with Articles 16 paragraph 2 letters b and c and 17 paragraph 2;

b. take the measures in accordance with Articles 7 and 8;

c. inform the data subjects in accordance with Articles 19 and 21;

d. conduct a data protection impact assessment in accordance with Article 22;

e. consult him or her in accordance with Article 23;

f. provide him or her or, if applicable, the data subject with information in accordance with Article 24;

g. provide the data subject with the information specified in Article 25.

[4] It may also order that private controllers with registered office or domicile abroad appoint a representative in accordance with Article 14.

[5] If the federal body or the private person has taken the required measures during the investigation in order to restore compliance with the data protection regulations, the FDPIC may simply issue an official warning.

CONTENT

I. PURPOSE OF THE NORM AND HISTORY OF ORIGINS

1 Art. 51 FADP describes the administrative measures that the FDPIC may issue in the event of a violation of data protection provisions. The authority granted to the FDPIC in Art. 51 FADP is a novelty in the new data protection law. With this expansion of the powers of the FDPIC, the legislator is responding to the suggestions of the 2014 Schengen evaluators, who had criticized the fact that under the old Data Protection Act of 1992 (aDSG), the FDPIC could only issue recommendations. The 2018 Schengen evaluation also recommended strengthening the enforcement powers of the FDPIC so that it can take legally binding decisions directly. Art. 51 FADP largely implements Art. 47(2) of Directive (EU) 2016/680, specified in Art. 58(2) of Regulation (EU) 2016/679 (General Data Protection Regulation, FADP). Likewise, the requirements of Art. 15 para. 2 lit. c of the Protocol of Amendment of 18 May 2018 to Council of Europe Convention ETS 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data are thus largely fulfilled.

2 In contrast, the FADP revision refrained from expanding the sanctioning powers of the FDPIC beyond the injunctive powers, despite a recommendation to this effect by the European Union and despite a corresponding mention in Art. 15 para. 2 lit. c of the Protocol of Amendment of 18 May 2018 to the ETS 108 Convention. In contrast to the data protection authorities of various other countries - such as the supervisory authorities in the territorial scope of the GDPR - the FDPIC thus continues to be unable to impose administrative sanctions on federal bodies in particular. In the case of private persons, the FDPIC also has no direct sanctioning power, but at least various breaches of duty are made punishable here in the 8th chapter of the FADP. Namely, the FDPIC can attach a threat of punishment to its orders of administrative measures under Art. 51 FADP against private persons under Art. 63 FADP. In the opinion of the legislator, this two-tier system is more in line with Swiss legal tradition than a direct sanctioning competence of the FDPIC and is effective enough.

3 Unlike under the new regime, the FDPIC had no competence to issue legally binding measures under the aDSG. If, in the course of an investigation against a federal body or a private person, it found a violation of data protection regulations, it could only issue a recommendation to the person responsible to change or refrain from data processing (Art. 27 para. 4 aDSG [for federal bod-

ies] or Art. 29 para. 3 aDSG [for private persons]). If the person responsible opposed the recommendation of the FDPIC by formally rejecting it or simply not complying with it in fact, the FDPIC had to submit his recommendation to the department or the Federal Chancellery (in the public sector) or directly to the Federal Administrative Court (in the private sector) in order to obtain a legally binding assessment. The decision subsequently issued by the department or the Federal Chancellery could then also be appealed to the Federal Administrative Court by the federal body concerned and - since the introduction of a corresponding right of appeal with the 2006 revision of the FADP - also by the FDPIC. In the final instance, the decisions of the Federal Administrative Court could be appealed to the Federal Supreme Court in public and private matters (Art. 82 lit. a in conjunction with Art. 86 para. 1 lit. a BGG). In addition to this multi-stage formal route via the recommendation and its possible referral, the FDPIC was able to lend de facto weight to its non-binding orders by informing the Federal Assembly and Federal Council and by publication with a corresponding reputational effect (Art. 30 aDSG).

In practice under the aDSG, the FDPIC issued only a few recommendations, both in the private and especially in the public sector; enforcement by way of complaint was even rarer. Frequently, the responsible parties already took the necessary measures to remedy the disclosed abuses in the course of the investigation procedure with the help of advice from the FDPIC (Art. 28 and Art. 31 Para. 1 lit. aDSG). If the FDPIC nevertheless made a recommendation once, this was generally followed without further ado. 4

Nevertheless, the lack of authority of the FDPIC to impose effective measures and, if necessary, also sanctions, has been and continues to be criticized in doctrine and data protection practice. In the political and legislative debate on the aDSG, corresponding weaknesses were also identified and a possible strengthening of the position of the FDPIC was discussed. However, opinions differed as to the concrete form this stronger position should take and in particular on the question of whether the FDPIC should have sanctioning powers. For example, in 2014, a parliamentary initiative calling for the introduction of administrative sanctioning powers for the FDPIC was not followed. The moderately restrained expansion of the position of the FDPIC undertaken with the revision of the FADP reflects the opinion in politics, doctrine and practice as well as the pressure due to international requirements (cf. n. 1 f. above). 5

6 Practice will show whether the newly designed regime, with the FDPIC's powers to issue orders but without direct sanctioning powers, will ensure effective supervisory activity. In addition to the appropriate division of powers, effective supervision also requires that the FDPIC be adequately resourced. In this regard, there has been some criticism in the literature of the resources, which are considered to be too scarce and which, despite an increase that has already taken place, will probably continue to force the FDPIC to proceed according to the principle of opportunity in its supervisory activities in the future. In this regard, the 2018 Schengen Evaluators were also critical and recommended that the FDPIC be allocated sufficient financial and human resources to fulfill all of its tasks in the Schengen context.

II. ADMINISTRATIVE MEASURES

7 Article 51 of the FADP gives the FDPIC wide latitude: if there is a breach of data protection rules, it may order measures aimed at remedying the unlawful situation, but it is not obliged to do so. The list of measures is not exhaustive. When deciding whether an order is to be issued and, if so, which, the principle of proportionality applies: those measures are to be ordered which are necessary to (re)ensure the lawfulness of the data processing in the specific individual case. The principle of proportionality is also explicitly anchored in Art. 51 (5) FADP: If the federal body or the private person has already taken the necessary measures during the investigation to restore compliance with data protection regulations, Art. 51 (5) FADP provides that the FDPIC may limit himself to issuing a warning. Furthermore, in view of the design of Art. 51 FADP as an optional provision, it should also be possible, in the interest of a targeted practice appropriate to the individual case, according to the view represented here, for the FDPIC to limit himself in the case of minor deficiencies to giving the responsible parties advice on how to remedy the deficiencies within the scope of his advisory activities (Art. 58 para. 1 lit. a FADP), instead of issuing an order for measures. It is to be expected that the FDPIC, if only for reasons of efficiency, will work towards ensuring that data controllers take the measures necessary to restore the lawfulness of the data processing without being forced to issue an order.

8 The FDPIC's power to issue an injunction pursuant to Art. 51 FADP is very broad in terms of content. It is limited only, but at least, by the fact that it is dependent on the violation of data protection provisions: the FDPIC cannot,

of course, order anything different or more extensive than would be required by the legal data protection provisions anyway.

The measures listed in Art. 51 FADP can be divided into two categories: Paragraphs 1, 2 and 4 provide for measures against data processing that violates data protection regulations. Para. 3 contains accompanying measures in the event of violations of regulatory provisions or obligations towards the data subject. The FDPIC may, if necessary, impose a penalty on administrative measures ordered against private individuals in accordance with Art. 63 FADP (cf. n. 2 above). 9

A. Measures against data processing in violation of data protection regulations (Art. 51 para. 1, 2 and 4 FADP)

The first category of measures covers data processing operations that violate data protection regulations and is aimed at restoring compliance with the violated regulations. Depending on the constellation, the FDPIC may issue the necessary orders pursuant to Art. 51 para. 1, 2 or 4 FADP. 10

In the sense of a general clause, Art. 51 para. 1 FADP grants the FDPIC the power, with regard to data processing that violates data protection regulations, to order a partial or complete adjustment, interruption or termination as well as the partial or complete deletion or destruction of the personal data concerned. 11

In addition, Art. 51 para. 2 and para. 4 FADP separately regulate two specific cases of data processing in breach of data protection regulations, namely the unlawful disclosure of data abroad and the failure to designate a Swiss representation for foreign data processors in accordance with Art. 14 FADP. 12

In the event of data being disclosed abroad in violation of the regulations, the FDPIC may order its suspension or prohibition (Art. 51 para. 2 FADP). This covers violations of Art. 16 and Art. 17 FADP, which regulate the export of data from Switzerland, and violations of provisions concerning the disclosure of personal data abroad in other federal laws. The inclusion of violations of other federal laws was left unchanged despite corresponding criticism in the consultation. In practice, however, it is likely to have little independent significance, since such data exports regularly violate the principle of the lawfulness of data processing (Art. 6 para. 1 FADP) and could thus also be subsumed under the general clause of Art. 51 para. 1 FADP. 13

14 In the event of a violation of Art. 14 FADP, the FDPIC may order the designation of a Swiss representation by private data controllers domiciled or headquartered abroad (Art. 51 para. 4 FADP).

B. Accompanying measures in the event of violations of regulatory provisions or obligations towards data subjects (Art. 51 para. 3 FADP)

15 The second category of measures is directed against cases in which regulatory provisions or obligations towards data subjects are not observed. It is not necessary that a data protection breach has occurred. Art. 51 para. 3 FADP contains a non-exhaustive list of possible orders. These should be read in conjunction with the obligations imposed on federal bodies and private persons by the second and third chapters of the FADP.

16 The majority of the measures listed in Art. 51 para. 3 FADP are information and consultation orders requiring the controller to inform or consult the FDPIC and/or the data subjects regarding specific operations (Art. 51 para. 3 lit. a, c, e, f and g FADP). Specifically, the FDPIC may request data controllers to do so by means of an order,

- to inform him in advance of the relevant clauses or guarantees, if data disclosure abroad is planned without adequate protection within the meaning of Art. 16 para. 1 FADP and data protection is to be ensured by means of contractual data protection clauses pursuant to Art. 16 para. 2 lit. b FADP or by means of specific guarantees drawn up by the competent federal body (Art. 16 para. 2 lit. c FADP) (Art. 51 para. 3 lit. a FADP);
- to inform him in accordance with Art. 17 para. 2 FADP about cases of data disclosure abroad that fall under the exemption rules of Art. 17 para. 1 lit. b no. 2, lit. c and lit. d FADP (Art. 51 para. 3 lit. a FADP);
- comply with its obligations to inform the data subjects when obtaining personal data (Art. 19 FADP) and when making automated individual decisions (Art. 21 FADP) (Art. 51 para. 3 lit. c FADP);
- to consult him pursuant to Art. 23 FADP in cases where a data protection impact assessment carried out still reveals a high risk to the personality or

fundamental rights of the data subjects despite the protective measures provided (Art. 51 para. 3 lit. e FADP);

- to report data security breaches to it in accordance with Art. 24 FADP and, under the conditions of Art. 24 para. 4 and 5 FADP, to inform the data subjects thereof (Art. 51 para. 3 lit. f FADP);
- to comply with its duty to provide information to the data subjects in accordance with Art. 25 FADP (Art. 51 para. 3 lit. g FADP).

The other measures listed in lit. b and d of Art. 51 para. 3 FADP are orders for action. Consequently, the FDPIC may request data controllers by means of an order to, 17

- to take the necessary technical and organizational measures (TOM) for data processing, in compliance with data protection regulations (Art. 7 para. 1 and 2 FADP), and to ensure adequate data security in accordance with Art. 8 FADP and Art. 1 et seq. FADP (Art. 51 para. 3 lit. b FADP);
- to use data protection-friendly default settings in accordance with Art. 7 para. 3 FADP (Art. 51 para. 3 lit. b FADP);
- to carry out a data protection impact assessment in accordance with Art. 22 FADP (Art. 51 para. 3 lit. d FADP).

III. PROCEDURAL LAW

A. General

The measures are issued by the FDPIC as an order: In procedural terms, the provisions of the FADP apply in principle to administrative measures under Art. 51 FADP (Art. 52 para. 1 FADP). Pursuant to Art. 52 para. 2 FADP, only the federal body or the private person against whom an investigation has been opened has party status. The persons affected by a data processing operation are therefore not parties, even if the investigation was initiated by their notification under Art. 49 para. 1 FADP. In principle, the FDPIC issues his rulings exclusively to the addressees. Only in cases of general interest does he inform the public (Art. 57 para. 2 FADP). The FDPIC must give sufficient reasons for his rulings so that the persons responsible are in a position to evaluate and implement the measures ordered or to lodge an appeal against them. In other words, the content of the order must in each case be a concrete instruction 18

for action, which can be enforced as such. Blanket orders stating that the addressee of the order must adapt its data processing in such a way that it complies with the data protection requirements of the FADP would therefore not be precise enough. If no measures are ordered after an investigation or if only a warning is issued in accordance with Art. 51 para. 5 FADP, the investigation procedure must nevertheless be formally concluded by the FDPIC.

19 Decisions on measures by the FDPIC pursuant to Art. 51 FADP may be contested by the federal body or the private person against whom they are directed by means of an appeal to the Federal Administrative Court in accordance with the general rules of the administration of federal justice (cf. Art. 52 para. 1 FADP in conjunction with Art. 44 ff. APA). Appeal decisions of the Federal Administrative Court are subject to appeal in public law matters to the Federal Supreme Court (Art. 82 lit. a in conjunction with Art. 86 para. 1 lit. a BGG). In addition to the addressee of the order, the FDPIC also has the right of appeal (Art. 52 para. 3 FADP). In the absence of party status (cf. Art. 52 para. 2 FADP and n. 18 above), however, the data subjects are not entitled to lodge appeals against decisions of the FDPIC and against appeal decisions.

20 With regard to the enforcement of the administrative measures ordered, Articles 39-43 of the FADP apply in addition pursuant to the reference in Article 52 para. 1 of the FADP.

21 Unlike under the aDSG, under which no fees could be imposed on the person responsible for issuing a recommendation (cf. Art. 33 aVDSG), Art. 59 para. 1 lit. d FADP now provides that a fee may be charged to private persons for ordering measures under Art. 51 FADP (cf. also Art. 44 FADP). No fee continues to be charged for orders against federal bodies in the absence of a corresponding legal basis (Art. 59 para. 1 lit. d FADP e contrario; cf. 2017 Dispatch, p. 7098).

B. Precautionary measures

22 In the FADP of 2017, it was envisaged that a paragraph in the article concerning the investigation procedure would explicitly empower the FDPIC to order precautionary measures for the duration of the investigation and to have them enforced by a federal authority or the cantonal or municipal police bodies (Art. 44 para. 2 FADP [2017]). However, after Parliament deleted this paragraph from Art. 50 FADP, the final version of Art. 44 E-FADP, the FADP no

longer directly grants the FDPIC the authority to issue precautionary orders for the duration of its investigations. Now the competence of the FDPIC to issue precautionary measures arises only indirectly from the article on fees, which in Art. 59 para. 1 lit. d FADP declares the issuance of precautionary measures by the FDPIC against private persons to be subject to a fee. As was already the case under the aDSG, however, the ordering of provisional or even superprovisional measures in the context of investigations under data protection law must be possible in any case; the deletion of the provision in question must be interpreted as a legislative oversight and not as a qualified silence.

Whereas under the old law the FDPIC had to appeal to the Federal Administrative Court (Art. 33 para. 2 aDSG) for the issuance of provisional measures due to the lack of its own competence to issue such orders, it can now issue them itself. 23

However, Article 32 para. 2 aDSG, which is no longer applicable under the new law, not only assigned jurisdiction to the Federal Administrative Court to issue precautionary measures in the context of data protection investigations, but also regulated the requirements and procedure. In the former context, Art. 33 para. 2 aDSG required that the data subjects be threatened with damage that cannot be easily remedied. Procedurally, the provision declared Art. 79-84 BZP to be applicable mutatis mutandis. 24

After the omission of Art. 33 para. 2 aDSG, there are now no explicit prerequisite and procedural rules for interim legal protection. As a result, however, there should be little change in the substantive assessment of provisional measures in data protection investigations. The FADP, which is applicable to the investigation procedure pursuant to Art. 52 para. 1 FADP, only contains provisions on the issuance of precautionary measures in the appeal procedure (cf. in particular Art. 55 and Art. 56 FADP), but not in the upstream administrative procedure. However, the admissibility of precautionary measures in administrative proceedings is recognized, since it results directly from the requirement to enforce substantive law. For the adoption of precautionary measures by the FDPIC in the investigation procedure, it is a prerequisite that a disadvantage that cannot be easily remedied is to be expected. Unlike under the aDSG, according to the view expressed here, this disadvantage does not necessarily have to threaten the persons affected by the data processing, even if in practice it will probably regularly be located with them. Furthermore, 25

there must be a corresponding urgency for the immediate order and it must appear suitable, necessary and proportionate based on the overall circumstances in order to protect overriding public or private interests. As provisional orders, provisional measures may neither prejudice nor render impossible the state of affairs that is ultimately to be regulated. At the time when provisional orders are under discussion, the outcome of the data protection investigation is usually still uncertain and only a summary examination of the factual and legal situation can take place. Accordingly, although a prognosis of the main case must be made in the course of the examination of precautionary measures, this only stands in the way of a provisional order if it is clearly negative.

26 In terms of content, the orders are likely to be based on the catalog of administrative measures under Art. 51 FADP. It will often be a question of using provisional orders to prohibit potentially data-protection-infringing data processing for the duration of the proceedings, in order to avoid additional damage that could result from the unchanged continuation of the processing in question during a sometimes complex and lengthy investigation.

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 52 FADP

A commentary by Nicolas Winkelmann

SUGGESTED CITATION

Nicolas Winkelmann, Commentary to art. 52 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Winkelmann, art. 52 FADP N. XXX.

Art. 52 Procedure

[1] The investigation proceedings and rulings under Articles 50 and 51 are governed by the APA.

[2] The only party is the federal body or the private person against which or whom an investigation has been opened.

[3] The FDPIC may contest appeal decisions of the Federal Administrative Court.

CONTENT

IN A NUTSHELL

Art. 52 para. 1 FADP sets out the rules governing the formal proceedings of the Federal Data Protection and Information Commissioner (FDPIC). The provision is a reference provision and stipulates that investigations pursuant to Art. 49 FADP and decisions pursuant to Art. 50 and 51 FADP are governed by the rules of the APA. Conversely, other actions of the FDPIC are not subject to the APA, namely informal preliminary investigations, low-threshold interventions, or advisory and supervisory activities. It is noteworthy that reference is also made to the APA for proceedings against federal bodies and that the FDPIC can "issue decisions" against federal bodies in accordance with the rules of the APA. 1

Paragraph 2 stipulates that only the federal body or private individual against whom an investigation has been initiated has party status. This restricts the circle of possible parties in formal proceedings of the FDPIC compared to the provisions of the APA. 2

Paragraph 3 provides the legal basis for the FDPIC's right of appeal to the Federal Supreme Court against decisions of the Federal Administrative Court. 3

I. GENERAL INFORMATION ON THE PROCEDURE

Based on the aDSG, the FDPIC conducted so-called fact-finding investigations from 1993 to 2023, which it concluded with a final report and recommendations. Due to the FDPIC's lack of decision-making authority, the APA did not apply to these proceedings. If such a **recommendation by the Commissioner** was not followed or was rejected, the FDPIC could refer the matter to the Federal Administrative Court for a decision. 4

With the total revision of the FADP, which came into force on September 1, 2023, the FDPIC was given new decision-making powers, which is why it has been concluding formal proceedings with a decision since the revised FADP came into force. On International Data Protection Day in January 2025, the FDPIC published its first interim report in figures. According to this report, the FDPIC received a total of 1,406 reports of violations of the FADP between 5

September 1, 2024, and January 21, 2025, of which 479 were pending at the time of publication. The **supervisory activities** were distributed as follows:

- Low-level interventions: 116
- Of these, voluntarily complied with by the responsible parties: approx. 90%
- Preliminary investigations: 16
- Open investigations / pending before the Federal Administrative Court: 8 / 2
- Campaigns 2

6 The published figures show that supervisory measures taken by the FDPIC only lead to the opening of a formal investigation in isolated cases and that **low-level intervention is the main instrument of supervision**. In practice, therefore, the FDPIC usually takes action after receiving a complaint without opening a formal investigation.

7 The prerequisite for **opening an investigation** is laid down in Art. 49 para. 1 FADP. According to this, the FDPIC shall initiate an investigation ex officio or upon complaint if there are sufficient indications that data processing may violate data protection provisions. As soon as the FDPIC initiates an investigation under Art. 49 FADP, the APA applies. This is the case as soon as it has decided internally to initiate proceedings. This may occur before the FDPIC takes any informal action, during or after such action.

8 In practice, the parties are notified of the initiation of proceedings by means of a **letter of notification**. The initiation of proceedings does not constitute a decision that can be challenged. Finally, the proceedings are concluded or discontinued by means of a decision in accordance with Art. 51 FADP.

9 From the perspective of the controller, it is important to know whether or not proceedings have been initiated. Once proceedings have been initiated, the parties are subject to a **duty to cooperate** (Art. 60 para. 2 FADP), which is punishable by law. Conversely, cooperation is not mandatory before an investigation is initiated. However, if the controller refuses to cooperate or cooperates insufficiently in the context of a preliminary investigation or low-threshold intervention, the requirements of Art. 49 para. 1 FADP are generally met,

so that the facts can be established on the basis of the obligation to cooperate (Art. 49 para. 3 FADP) or with the aid of coercive measures (Art. 50 para. 1 FADP). The FDPIC may charge fees for such actions (Art. 59 para. 1 lit. d FADP), which is why it is generally in the interest of the controller to cooperate voluntarily with the FDPIC before an investigation is opened.

The principle of the **right to be heard**, which is enshrined in Art. 29 para. 2 FC and specified in Art. 29 ff. APA, guarantees the parties a personal right to participate in the proceedings. They must be given the opportunity to comment on the matter before a decision is made, to provide relevant evidence, to participate in the collection of evidence, or at least to comment on the results of the evidence. In other words, the party concerned must be given the opportunity to comment on the essential points before a decision is made. This primarily includes the legally relevant facts of the case. Accordingly, parties may only comment on the facts of the case before a decision is issued; however, the right to be heard does not extend to the intended legal assessment. Only in exceptional cases – for example, if the FDPIC intends to apply unexpected special provisions – may the right to be heard also cover the applicable provisions and the intended legal reasoning. The FDPIC's legal assessment is disclosed to the parties in the reasoned decision. If a party disagrees with the FDPIC's legal reasoning, it may lodge an appeal. 10

II. REFERENCE TO THE APA (PARA. 1)

A. Proceedings under the APA against private individuals

The APA is applicable to proceedings of the FDPIC in which it issues a decision in the first instance, based on Art. 1 para. 1 and para. 2 lit. c APA. There is no exception under Art. 2 ff. APA. Art. 52 para. 1 FADP therefore constitutes a **declaratory reference provision** vis-à-vis private individuals and serves to clarify the situation. 11

B. Proceedings under the APA against federal bodies

Before the total revision of the FADP, supervision of federal bodies and private individuals was regulated in two separate provisions, with the conditions for opening an investigation differing in particular. In the revised FADP, the investigation of violations of data protection provisions is now regulated in a single section (Art. 49 ff.) for federal bodies and private individuals. It is note- 12

worthy that, with a few minor exceptions, **no different rules have been legislated for proceedings against federal bodies or private individuals**.

13 According to established case law and doctrine, decisions within the meaning of Art. 5 APA are authoritative, unilateral, individually specific orders issued by an authority in application of administrative law, which are intended to have legal effects and are binding and enforceable. The procedure for issuing a decision presupposes a relationship of authority between an authority and a private individual. Orders issued by the FDPIC to other federal bodies therefore do not fulfill all the structural characteristics of the concept of a decision due to the lack of a relationship between the authority and the private individual. Therefore, insofar as the FDPIC conducts proceedings against a federal organ, the proceedings are governed by the APA pursuant to Art. 49 FADP, whereby Art. 52 para. 1 FADP corresponds to a **constitutive reference provision** in this area and the provisions of the APA apply *mutatis mutandis*.

14 The **authority of the FDPIC to issue orders against federal bodies** derives, on the one hand, from the wording of numerous legal provisions, which expressly refer to federal bodies and private individuals and also make a sensible distinction between federal bodies and private individuals. On the other hand, the legislature deliberately harmonized the procedures against private individuals and federal bodies, which were still different under the old law. Finally, the legislature brought the investigative powers and administrative measures into line with European requirements in order to ensure that the European Commission renews or maintains its adequacy decision with regard to Switzerland, which is of central importance for the Swiss economy in particular.

15 Apart from the FDPIC, there is no other administrative unit that can issue orders to other administrative units in accordance with the rules of the APA. The **Federal Audit Office**, as a comparable supervisory authority, can also request and enforce measures against other federal authorities that are not hierarchically subordinate to it, but not in accordance with the rules of the APA.

16 In our view, an order issued by the FDPIC pursuant to Art. 51 FADP against federal bodies corresponds to a **"quasi-decision"** because, on the one hand, the substantive requirements for a decision pursuant to Art. 5 APA are not met, but on the other hand, federal bodies are *mutatis mutandis* subject to the same rights and obligations as private addressees of decisions. With the con-

stitutive reference provision, the legislature has pragmatically regulated the procedural rules under which the FDPIC, as the supervisory authority, can conduct investigations against federal bodies and issue and enforce binding orders.

It is noteworthy that the **draft bill on the revision of the Data Protection Act** of 2014 still differentiated between investigations against private individuals and federal bodies. It proposed a model whereby the FDPIC would first issue a recommendation to federal bodies and only issue an order if this was rejected or not complied with. This option delays the procedure through unnecessary intermediate steps. The explanatory report on the preliminary draft for the total revision of the FADP of 2016 no longer distinguishes between proceedings against private individuals and federal bodies. 17

Proceedings by the FDPIC against federal bodies under Art. 49 FADP must be distinguished from **administrative assistance**. Federal authorities that cooperate within the framework of administrative assistance are organizationally equal, which is why there is no relationship of subordination between them and cooperation is based on partnership. If the FDPIC initiates proceedings against a federal body on the basis of Art. 49 FADP and requests documents from the federal body under investigation, this does not fall under administrative assistance, which is why Art. 36a VGG is not applicable. In proceedings, federal authorities under investigation are subject to a duty to cooperate, which creates a relationship of subordination in such cases, as this is the only way in which the FDPIC can effectively monitor and enforce compliance with data protection regulations by federal authorities. 18

The analogous application of the provisions of the APA to proceedings against federal bodies leads in particular to the following differences in comparison with proceedings against private individuals: 19

According to the wording of Art. 60 para. 2 FADP, which is expressly directed only at private individuals, **violation of the obligation to cooperate** is not punishable for federal bodies. This exclusion makes sense, as application to federal bodies would be completely contrary to the system. 20

The FDPIC cannot levy **fees on** federal bodies, in particular for ordering precautionary measures and measures under Art. 51 FADP. According to the wording of Art. 59 para. 1 FADP, fees may only be levied on private individu- 21

als. This exclusion is also consistent, as levying fees on federal bodies would again be contrary to the system.

22 According to the wording of the law, the FDPIC may also call on other federal authorities and cantonal or municipal police authorities to enforce orders under Art. 50 para. 1 FADP. Because federal authorities are entitled to the rights under the FADP and APA and the FDPIC can inform the public about the finding of non-compliance by a federal organ under Art. 57 para. 2 FADP, this option will probably only be used in exceptional situations. With regard to the **use of coercive measures** under Art. 50 para. 3 FADP, there is therefore no difference between private individuals and federal authorities, which means that, in our view, the FDPIC can also use coercive measures against federal authorities.

23 For the **party status** of federal authorities, see the comments on paragraph 2.

C. Delimitations

1. On "informal preliminary investigations"

24 Before the FDPIC opens an investigation under Art. 49 FADP and the provisions of the APA apply, it often takes informal action in a first step. The starting point is usually a complaint or media reports, which, however, regularly contain **insufficient evidence** for the direct opening of an investigation. The FDPIC can therefore first examine whether there are sufficient grounds for opening an investigation. In doing so, it can use all possible sources of information and, for example, examine public sources or question the controller, data subjects or third parties about the facts of the case. The preliminary investigation stage is classified as "informal administrative action," whereby the FDPIC must adhere to the principles of the rule of law (see Art. 5 FC) and may not act arbitrarily or in violation of the principle of equality before the law. During the informal preliminary investigation, the controller is not subject to any mandatory obligations to cooperate and the penal provision of Art. 60 para. 2 FADP does not apply – these provisions only become applicable after a formal investigation has been opened in accordance with Art. 49 FADP.

25 The informal preliminary investigation may lead to the refutation of the indications of a suspected data protection violation, so that no further action by

the FDPIC is necessary. This is regularly the case because, for example, the facts of the case were inaccurately reported in a complaint. Alternatively, a low-threshold intervention may be initiated or an investigation opened.

2. On "low-threshold intervention"

The informal preliminary investigation must be distinguished from the instrument of "low-threshold intervention." The term "low-threshold intervention" is not found in the law but was developed by the FDPIC. While the informal clarification aims to establish the facts in order to assess whether there are sufficient grounds for opening an investigation in accordance with Art. 49 FADP, low-threshold intervention pursues a different purpose. Low-threshold intervention attempts to restore the **legal situation by means of administrative measures** such as a simple letter, whereby the controller voluntarily takes the necessary measures. However, as with informal preliminary clarifications, no investigation is opened in accordance with Art. 49 FADP, which means that low-threshold intervention also qualifies as informal administrative action and the provisions of the APA do not apply. In the FDPIC's experience, this means that the necessary adjustments are implemented in a timely manner in many cases. The aim is to pursue a solution-oriented and resource-efficient approach. 26

For example, the FDPIC may be notified that a controller has not responded to a request for information made by the person making the notification. Based on one or more such reports, the FDPIC can contact the controller and request that it process the specific request for information made by the person who filed the report and provide a statement on the general procedure for processing requests for information. If the response from the controller indicates that requests for information will be handled correctly and within the statutory time limit in future, there is no need to open an investigation in such cases. 27

If the low-level intervention does not result in compliance with data protection requirements, there are usually sufficient grounds to open a formal investigation. This is the case, for example, if the FDPIC receives further complaints about the same matter after a low-level intervention has been carried out. Irrespective of any action taken outside the scope of an investigation, the FDPIC may open an investigation as soon as there are sufficient indications that this is necessary. 28

3. About the campaign

29 In addition to conducting investigations in accordance with Art. 49 FADP, the FDPIC also exercises supervisory activities based on Art. 4 para. 1 in conjunction with Art. 57 para. 1 lit. a, c and g FADP. The FDPIC refers to such activities as campaigns. From the perspective of controllers, **investigations are conducted on a case-by-case basis**, while the data protection authority may initiate contact **as part of campaigns without specific cause**. In other words, the FDPIC does not take action as part of campaigns on the basis of information concerning a specific data protection violation by a specific controller, but because the same or similar data protection problems have been identified repeatedly in a particular area of data protection law. In order to achieve effective control and enforcement of data protection regulations, the FDPIC can address several controllers at the same time, draw attention to general data protection problems identified in a specific area, and remind them of the relevant requirements. It is also possible to announce future supervisory activities in a specific area.

30 The FDPIC is not yet aware of any campaigns. A look at Germany shows what such a campaign could look like: As part of its supervisory activities, the Bavarian State Office for Data Protection Supervision (BayLDA) carries out various so-called focused data protection audits, i.e., audits without specific cause that have a particular focus. For example, the data protection requirements for advertising to prospective tenants were audited in this way. To this end, **responsible parties were selected at random** and specifically checked with regard to data protection requirements when searching for tenants by requiring them to complete a checklist within a statutory period. This action is based in particular on Art. 58 para. 1 lit. a GDPR, according to which all information necessary for the fulfillment of legal tasks must be provided.

31 The supervisory activity of the BayLDA described in the previous no. can, depending on its specific form, be classified as an **informal preliminary clarification or low-threshold** intervention, but which is **simultaneously directed at several controllers** in a specific area.

32 Unlike European data protection authorities, which, based on Art. 58 para. 1 lit. a GDPR, can request all information necessary for the performance of their *statutory tasks*, the FDPIC can, based on Art. Although Art. 50 FADP is intended to meet European requirements, the aforementioned provision in

the FADP has been restricted compared to the European provisions. Controllers are not subject to the obligation to cooperate under penalty of law pursuant to Art. 60 para. 2 in conjunction with Art. 49 para. 2 FADP within the scope of the EDÖB's supervisory activities. Within the scope of the FDPIC's supervisory activities, controllers are not subject to the obligation to cooperate under penalty of law pursuant to Art. 60 para. 2 in conjunction with Art. 49 para. 3 FADP, and no fees are payable (Art. 59 para. 1 FADP e contrario).

4. Informing the public about findings and decisions

Pursuant to Art. 57 para. 2 FADP, the FDPIC shall inform the public of its findings and decisions in cases of general interest. Since the administrative procedure is concluded with the delivery of the decision, the provisions of the APA are no longer applicable on the basis of Art. 52 para. 1 FADP. The official **publication** of a **decision** is considered an actual administrative act and is therefore not contestable as such, as it is a so-called **real act**. If the FDPIC and the party disagree on the form or type of publication and if the party's legitimate interests are affected, a contestable decision must be issued in accordance with Art. 25a APA. This publication order then constitutes a decision within the meaning of Art. 5 para. 1 lit. c APA, which obliges the party to tolerate the publication to the extent ordered. 33

A party's **legitimate interests** are affected if it asserts **business secrets** or **official secrets** which, in the opinion of the FDPIC, do not constitute such secrets and therefore, in its view, do not need to be anonymized or published. The definition in Art. 7 para. 1 lit. g LTras must be used as a basis for this. 34

The relevant legal requirements must be met for the **disclosure of personal data or data relating to legal entities**. 35

5. For consultation

In practice, the distinction between fee-based consultation in accordance with Art. 59 para. 1 lit. e FADP and informal preliminary clarification or low-threshold intervention can lead to uncertainty. If, for example, the FDPIC informs the controller in an informal preliminary investigation or as part of a low-threshold intervention what measures must be taken to ensure that a data protection violation can be ruled out or that an investigation can be refrained from being opened, such information can be classified as free advisory services. From a legal policy perspective, such an approach becomes question- 36

able at the latest when controllers are contacted by the FDPIC after data protection violations have become known and are advised on how to correct the situation in accordance with data protection requirements; and the situation is then voluntarily corrected in a timely manner so that the FDPIC refrains from opening an investigation. Instead of a sanction – such as a fine – those responsible would receive free legal advice after a data protection violation had become known. On the other hand, this is precisely the purpose of low-threshold intervention, which is why this approach should be limited to violations of minor importance in accordance with Art. 49 para. 2 FADP.

D. Special provisions in relation to the APA

37 The FADP contains **special provisions** that take precedence over the APA as lex specialis. The most important provisions are:

- Restriction of parties (Art. 52 para. 2 FADP)
- Information to the person who made the complaint (Art. 49 para. 4 FADP)
- Obligation to cooperate (Art. 49 para. 3 FADP)
- Taking of evidence (Art. 50 para. 1 FADP)
- Compulsory taking of evidence (Art. 50 para. 3 FADP)
- Information to the public (Art. 57 para. 2 FADP)

The special provisions in the FADP take into account the **special position of the FDPIC** as a supervisory authority, which is why, for example, the obligations to cooperate and the possibilities for taking evidence go further than in the APA. These must be distinguished from the rights to participate, which are governed by the general provisions of the APA.

III. PARTIES TO THE PROCEEDINGS (PARA. 2)

A. Overview

38 According to Art. 52 para. 2 FADP, only the federal body or private individual against whom an investigation has been opened is a party. This means that the status of parties is regulated differently in Art. 52 para. 2 FADP than in Art. 6 APA.

While, under the provisions of the APA, private organizations, associations, and authorities or third parties affected by the administrative act may also be parties, the **party status** in the FDPIC's investigation proceedings is **limited** to the federal body or private individual against whom the investigation has been initiated.

Proceedings may be conducted against **several parties**, in particular if the facts to be investigated concern several parties. If several parties are involved in processing, information provided to one party in the course of the proceedings may adversely affect the other party. In order to ensure that the right to be heard is upheld in such situations, it is necessary to combine the proceedings. Such situations arise, for example, when processing is carried out on behalf of a controller by a processor. 39

B. Private individuals as parties

Only the private individual against whom an investigation has been opened is a party. This means that party status is restricted to the person to whom the decision is addressed. The **data subject**, even if the FDPIC has opened the investigation on the basis of a complaint made by the data subject, is not a party to the proceedings. Private individuals are both natural persons and legal entities under private law. 40

Any private individual may be a party to proceedings if there are sufficient indications of a violation of data protection provisions. As soon as the FDPIC opens proceedings, it may order administrative measures based on Art. 51 FADP, thereby affecting the rights and obligations of the party and fulfilling the requirements of Art. 49 FADP and Art. 6 APA. In order to initiate proceedings against a private individual, **no data processing is necessary** on their part. This follows from the examples of administrative measures in Art. 51 FADP, according to which, for example, the measures under Art. 7 FADP or a data protection impact assessment may be ordered before data processing takes place. This is possible, for example, on the basis of reports or in the context of legislative projects, or if the FDPIC learns of large projects from media reports. 41

In addition to the controller pursuant to Art. 5 lit. j FADP, **processors** pursuant to Art. 5 lit. k FADP, a **data protection advisor** pursuant to Art. 10 FADP and the **representative** pursuant to Art. 14 FADP as parties to pro- 42

ceedings, provided that the content of the investigation involves a violation of data protection regulations by the private individual under investigation.

43 The question of a party's **passive legal standing** arises in particular in the case of **international corporations**, because the controller is regularly listed as a legal entity based in Ireland. For example, the data protection guidelines of Instagram, Facebook, and Threads name Meta Platforms Ireland Ltd (MPIL) as the controller. MPIL has also designated a representative in Switzerland and has a branch in Switzerland (Facebook Switzerland GmbH). In principle, all three entities mentioned above are eligible as parties. In our opinion, all three entities mentioned above can be parties to proceedings, provided that the subject matter of the investigation falls within the scope of their respective responsibilities.

44 For example, proceedings against Meta's branch in Switzerland are possible. Even if it is argued that the Swiss branch has nothing to do with the processing in question because it merely acts as a research laboratory for the entire group, that the owner of the intellectual property rights is another entity and that requests for deletion are also answered by that entity, proceedings against the branch in Switzerland are possible. In our opinion, a location in Switzerland always constitutes a link to the rest of the international group and is therefore responsible for compliance with Swiss regulations, including the FADP. Even if the Swiss location is not organizationally entitled to adapt the data processing in question, the FDPIC can at least establish the violation and order the branch to have the processing in question adapted for data subjects in Switzerland in accordance with data protection requirements via the competent body within the group. International groups should not be able to evade Swiss data protection obligations through internal organization.

C. Federal bodies as parties

45 A federal body may also be a party in data protection proceedings. According to Art. 5 lit. i DSG, a federal body is an authority or agency of the federal government or persons entrusted with public tasks. The **term "federal body"** corresponds to the definition in Art. 3 lit. h aDSG. Federal departments and federal offices, as well as their divisions and sections, are considered federal bodies. This also includes federal institutions and enterprises, as well as military commands. However, all natural and legal persons who process data for the federal government in the performance of public law tasks are also con-

sidered federal bodies. Cantonal and municipal bodies are not considered federal bodies, even if they perform federal tasks.

In proceedings not conducted under Art. 49 FADP, authorities or federal organs in proceedings against private individuals do not have party status within the meaning of Art. 6 APA due to the sovereign relationship with private individuals, but they have similar powers and are referred to as the "lower instance" in appeal proceedings. If the FDPIC initiates proceedings against a federal organ on the basis of Art. 49 FADP, the federal organ has the same status and powers as private individuals as the addressee of the substantive decision due to the constitutive reference provision. Consequently, the federal organ against which proceedings have been initiated is a party in the **appeal proceedings** and the FDPIC is the lower court. 46

IV. RIGHT OF APPEAL OF THE FDPIC (PARA. 3)

Decisions of the FDPIC are subject to appeal in accordance with Art. 44 APA. The appeal authority is the Federal Administrative Court (Art. 47 para. 1 lit. b APA in conjunction with Art. 31 and 33 lit. d VGG). Based on Art. 52 para. 3 FADP, the FDPIC has the right to appeal against decisions of the Federal Administrative Court. This provides a special legal basis in accordance with Art. 89 para. 2 lit. d BGG. For further information, please refer to the relevant provisions. 47

The opinion expressed reflects the personal opinion of the author and is not binding on the FDPIC.

BIBLIOGRAPHY

Auer Christoph/Müller Markus/Schindler Benjamin (Hrsg.), VwVG Kommentar, 2. Aufl., Zürich 2019 (zit.: VwVG-Kommentar, Bearbeiter/-in).

Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2022 (zit. SHK-DSG, Bearbeiter/-in).

Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023 (zit. OFK-DSG, Bearbeiter/-in).

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

Da Molin Luca/Wesiak-Schmidt Kirsten (Hrsg.), Datenschutz im Unternehmen, Praxishandbuch mit Beispielen und Checklisten, Zürich 2023 (zit.: Datenschutz im Unternehmen, Bearbeiter/-in).

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

Métille Sylvain/Meier Philippe (Hrsg.), Commentaire Romand Loi sur la protection des données (LPD), Basel 2023 (zit. CR-LPD, Bearbeiter/-in).

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

Waldmann Bernhard/Krauskopf Patrick (Hrsg.), Praxiskommentar Verwaltungsverfahrensgesetz (VwVG), 3. Aufl., Freiburg und Zürich 2022 (zit. PK VwVG, Bearbeiter/-in).

MATERIALS

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).

COMMENTARY ON

Art. 54 FADP

A commentary by Florian Roth / Simon Mazidi

SUGGESTED CITATION

Florian Roth/Simon Mazidi, Commentary of art. 54 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Roth/Mazidi, art. 54 FADP N. XXX.

Section 3 Administrative Assistance

Art. 54 Administrative assistance between Swiss authorities

[1] Federal authorities and cantonal authorities shall provide the FDPIC with the information and personal data that it requires to fulfil its statutory duties.

[2] The FDPIC shall provide the following authorities with the information and personal data that they require to fulfil their statutory duties:

a. the authorities responsible for data protection in Switzerland;

b. the competent prosecution authorities, where the matter relates to an offence reported under Article 65 paragraph 2;

c. the federal authorities and the cantonal and communal police for the implementation of measures in accordance with Articles 50 paragraph 3 and 51.

CONTENT

IN A NUTSHELL

Art. 54 FADP governs administrative assistance between the FDPIC and other federal and cantonal authorities. Administrative assistance is of considerable importance for the fulfillment of the FDPIC's statutory tasks. It enables cooperation between the FDPIC and other federal and cantonal authorities and thus contributes significantly to the enforcement of data protection law. Para. 1 regulates the administrative assistance in favor of the FDPIC, which is necessary for the enforcement of the FADP. Para. 2 obliges the FDPIC to provide administrative assistance to other authorities. The authorities to which the FDPIC is obliged to provide administrative assistance are listed exhaustively in para. 2.

I. GENERAL INFORMATION

A. Subject matter

1 Art. 54 FADP governs administrative assistance between the FDPIC and other federal and cantonal authorities. The provision is part of the FDPIC's administrative powers, which serve to enforce data protection. It also represents a concretization of Art. 58 para. 1 lit. b FADP. In para. 1, it regulates the administrative assistance in favor of the FDPIC, which is necessary for the enforcement of the FADP. Para. 2 obliges the FDPIC to provide administrative assistance to other authorities, which should enable these authorities to fulfill their respective legal tasks within the scope of application of the FADP.

2 Art. 44 para. 2 sentence 2 FC obliges the Confederation and the cantons to provide each other with administrative assistance. The obligation to provide administrative assistance is, on the one hand, a manifestation of the requirement in Art. 44 para. 1 FC that the authorities work together as partners in the federal state; the constitutional provision obliges the Confederation and the cantons to support and cooperate with each other in the performance of their tasks. On the other hand, it is an application of the mutual assistance obligation of Art. 44 para. 2 sentence 1 FC. Even before the totally revised Federal Constitution of 1999 came into force, the Federal Data Protection Commission described the fundamental duty of all authorities to cooperate with re-

gard to information as an unwritten constitutional principle of Swiss law. This constitutional principle is now enshrined in positive law in Art. 44 para. 2 FC.

The constitutional provision must be concretized at the legislative level. Art. 54 FADP represents such a concretization insofar as administrative assistance between the FDPIC and cantonal authorities is concerned. It should be noted that Art. 44 FC only concerns administrative assistance between authorities of different municipalities and not between authorities of the same municipality. Art. 54 FADP therefore constitutes a separate legal basis with regard to administrative assistance between the FDPIC and other federal authorities. 3

The term "administrative assistance" is not clearly defined by law. Administrative assistance is generally understood as the mutual support of administrative units (which are not in a subordinate relationship with each other) in fulfilling their statutory duties by providing assistance that is not regulated by procedural law (civil, criminal or administrative procedural law) (see N. 15 ff.). They may or may not be related to administrative proceedings in the first instance. Assistance outside or in advance of administrative proceedings is also part of administrative assistance. 4

Administrative assistance generally covers all assistance with which a federal or cantonal administrative authority supports another federal or cantonal administrative authority in the performance of its statutory duties. In addition to the provision of information and data (informational administrative assistance), this also includes the provision of physical or technical resources (vehicles, premises, technical equipment, etc.). The term "administrative authority" is to be understood functionally and includes all legal and natural persons who are directly tasked with the fulfillment of public law duties of the Confederation, the cantons or the municipalities. In the context of Art. 54 FADP, the focus is on informational administrative assistance (see n. 13). 5

B. History of origin

Art. 54 FADP did not give rise to any discussion during the legislative process. Administrative assistance was undisputed as a necessary prerequisite for the FDPIC to fulfill his statutory duties. The preliminary draft (Art. 46 of the FADP) already contained a materially identical provision. Under the old FADP, the article on administrative assistance only obliged the FDPIC to cooperate with domestic and foreign data protection authorities (Art. 31 para. 1 6

lit. c aDSG). The extension of administrative assistance to all authorities as a result of the revision of the FADP is in line with the FDPIC's manifold expansion of powers under the revised FADP.

7 In the consultation procedure, individual cantons complained that the additional workload for the cantonal and communal authorities was not clear and that the information to be provided should be specified more precisely in the ordinance. Several participants from the business community argued that business or manufacturing secrets should not be disclosed as part of administrative assistance proceedings.

8 The provision on national administrative assistance (Art. 48 FADP) only had a few editorial changes in the draft decree compared to the preliminary draft. For example, the wording in para. 1 was amended to the effect that federal and cantonal authorities now disclose to the FDPIC the information and personal data required to fulfill its statutory duties. In the preliminary draft, the provision still required the authorities to disclose the information and personal data required for the enforcement of this Act. Para. 2 lit. a also underwent a minor editorial change, whereby the FDPIC now discloses information and personal data to the authorities responsible for data protection in Switzerland, insofar as this is necessary for the fulfillment of their statutory duties. The preliminary draft still limited the wording to the cantonal authorities responsible for data protection. In the subsequent deliberations in the Federal Assembly, national administrative assistance no longer gave rise to any discussion; the provision was adopted in the version of the draft decree without any material or editorial changes.

9 The fact that national administrative assistance was not the subject of any significant controversy can be attributed to several factors. Firstly, the official benefit of national administrative assistance for the fulfillment of statutory duties is undisputed. Accordingly, Poltier puts it simply and aptly: "[...] l'entraide relève de l'évidence [...]." The forms of cooperation and collaboration made possible by administrative assistance enable data protection to be enforced more effectively. On the other hand, the provision on national administrative assistance is also a provision that can be found in many other federal laws, where it also aims to fulfill the statutory duties of the respective authorities. The fact that the Federal Council speaks of a standard provision in the dispatch, which can also be found in many other federal laws, can at most be understood to mean that administrative assistance is widely recognized as an in-

strument in the federal state. In any case, there is no uniform formulation across the individual substantive laws (see n. 14). The individual provisions regulate the scope of administrative assistance too differently.

C. Purpose of the norm

The federalist structure of the state and the task-sharing organization of the administration result in a high degree of technical specialization of the individual authorities. This is associated with a factual and local restriction of jurisdiction, which constantly threatens to hinder the fulfillment of statutory tasks. Administrative assistance is used to overcome such jurisdictional restrictions by providing assistance. The FDPIC thus comprehensively supervises the application of federal data protection regulations. However, data protection issues also arise in connection with specific areas of law and subject matter in which, for example, another federal authority (FINMA, COMCO, etc.) is entrusted with supervision and enforcement. Administrative assistance is also indispensable due to the vertical division of powers between the Confederation and the cantons: For example, to enforce the FDPIC's orders pursuant to Art. 50 f. FADP, the cantonal enforcement authorities are generally involved (see Art. 50 para. 3 FADP). Administrative assistance enables the necessary exchange of information and cooperation between the authorities, whereby the fulfillment of legal mandates can be guaranteed despite the factual and local differentiation of official activities. 10

The purpose of administrative assistance is to ensure that public tasks are performed as optimally and efficiently as possible and thus aims to enable and promote effective government action. On the basis of Art. 54 FADP, the FDPIC can draw on the expertise and experience of other authorities when fulfilling his statutory duties. As the FDPIC may be confronted with a wide range of sector-specific issues, he is often dependent on information and support from other authorities in order to carry out investigations correctly and efficiently. Art. 54 FADP ensures this cooperation for the benefit of the FDPIC and thus contributes to the enforcement of data protection law. 11

Another important function of administrative assistance is the gathering of evidence. The information and documents that the FDPIC has received from other authorities as a result of administrative assistance for the establishment of the relevant facts can be used as evidence in first instance administrative proceedings by the FDPIC. 12

D. Forms of cooperation and significance

13 In practice, the forms of cooperation in the context of administrative assistance are manifold. In the context of the FADP, the focus is on informational administrative assistance. This includes the disclosure of factual and personal data for the purpose of supporting the FDPIC and vice versa by the FDPIC to other authorities and is expressly addressed in Art. 54 para. 1 and 2 FADP. In principle, all procedural acts that serve to clarify the facts (including measures of evidence) or enforcement measures can be considered as administrative assistance measures. As part of the clarification of facts, the focus is on internal administrative assistance such as the provision of information, the inspection of official files, the submission or procurement of official documents or other necessary documents, cooperation in the clarification of relevant facts or access to a database. Interviews or an inspection may also be carried out as measures of evidence. Administrative assistance in the context of enforcement measures relates to measures that serve to enforce an official order. Art. 50 para. 3 FADP explicitly addresses the FDPIC's administrative assistance measures of evidence and enforcement.

14 Together with legal assistance (see n. 15 ff.), administrative assistance is an indispensable prerequisite for ensuring a uniform legal area in Switzerland. Administrative assistance is of considerable importance for the fulfillment of the FDPIC's statutory tasks. Nevertheless, Bellanger's statement that national administrative assistance appears "[...] comme un parent pauvre du droit [...]" has lost none of its validity even today. This is due in particular to the fact that national administrative assistance is not uniformly regulated at federal level. The APA does address administrative assistance in Art. 43. However, this only concerns assistance in the enforcement of orders issued by the federal authorities that are not aimed at monetary payment or the provision of security. Administrative assistance in the area of fact-finding, on the other hand, does not fall under Art. 43 APA. There is no overarching regulation governing both the procedure and the rights and obligations of the parties involved. Consequently, administrative assistance is regulated at the level of the individual special laws. The scope of the obligation to provide administrative assistance differs in individual cases, depending on which special law is applicable. In the present case, the scope of the obligation to provide administrative assistance is primarily determined by the FADP, in particular Art. 54 para. 1 and 2 and Art. 50 para. 3 in conjunction with Art. 50 para. 1 FADP. para. 1 FADP. The

scope of application and the modalities of administrative assistance remain to be specified in detail.

E. Delimitations

Administrative assistance between Swiss authorities (hereinafter: administrative assistance) must be distinguished from legal assistance on the one hand and international administrative assistance on the other. Administrative assistance can hardly be clearly distinguished from legal assistance. Nevertheless, the distinction is essential due to the associated legal effects. Both the choice of the applicable law - and thus the procedure - as well as the limits of the measures and the specific form of legal protection can depend on the classification. At the level of international administrative and legal assistance, the differences and their consequences are pronounced: for example, international legal assistance in criminal matters may fall within the scope of Art. 6 ECHR under special circumstances. An appeal to the Federal Supreme Court is only admissible in the case of international mutual assistance in criminal matters and administrative assistance in tax matters, which generally has a criminal prosecution purpose. With the exception of administrative assistance in tax matters, an appeal to the Federal Supreme Court is not permitted against decisions in the area of administrative assistance in international administrative assistance. 15

In order to differentiate between administrative and legal assistance, doctrine and case law are based on different criteria, whereby a combination of criteria is sometimes used for qualification. In particular, the following criteria can be mentioned: 16

- Type or function of the authorities involved: If judicial authorities are involved, this is referred to as legal assistance. Administrative assistance, on the other hand, refers to administrative authorities.
- Nature of the assisted proceedings (non-contentious or contentious proceedings or proceedings for the issuance of an order or appeal proceedings): Legal assistance covers forms of cooperation that relate to proceedings outside the administration. The latter take place before an authority that is external to the administration and institutionally independent of it. Legal assistance therefore mainly relates to (civil, criminal or administrative) procedural assistance in the context of court proceedings. A classic

example is the enforcement of judgments. Administrative assistance, on the other hand, covers assistance between federal and cantonal administrative authorities that is provided outside of proceedings defined by procedural law. It therefore takes place within the framework of internal administrative procedures or outside of administrative proceedings and is carried out at the request of an administrative authority or spontaneously.

17 Following these criteria, it is possible to speak of administrative assistance if assistance is provided between administrative authorities as part of an internal administrative procedure or a procedure outside of an administrative procedure. On the other hand, legal assistance is provided in the context of or in support of proceedings governed by procedural law - often judicial proceedings.

18 Since the proceedings before the FDPIC pursuant to Art. 49 et seq. FADP is a first-instance, non-contentious administrative procedure - and not a (court) procedure regulated by procedural law - official cooperation takes the form of administrative assistance. For this reason, legal assistance is not addressed in Art. 54 FADP. Administrative assistance also includes the enforcement of (precautionary) measures that the FDPIC may order as part of an investigation.

19 Art. 54 FADP only covers administrative assistance between Swiss authorities. Cross-border assistance falls under the regulation on international administrative assistance (Art. 55 FADP).

20 Furthermore, not all assistance within an internal administrative procedure or outside of an administrative procedure is covered by administrative assistance. The assistance provided within the scope of administrative assistance serves to fulfill the statutory duties of the requesting authority. General forms of cooperation or certain cooperation arrangements between authorities do not constitute administrative assistance. Such cooperation exists when different authorities are responsible for dealing with a specific matter. Within the scope of application of the FADP, cooperation is governed by Art. 53 FADP.

21 Finally, administrative assistance is always directed at other authorities. It is not personal. If the FDPIC requests assistance from an official with specific expertise as part of an investigation, the provisions on expert opinions apply. Based on Art. 52 para. 1 FADP, Art. 12 lit. e APA in conjunction with Art. 57 et seq. Art. 57 ff. BZP apply.

F. Limitations

Art. 54 FADP establishes a legal obligation of the authorities concerned to provide administrative assistance. However, information and personal data may only be exchanged insofar as this is permitted by official secrecy and the requirements of the protection of fundamental rights, data protection and administrative assistance, which overlap in part, are complied with. 22

1. Official secrecy

Official secrecy is the first barrier to administrative assistance. Official secrecy has been greatly relativized by the principle of publicity: Information must either be explicitly designated as secret under the FoIA or there must be weighty interests to counter the principle of publicity. The authorities may now pass on all information to other authorities that they would also have had to make available to private individuals on the basis of the principle of publicity. Nevertheless, statutory confidentiality obligations can be an obstacle to the disclosure of information to other authorities (Art. 36 para. 6 lit. b FADP). Such confidentiality obligations result on the one hand from official secrecy protected by criminal law (Art. 320 SCC), professional secrecy (Art. 321 SCC), manufacturing and business secrecy (Art. 162 SCC) or tax secrecy (Art. 110 DBG). On the other hand, under personnel law, public sector employees are prohibited from disclosing professional and business matters which, by their nature or due to legal provisions or instructions, must be kept secret (Art. 22 BPG in conjunction with Art. 94 BPV). Official secrecy also applies to civil servants from other offices who are obliged to maintain confidentiality: It is therefore a breach of official secrecy if the civil servant discloses a secret to another office within or outside his or her department or to a superior to whom he or she is not directly subordinate. There is no violation of official secrecy if there is a justification. This is the case if the disclosure of the information is expressly permitted in a substantive law or the disclosure of the secret is permitted by the written consent of the superior authorities. 23

Art. 54 FADP does not expressly address the question of whether the provision permits a breach of the statutory duty of confidentiality. In our opinion, the provision cannot be understood as a blanket authorization to disclose statutory confidentiality obligations by way of administrative assistance, otherwise the confidentiality obligation could be lifted solely by request from another authority. In the absence of a more specific legal provision, Art. 36 24

FADP can be applied analogously with regard to information other than personal data. According to para. 6 lit. b, federal bodies may refuse to disclose information, restrict it or attach conditions to it if this is required by statutory confidentiality obligations. In our opinion, the requested authority must therefore also weigh up the interests in connection with the granting of administrative assistance. If, as has been seen, Art. 54 FADP does not in itself constitute a sufficient legal basis for the disclosure of information and personal data, disclosure is only permitted in accordance with Art. 36 para. 2 if it is indispensable for the fulfillment of legal tasks (lit. a) or if there are other reasons, such as the consent of the person concerned (lit. b). A balance must always be struck between the interest in administrative assistance and the conflicting interests in confidentiality (see also Art. 36 para. 6 lit. a FADP). In connection with this balancing of interests or to protect statutory confidentiality obligations (Art. 36 para. 6 lit. b FADP), it may also be appropriate to make the disclosure of personal data subject to conditions or to anonymize the personal data. The provision of administrative assistance must also be permitted if there is another justification in accordance with Art. 320 SCC, such as the authorization of the superior authority (Art. 320 no. 2 SCC).

2. Fundamental law requirements

25 Another barrier to administrative assistance is the protection of fundamental rights. For example, Art. 13 para. 2 FC protects personal data, whereby the material scope of protection also includes the disclosure of such data to third parties. The disclosure of personal data to other authorities therefore generally constitutes an encroachment on the fundamental rights of the persons concerned. Assistance that interferes with the fundamental rights of private individuals in the context of administrative assistance must satisfy the requirements of Art. 36 FC. In these cases, Art. 36 para. 1 FC requires a sufficient legal basis for administrative assistance. While federal authorities - as well as the FDPIC - must comply with the FADP when providing administrative assistance, cantonal authorities that provide administrative assistance to the FDPIC are subject to the respective cantonal data protection laws. The other conditions for interference in the form of overriding public interest and proportionality must also always be observed when disclosing personal data to other authorities. Finally, the authorities are also bound by the principles of the rule of law (Art. 5 FC) when providing administrative assistance that does not interfere with fundamental rights. These include, for example, the princi-

ple of legality, the requirement of public interest and the principle of proportionality. The federal legislator has incorporated the constitutional requirements for the disclosure of personal data into the Data Protection Act and further specified them.

3. Principle of purpose limitation

In addition to the requirement of a legal basis for the disclosure of personal data, the FADP provides for purpose limitation (Art. 6 para. 3 FADP). The further use of personal data as a result of administrative assistance may often not be in line with the purpose limitation of the original data collection and processing under data protection law. However, this does not rule out the possibility of personal data being used for other purposes at a later date, provided there is a legal basis or justification for this. Art. 54 FADP in conjunction with Art. 36 FADP constitutes such a legal basis, which allows the authorities to deviate from the original purpose limitation when disclosing personal data. 26

4. Principle of speciality

Another manifestation of the principle of purpose limitation has emerged in the context of international legal and administrative assistance. Like the purpose limitation under data protection law, it serves to ensure the proportionate handling of information and personal data. This requirement, known as the principle of specialty, demands that the information and personal data may only be used by the requesting authority for the purposes for which they were transmitted by the requested authority. To this end, the requesting authority must specify the purpose for which the requested information or personal data is required. Even if the principle of specialty is often only discussed in connection with international administrative assistance, it is just as relevant for national administrative assistance. The purpose limitation under administrative assistance law therefore has a restrictive effect on the disclosure of information and personal data. 27

G. Enforcement and legal protection

The nature of administrative assistance as a partnership between authorities means that the authorities are on an equal footing in organizational terms and that there is therefore no relationship of subordination between them. The FDPIC cannot enforce his request for administrative assistance against the 28

federal authorities or the cantonal authorities with an internal administrative directive or order. Nor can he determine how, by when and to what extent administrative assistance must be provided; conversely, the same applies to administrative assistance provided by the FDPIC to other authorities. The modalities of administrative assistance must be mutually agreed between the authorities involved. The situation is different if the FDPIC orders investigative measures vis-à-vis federal bodies in accordance with Art. 50 para. 3 FADP, in which case these measures are not covered by administrative assistance. In this case, the federal body does not provide assistance to the FDPIC, but is obliged to cooperate as the addressee of the investigation.

29 Administrative assistance takes place between the authorities. If the requested authority refuses to disclose the information or personal data after examining a request, the requesting authority cannot contest the decision. The FADP does not grant the FDPIC or the other authorities mentioned in para. 2 a special right of appeal within the meaning of Art. 48 para. 2 APA. However, it is conceivable that in the event of a persistent refusal by the requested authority, the requesting authority may turn to its superior body or higher supervisory authority by means of a supervisory complaint. It is then up to the supervisory authority to enforce compliance with the obligation to provide administrative assistance in the event of unjustified resistance and, if necessary, to issue the requested authority with the necessary instructions. Authorities that do not belong to the same municipality may appeal to the Federal Supreme Court on the basis of Art. 120 para. 1 lit. b BGG. If there is a dispute between the FDPIC and a cantonal enforcement authority regarding the existence and scope of the obligation to provide administrative assistance in accordance with Art. 54 FADP, legal action may be taken.

30 Even if administrative assistance takes place between authorities and can therefore be described as an "[...] act within the authority [...]", it can have a reflex effect on private individuals. The official acts carried out in the context of administrative assistance may affect legal positions or interests worthy of protection of the parties to the proceedings or third parties. This includes, for example, the transfer of personal data in the context of informational administrative assistance or the use of coercive measures in the context of enforcement. Art. 54 FADP does not state whether the authorities are obliged to conduct administrative proceedings when providing administrative assistance. According to Art. 52 para. 1 FADP, the investigation procedure is governed by

the APA. It follows that - if the FDPIC requests administrative assistance as part of the investigation procedure - and this has an impact on the rights and obligations of the data subjects, the procedural rights guaranteed in the APA come into effect. The decision of the requested authority to provide administrative assistance is to be regarded as an order if the interests of private individuals worthy of protection are affected. In this case, the private individuals must have the opportunity to participate in the proceedings. For this purpose, the private person has party status and must be heard in accordance with Art. 30 APA. The decision to grant administrative assistance then constitutes an order in accordance with Art. 5 APA, which must be substantiated and contain information on the right of appeal (Art. 35 APA).

With regard to the point in time at which procedural rights are exercised, various differentiations can be made according to doctrine and case law: 31

- The requesting authority does not have to hear the parties to the proceedings or third parties if it requests administrative assistance from other authorities. The waiver of administrative proceedings can be justified by the legal protection subsequently granted in the main proceedings. This allows the party to the proceedings to assert its rights before the FDPIC as the requesting authority at a later date. If the FDPIC bases his decision during the investigation procedure on the information obtained through administrative assistance, he must inform the party to the proceedings and grant them access to the files. On this basis, the party to the proceedings may contest the accuracy of the information or the permissibility of obtaining and disclosing the information.
- The decision of the requested authority to provide administrative assistance is generally made in the form of an order if the interests of private persons worthy of protection are affected. However, it does not have to issue an order if it is obliged to provide administrative assistance and has no discretion. However, administrative proceedings are often appropriate. This is particularly the case if the statutory administrative assistance provision opens up a margin of discretion, which is conceivable in a large number of constellations: Such a margin of discretion may arise if the requested authority must decide whether the disclosure of the information and personal data is actually necessary for the fulfillment of the requesting authorities' statutory task. Furthermore, when disclosing personal data, the proportionality of the disclosure must always be examined due to the in-

terference with Art. 13 para. 2 FC and, if necessary, conditions or other restrictions (e.g. redactions) must be imposed. Finally, since Art. 54 FADP does not comment on statutory confidentiality obligations, it may be necessary in individual cases to weigh up the interests between the indispensability of providing assistance in accordance with Art. 36 para. 2 lit. a FADP and any conflicting interest in confidentiality. However, as there is also subsequent legal protection for parties to proceedings in these cases, it is argued in the doctrine that administrative proceedings are only necessary if there is a threat of irreparable disadvantage beyond the scope of assessment. If both conditions are met, the party to the proceedings should be given a fair hearing and thus legal protection before the requested authority decides whether to grant administrative assistance.

- Finally, the requested authority must also take into account the legal position of third parties. Insofar as personal data is transmitted in the context of administrative assistance that affects the rights and obligations of persons not involved in the main proceedings, they must be granted party status. As there is no possibility of subsequent legal protection for third parties, procedural rights must be observed at the time the personal data is disclosed. This is only possible if they are heard in advance and a reasoned and contestable decision is issued.

32 The appeal procedure is governed by the APA. The rulings are subject to appeal to the Federal Administrative Court in accordance with Art. 44 APA. In the final instance, an appeal in public law matters may be lodged with the Federal Supreme Court in accordance with Art. 82 et seq. BGG; decisions concerning domestic administrative assistance can be appealed against without restriction. Only decisions in the area of international administrative assistance, with the exception of administrative assistance in tax matters, are excluded from appeal in matters of public law. Furthermore, the exception of Art. 83 lit. v BGG only applies to decisions of the Federal Administrative Court on differences of opinion between authorities in the context of domestic administrative assistance. Appeals by private parties are not affected.

33 The acts of enforcement themselves constitute real acts, which is why they are generally not contestable. In this context, only a supervisory complaint is possible. This can be lodged either with the competent cantonal supervisory authority or with the FDPIC. As the requesting federal authority, the latter re-

mains responsible for enforcement, which is why it must also monitor the proper execution of enforcement assistance by the cantons.

II. ADMINISTRATIVE ASSISTANCE IN FAVOR OF THE FDPIC (PARA. 1)

Para. 1 lays down the principle that the federal and cantonal authorities shall provide the FDPIC with the information and personal data necessary for the performance of his statutory duties. Para. 1 has a dual nature in that, on the one hand, it authorizes the FDPIC to obtain administrative assistance from other authorities. On the other hand, it obliges the requested authorities to provide administrative assistance. 34

The requested authorities are federal authorities and cantonal authorities. The municipal authorities are not expressly mentioned in Art. 54 para. 1 FADP. Baeriswyl infers from this that the municipal authorities are not obliged to provide administrative assistance to the FDPIC. This view is supported by a systematic interpretation: The municipal authorities are explicitly mentioned in para. 3, but not in para. 1. Furthermore, according to widespread opinion, the municipalities are not addressees of Art. 44 FC, which regulates the principles of administrative assistance in the federal state. However, there are good reasons for a contrary view: Firstly, there is no indication in the materials that the national administrative assistance in Art. 54 FADP is to be understood in such a way that municipal authorities are excluded from the term "cantonal authorities". Secondly, it seems questionable whether the exclusion of municipal authorities is expedient with regard to the function of administrative assistance - namely to enable the FDPIC to fulfill his tasks in the context of consistent enforcement of data protection - especially since the scope of the transfer of public tasks to the municipalities is left to the cantons and thus authorities with far-reaching areas of responsibility would be excluded from the administrative assistance obligation. Especially in view of the purpose, it is reasonable to assume that the municipalities should also provide administrative assistance to the FDPIC. 35

The content and scope of the information to be provided are not described in more detail in para. 1. The provision refers to information and personal data that are required to fulfill the FDPIC's statutory duties. The explicit mention of personal data in para. 1 at least clarifies that the FDPIC may be provided 36

with all information relating to an identified or identifiable natural person in the context of administrative assistance. This provision is supplemented by Art. 39 lit. c FADP, according to which the FDPIC may process personal data, including particularly sensitive personal data, in the context of cooperation with federal, cantonal and foreign authorities. The reference to information makes it clear that Art. 54 FADP refers to informational administrative assistance. In addition to the expressly mentioned disclosure of personal data, this also refers to the disclosure of factual data (see n. 13). Administrative assistance in the context of enforcement measures is mentioned in Art. 50 para. 3 FADP. Due to the broad wording of para. 1, the content of the type of information and personal data is primarily determined by an interpretation based on the FDPIC's statutory tasks.

37 The FDPIC's statutory tasks are diverse and are listed in Chapter 7 of the FADP. First of all, the investigation of breaches of data protection regulations in accordance with Art. 49 et seq. FADP. Other tasks of the FDPIC include keeping a register of the processing activities of federal bodies (Art. 56 FADP) and annual reporting to the Federal Assembly (Art. 57 FADP). Art. 58 FADP then lists additional tasks in a non-exhaustive manner. It is not clear from the outset for which tasks and to what extent the FDPIC requires information and personal data from other authorities. It will therefore become clear in practice in which situations and for which actions the FDPIC is dependent on such information or personal data to fulfill a legal task. However, it stands to reason that the FDPIC will request administrative assistance from federal or cantonal authorities when investigating breaches of data protection regulations. Administrative assistance is a key instrument both for clarifying the facts and for enforcing administrative measures in accordance with Art. 51 FADP. The FDPIC may, for example, request assistance from the cantonal police authorities in carrying out investigative measures.

38 The disclosure of information or personal data referred to in para. 1 may take place spontaneously or upon request. However, the wording of the provision is far less clear than, for example, Art. 112 para. 1 DBG, which expressly refers to both forms of administrative assistance. Spontaneous administrative assistance occurs when an authority is legally obliged to inform another authority ex officio of facts of which it has knowledge. Other authorities can, for example, inform the FDPIC on their own initiative that data processing by a federal body or a private individual could violate data protection regulations. On the

other hand, administrative assistance can also be provided at the request of the FDPIC. Administrative assistance on request is the classic concept of administrative assistance.

As the other authorities are obliged to disclose the information or personal data, in this case the assistance is mandatory and not at the discretion of the requested authority. In terms of wording ("disclose"), the provision is comparable to Art. 32 para. 1 ATSG and Art. 87 para. 1 BVG, which also prescribe mandatory assistance. However, it should be noted that there is only an obligation to provide administrative assistance if it is necessary to disclose the information and personal data. This presupposes that the requested authority is authorized to check the necessity of the disclosure. Administrative assistance may only be provided if and insofar as the FDPIC would not be able to fulfill its respective legal mandate without the information or personal data, or would only be able to do so with considerable additional effort. Accordingly, Kerboas/Lennman also state that a mere improvement or better efficiency in the fulfillment of the statutory task cannot serve as justification for the disclosure. If the necessity is not given, there is also no obligation to disclose the information or personal data. For the disclosure of personal data (Art. 36 para. 3 FC) as well as information (Art. 5 para. 2 FC), this already follows from the principle of proportionality (see n. 25). In addition, a refusal to provide administrative assistance or, if necessary, disclosure subject to conditions or restrictions (e.g. redactions) may be justified (see n. 24). 39

In contrast to the provisions on administrative assistance in other substantive laws (Art. 32 para. 1 ATSG, Art. 45 para. 1 BüG or Art. 87 para. 1 BVG), Art. 54 FADP does not expressly stipulate that the requesting authority must submit a written and reasoned request to the requested authority. A written and reasoned request is required, for example, where there is an increased need for legitimacy for the disclosure of the information in question. This is the case, for example, in social insurance law, as the disclosure of data constitutes a deviation from the principle of confidentiality; in the naturalization procedure, the data required to assess the acquisition or loss of Swiss citizenship is often particularly sensitive personal data within the meaning of Art. 5 lit. c FADP. Not all information obtained by the FDPIC is subject to such a legitimation requirement. The waiver of the requirement for a written request in para. 1 expresses the fact that the FDPIC's scope for action should not be excessively restricted and that there is an interest in the simplest and most efficient possi- 40

ble enforcement of data protection. Especially when the FDPIC requests simple information from other offices, a written request is not mandatory. If the FDPIC requests the disclosure of personal data or if the information is to be used as part of an investigation into breaches of data protection regulations, the view expressed here is that the request should be made in writing - also in view of the legal protection claims of data subjects (see n. 30 f.).

41 Art. 54 FADP does not provide a basis for mass information on a large number of persons. Under the old FADP, the FDPIC stated in an opinion: "More comprehensive data disclosures, for example by means of (electronic) lists and the transfer to other data collections, require an explicit legal basis in which the necessary limits of data processing and security are also to be regulated." In the absence of express authorization in Art. 54 FADP, it can be assumed that the FDPIC may not obtain or disclose mass information in connection with personal data. It can also be assumed that requests without a precise reason or specific question (so-called "fishing expeditions") are not permitted in the case of administrative assistance upon request. With reference to Art. 19 para. 1 lit. a aDSG (which today corresponds to Art. 36 para. 2 lit. a FADP), the Federal Administrative Court has stated that "[t]he requesting authority [...] must describe the relevant facts to the requested authority, specifically identify the information and documents requested and state the reason for the request [...]". In our opinion, this also applies in connection with Art. 54 FADP.

42 A reason must always be given, even if this requirement is not expressly stated in para. 1: On the one hand, the requested authority must be able to assess the necessity of disclosing the information and personal data. Secondly, the principle of purpose limitation under administrative assistance law (principle of specialty) requires an indication of the purpose for which the requested information or personal data is required (see n. 27). If administrative assistance is provided at the request of the FDPIC, the FDPIC must therefore always justify the extent to which he needs the information or personal data to fulfill his legal duties in the specific individual case.

III. ADMINISTRATIVE ASSISTANCE FOR THE BENEFIT OF OTHER AUTHORITIES (PARA. 2)

43 The FDPIC shall disclose information and personal data to certain authorities insofar as this is necessary for the fulfillment of their statutory duties. Para. 2

provides an exhaustive list of the authorities for which the FDPIC is obliged to provide administrative assistance.

Art. 54 FADP serves as the legal basis for the mutual provision of administrative assistance. Therefore, with regard to the content and scope of the information ("information and personal data"), the necessity of disclosure and the further modalities, reference can be made to the comments on para. 1. As with para. 1, administrative assistance can be provided both spontaneously and at the request of the authorities named in para. 2. In the case of a request, the FDPIC is obliged to provide assistance. In other words, the disclosure of information and personal data is not at the discretion of the FDPIC. The prerequisite for this is, however, that the disclosure is necessary and that there are no other barriers to it. For example, the FDPIC is also subject to official secrecy under Art. 22 BPG. 44

A. Administrative assistance to data protection authorities (lit. a)

Para. 2 lit. a establishes reciprocity for the transfer of information and personal data in relation to other data protection authorities: Just as the FDPIC can request information and personal data from these authorities in accordance with para. 1, the other data protection authorities can request information from the FDPIC. The authorities responsible for data protection in Switzerland are authorities whose legal mandate also lies in the supervision and enforcement of data protection. This results from the relevant legal bases at federal, cantonal or municipal level. 45

The requirements of Art. 15 Convention 108+ can be used to specify the concept of data protection authorities. Art. 15 para. 5 Convention 108+ stipulates, among other things, that the supervisory authority shall act with complete independence and impartiality and not be bound by instructions when performing its tasks and exercising its powers. Against this background, independent cantonal and communal data protection authorities as well as other public-law organizations can be considered as independent data protection authorities within the meaning of Art. 15 para. 5 Convention 108+. 46

Data protection advisors to federal bodies (Art. 10 para. 4 FADP) exercise their function in relation to the federal body in a professionally independent manner and are bound by instructions in accordance with Art. 26 para. 1 lit. b DPA. However, they do not have the status of an authority. 47

48 In addition to the disclosure of information and personal data at the request of another authority in individual cases, an exchange of information takes place via the following institutionalized mechanisms and forums. These ensure a mutual flow of information between the FDPIC and the cantonal and communal data protection authorities and enable the authorities to contribute their concerns and expertise.

- In the privatim association, the independent data protection authorities of Switzerland's public bodies come together to form the Conference of Swiss Data Protection Commissioners. This promotes cooperation between the cantons, municipalities and the Confederation in the area of data protection through a constant exchange of information. The association expresses its views on data protection issues in the form of statements, consultation responses, guidelines and information sheets. For example, privatim has published a leaflet on cloud-specific risks and measures and commented on the decision of various cantonal governments to use "Microsoft 365" in the administration. Together with the FDPIC, the association has also updated its guidelines on the application of data protection law to the digital processing of personal data in connection with elections and votes in Switzerland. This is a general form of cooperation between the authorities.
- Based on Art. 111g AIG, Art. 102d AsylG and Art. 8b FPI, the cantonal data protection authorities and the FDPIC work together within the scope of their respective competences with a view to coordinated supervision of the processing of personal data in the context of Schengen/Dublin cooperation. To this end, the FDPIC has set up a coordination group of Swiss data protection authorities in the context of the implementation of the association agreements. The Coordination Group is dedicated to the exchange of information necessary for the effective supervision of data processing, discusses difficulties in the interpretation and application of legislation, analyses problems that may arise in the exercise of supervision or in connection with the rights of data subjects, and draws up harmonized proposals and opinions with a view to finding common solutions.

B. Administrative assistance to law enforcement authorities (lit. b)

In accordance with Art. 65 para. 2 FADP, the FDPIC has the right to report suspected violations of the criminal provisions of Chapter 8 of the FADP. In contrast, reports on breaches of data security in accordance with Art. 24 FADP may only be used in criminal proceedings against the person subject to the reporting obligation with their consent. 49

In the interest of effective enforcement of data protection, the FDPIC can use this right of notification to work towards uniform application of the FADP. He can constitute himself as a private plaintiff in the context of cantonal criminal proceedings. In addition, he can also challenge discontinuation orders and appeal against cantonal decisions. 50

Reporting the alleged offense to the competent cantonal prosecution authority generally involves the disclosure of personal data. This involves particularly sensitive personal data in accordance with Art. 5 lit. c no. 5 FADP. Art. 54 para. 2 lit. b FADP provides the necessary legal basis for the disclosure of personal data. 51

C. Administrative assistance to federal authorities and cantonal and communal police bodies (lit. c)

According to Art. 50 para. 3 FADP, the FDPIC may call in other federal authorities and cantonal or communal police bodies to implement the measures under Art. 50 para. 1 FADP. The measures consist of the FDPIC being able to order access to all information, documents, lists of processing activities and personal data required for the investigation (lit. a), access to premises and facilities (lit. b), hearings of witnesses (lit. c) or expert opinions (lit. d). However, this is only possible if it has opened an investigation and the private person or federal body does not comply with its duty to cooperate. Administrative assistance by the cantonal or communal police bodies takes the form of enforcement measures that serve to enforce the FDPIC's official order. This administrative assistance is provided for the benefit of the FDPIC and therefore falls under Art. 54 para. 1 FADP. Art. 54 para. 2 lit. c FADP provides the necessary legal basis for the FDPIC to transmit the necessary information and personal data to the aforementioned authorities for the effective enforcement of his orders. 52

53 For the enforcement of measures under Art. 51 FADP, the FDPIC may also disclose information and personal data to the federal authorities and cantonal and communal police bodies that are necessary for the performance of their statutory duties. Art. 51 provides for administrative measures and confers powers of disposal on the FDPIC. According to para. 1, in the event of a breach of data protection regulations, he may order that the processing be adapted, interrupted or discontinued in whole or in part and that the personal data be deleted or destroyed in whole or in part.

54 In contrast to the enforcement of measures ordered under Art. 50 FADP, the enforcement of FDPIC orders under Art. 51 FADP is not expressly regulated in the FADP. This is governed by the APA. At least in relation to private individuals, this is already evident from the fact that the FDPIC has powers to issue orders, which means that he is subject to the APA in accordance with Art. 1 para. 2 lit. c APA. The APA is already applicable to administrative proceedings under the APA in the absence of applicable exceptional provisions pursuant to Art. 2 f. APA are applicable to administrative proceedings of the FDPIC. Art. 52 para. 1 FADP once again expressly confirms the applicability of the APA to the FDPIC's administrative proceedings. This provision is primarily for clarification purposes.

55 Art. 41 APA provides the necessary legal basis for the enforcement of orders. The FDPIC can make use of the - admittedly non-exhaustive - catalog of enforcement measures contained in the provision. The FDPIC must adhere to the procedure provided for in Art. 41 APA, which includes the threat of enforcement with the setting of a (subsequent) deadline, the determination and enforcement of the coercive measures. In the event of imminent danger, he may dispense with the threat of coercive measures and the granting of a deadline for compliance.

56 If the FDPIC orders the partial or complete deletion or even destruction and the private person or federal body refuses, he may arrange for the deletion or destruction himself in accordance with Art. 41 para. 1 lit. a and lit. b APA.

57 The FDPIC may call in federal authorities and cantonal and communal police bodies for enforcement. Based on Art. 54 para. 2 lit. c FADP, the FDPIC may transmit the necessary information and personal data to the aforementioned authorities so that they can carry out the enforcement action.

BIBLIOGRAPHY

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).

MATERIALS

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.

COMMENTARY ON

Art. 55 FADP

A commentary by Florian Roth / Simon Mazidi

SUGGESTED CITATION

Florian Roth/Simon Mazidi, Commentary of art. 55 FADP, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (eds.), Online Commentary of the Federal Act on Data Protection

Short citation: OK-Roth/Mazidi, art. 55 FADP N. XXX.

Art. 55 Administrative assistance for foreign authorities

[1] The FDPIC may exchange information or personal data with foreign authorities that are responsible for data protection in order that they may fulfil their respective statutory duties in relation to data protection, provided the following requirements are satisfied:

a. Reciprocity with regard to administrative assistance is guaranteed.

b. The information and personal data are used only in the proceedings related to data protection that are the subject of the request for administrative assistance.

c. The recipient authority undertakes to preserve professional secrecy as well as trade and manufacturing secrecy.

d. The information and personal data are only disclosed to third parties if the authority that provided them gives its approval beforehand.

e. The recipient authority undertakes to comply with the requirements and restrictions imposed by the authority that provided the information and personal data.

2 In order to justify its request for administrative assistance or to comply with the request from an authority, the FDPIC may provide the following information in particular:

a. the identity of the controller, of the processor or of other third parties involved;

b. the categories of data subjects;

c. the identity the data subjects, provided:

the data subjects have consented, or
disclosure of the identity of the data subjects is essential for the FDPIC or the foreign authority to fulfil statutory duties;

d. processed personal data or categories of processed personal data;

e. the purpose of processing;

f. the recipients or the categories of recipients;

g. technical and organisational measures.

3 Before the FDPIC provides information that may include professional, trade or manufacturing secrets to a foreign authority, it shall inform the natural persons or legal entities concerned that hold these secrets, and invite them to comment, unless this is not possible or requires disproportionate effort.

CONTENT

IN A NUTSHELL

Art. 55 FADP regulates international administrative assistance between the FDPIC and foreign authorities responsible for data protection. The provision enables cross-border cooperation between data protection authorities and thus contributes significantly to the enforcement of data protection law. Para. 1 regulates the conditions under which the FDPIC may exchange information or personal data with foreign authorities. Para. 2 specifies what information the FDPIC may disclose in connection with such exchanges. Para. 3 sets out the rights of certain persons who may be affected by administrative assistance measures.

I. GENERAL

A. Subject matter

1. Basis

1 The purpose of international administrative assistance is to provide **mutual and cross-border support to the authorities responsible for data protection** (hereinafter: data protection authorities) in the performance of their statutory duties by means of assistance that takes place outside of a procedure governed by procedural law. Art. 55 FADP regulates international administrative assistance between the FDPIC and foreign data protection authorities.

2 Art. 55 is a **new provision** in the FADP. The previous provision (Art. 31 para. 1 lit. c aDSG) only obliged the FDPIC to cooperate with foreign data protection authorities. This was understood to mean professional exchanges on individual topics or regular cooperation in committees, working groups, or conferences. However, the provision did not provide a sufficient legal basis for the FDPIC to cooperate with foreign authorities and exchange information within the framework of supervising and monitoring federal data protection law. Nevertheless, the FDPIC already cooperated fully with foreign data protection authorities under the aDSG. At that time, cross-border data exchange was largely governed by the general rules of administrative assistance, with primary reference to obligations under international law (Art. 13 ff. Convention 108).

Art. 55 FADP now establishes **actual procedural rules** by regulating the conditions for the exchange of information or personal data with foreign authorities (para. 1) and the information that may be transmitted (para. 2). Para. 3 then gives holders of professional, business, or manufacturing secrets the right to information and the opportunity to comment if the FDPIC discloses information to a foreign authority that may contain such secrets. 3

Art. 55 FADP is in line with **European law**. Art. 50 of Directive (EU) 2016/680 requires supervisory authorities to provide mutual administrative assistance to each other. At the same time, the provision meets the requirements of Art. 61 DSGVO and Art. 16–21 Convention 108+. 4

2. International context

The aim of Convention 108+ is to create a uniform level of data protection and to strengthen **enforcement mechanisms**. This includes, in particular, cross-border cooperation between supervisory authorities. Switzerland ratified Convention 108+ on September 7, 2023. Convention 108+ requires ratification by 38 contracting states in order to enter into force. This number had not yet been reached in spring 2025. Subsequent references to Convention 108+ should therefore take into account that it has not yet entered into force. However, it is likely to enter into force soon. 5

Convention 108+ obliges the contracting parties to cooperate and provide mutual assistance in the implementation of the Convention. It provides for various forms of cooperation in a non-exhaustive manner. First and foremost, the supervisory authorities provide each other with administrative assistance, in particular by exchanging all **relevant and useful information**. This may involve two types of information: 6

- The **general exchange of information and documents** on the law and administrative practice in the field of data protection. This exchange should not be problematic, as the information can be freely exchanged and made publicly available.
- The **exchange of confidential information**, including personal data. In relation to personal data, Convention 108+ stipulates that such data may only be processed if it is either essential for cooperation (i.e., if cooperation would be ineffective without its provision) or if the data subject has given their explicit, voluntary, and informed consent in relation to the spe-

cific case. Otherwise, the exchange of personal data from specific data processing is excluded.

7 In addition to the exchange of relevant and useful information, the objectives of cooperation can also be achieved through **coordinated investigations**, such as coordinated inquiries or operations, and through the implementation of joint measures.

8 Supervisory authorities are obliged to comply with requests made to them by other supervisory authorities. Art. 20 of Convention 108+ provides for a definitive **rejection of requests** only if the request is incompatible with the powers of the supervisory authority (lit. a), the request does not comply with the provisions of Convention 108+ (lit. b) or the fulfillment of the request would not be compatible with the sovereignty, national security, or public order (e.g., to ensure the confidentiality of police investigations) of the Contracting Party or with the rights and fundamental freedoms of persons subject to the jurisdiction of that Contracting Party (lit. c).

9 At
the level of EU law, there are two legal acts relevant to data protection. The **DSGVO** is the fundamental act on data protection and regulates the protection of data processed within the internal market. In Article 61, it regulates in detail the mutual assistance between the supervisory authorities of the EU and EEA member states, without the need for special agreements between the member states in individual cases. International administrative assistance is regulated in Article 50(b) DSGVO. The DSGVO is not part of the Schengen acquis and is therefore not binding on Switzerland.

10 Directive (EU) 2016/680 serves to protect personal data processed for the purposes of preventing, investigating, detecting, or prosecuting criminal offenses or enforcing criminal penalties, including the protection against and prevention of threats to public security. As the content of Directive (EU) 2016/680 is based on the DSGVO, the provisions of both legal acts are largely consistent. The Directive is part of the Schengen acquis. As a Schengen-associated state, Switzerland is obliged to accept, implement, and apply further developments of the Schengen acquis, whereby implementation in Switzerland has taken place with regard to the supervisory authority as part of the total revision of the FADP. The obligation of supervisory authorities to provide

mutual administrative assistance is laid down in Article 50 of Directive (EU) 2016/680.

B. History

In the **preliminary draft** of the FADP, the provision on international administrative assistance (Art. 47 VE-FADP) was still divided into two paragraphs, with the first paragraph regulating requests for administrative assistance from the FDPIC to foreign authorities and the second paragraph regulating administrative assistance from the FDPIC to foreign authorities. The first paragraph specified the information that the FDPIC may disclose to foreign authorities in order to obtain administrative assistance; the second paragraph laid down the conditions under which the FDPIC may provide administrative assistance to foreign authorities. 11

During the **consultation process**, some participants argued that the structure of Art. 47 was flawed. They pointed out that the conditions for disclosing information differed depending on whether the FDPIC was the requesting or the requested authority. Several participants ultimately argued that information constituting business or manufacturing secrets should not be disclosed in the context of administrative assistance proceedings between the FDPIC and a foreign data protection authority without the protection of these secrets being guaranteed or the consent of the holder of the secrets being obtained. 12

The structure of the provision underwent a fundamental change in the **draft** of the FADP and after consultation (Art. 49 E-FADP). Instead of subjecting the FDPIC's requests for administrative assistance to foreign authorities and the FDPIC's administrative assistance to foreign authorities to different regulations, the conditions for the exchange of information or personal data with foreign authorities in para. 1 and the disclosure of personal data in para. 2 were standardized. Para. 2 thus uniformly regulates what information the FDPIC may disclose to foreign authorities to justify its request for administrative assistance or to comply with a request from a foreign authority. The amendments also meant a tightening of the rules: the draft was supplemented with the requirement of reciprocity (Art. 49 para. 1 lit. a E-FADP) and a new para. 3 was added with regard to professional, business, or manufacturing secrets. The concerns expressed in the consultation process regarding the systematics and disclosure of business and manufacturing secrets thus appear to have been heard. 13

14 In the subsequent **deliberations** in the Federal Assembly, international administrative assistance no longer gave rise to discussion; the provision was adopted in the version of the draft decree with only minor editorial changes.

C. Purpose of the standard

15 In view of the **increasingly cross-border nature of data processing**, international cooperation between data protection authorities is becoming increasingly important. The quantitative increase in the cross-border processing of personal data has increased the risk of violations of privacy and data protection in general. To counter this risk, effective and close cooperation in the form of international administrative assistance is essential. The focus is on mutual support between data protection authorities: As part of their supervisory and advisory activities, it is their task to ensure compliance with the relevant data protection regulations, including in a cross-border context, thereby effectively protecting the rights of data subjects.

16 Art. 55 FADP provides the **legal basis** for the FDPIC to cooperate with foreign data protection authorities and exchange information and personal data as part of its supervisory activities. This enables the FDPIC to exercise its supervisory activities even in cases of cross-border data processing by federal bodies and private individuals, thereby fulfilling its statutory duties. For example, in the context of its supervision and advisory activities relating to cross-border data processing by federal bodies and private individuals, it can contact the data protection authority of the respective recipient country if necessary. This is appropriate, for example, if, due to a lack of local expertise, it needs to draw on the knowledge and information of a foreign data protection authority in order to assess the extent to which the data protection requirements for data exchange are met.

17 International cooperation in the form of administrative assistance always serves to **preserve sovereignty**. Based on territorial sovereignty in international law, a state has exclusive sovereign authority over its own territory. This must be respected by other states. Authorities of a foreign state may therefore not carry out official acts on foreign territory without the consent of the state concerned. They therefore also have no direct access to data and information located on foreign territory. Administrative assistance makes it possible to overcome this barrier to sovereignty in an orderly procedure by enabling the FDPIC, which has the necessary data and information at its disposal, to pro-

vide administrative assistance to foreign data protection authorities. Foreign data protection authorities can thus be referred to the route of administrative assistance. This ultimately prevents foreign data protection authorities from taking extraterritorial (investigative) measures on their own authority. Of course, this also applies in the reverse case, when the FDPIC is dependent on information and personal data held by foreign data protection authorities.

D. Distinctions

1. National administrative assistance

In contrast to national administrative assistance, international administrative assistance covers assistance provided to foreign or international authorities or received by the FDPIC from foreign or international authorities. The subject matter is therefore **cross-border support** between the FDPIC and foreign data protection authorities. It always involves assistance provided to another country. It does not include national administrative assistance provided between the FDPIC and other federal or cantonal authorities for the purpose of fulfilling their respective legal duties, which is governed by Art. 54 FADP. 18

2. Distinction from legal assistance

It is difficult to distinguish between administrative assistance and legal assistance in an international context. While there are at least some criteria for differentiation in the domestic context – even if a clear distinction cannot always be made here either – the legal situation in the international context is even more confusing. Often, the two legal institutions are no longer distinguished at all, but are treated **jointly**. Some legal scholars therefore call for administrative assistance and legal assistance to be treated together in dogmatic terms. Certain laws then also cover both types of assistance under the same paragraph. 19

However, in our opinion, the distinction is essential due to the associated **legal effects**. Both the choice of applicable law (legal basis) – and thus the procedural and legal provisions – and the respective requirements and restrictions of the measures may differ: For example, international legal assistance in criminal matters may, under certain circumstances, fall within the scope of Art. 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR; SR 0.101). An appeal to the Federal Supreme Court is 20

only admissible in cases of international legal assistance and administrative assistance in tax matters, which generally have a criminal prosecution purpose.

21 The following **criteria**, which can also be applied in combination, can generally be used to determine administrative and legal assistance:

- **Type or function of the authorities involved:** International legal assistance is provided between judicial authorities. Administrative assistance, on the other hand, is provided between administrative authorities of the requesting and requested states.
- **Nature of the proceedings supported**: In procedural terms, international legal assistance is provided when a foreign or international authority is granted assistance for criminal, administrative, or civil proceedings. It is usually provided in connection with external administrative (i.e., judicial) proceedings. International administrative assistance, on the other hand, involves assistance between authorities of the requesting and requested states outside of proceedings governed by procedural law (judicial proceedings) for the purpose of fulfilling statutory tasks.

22 Since cooperation under Art. 55 FADP involves cross-border assistance between administrative authorities (FDPIC and foreign data protection authorities) and is provided outside of proceedings governed by procedural law, administrative cooperation takes the **form of administrative assistance**. Art. 55 FADP therefore only regulates international administrative assistance; the FADP does not regulate international legal assistance.

3. Simple administrative cooperation

23 Not all cross-border assistance between the FDPIC and foreign data protection authorities that takes place outside of a procedure governed by procedural law constitutes administrative assistance. Cross-border administrative assistance always relates to specific or identifiable persons and therefore takes place within the framework of a specific case. Para. 1 clearly refers to **specific individual cases** in which information and personal data are disclosed to a data protection authority so that it can fulfill its legal mandate.

24 Administrative cooperation for the purpose of general information and experience exchange (e.g., on *best practices*) is simple **administrative cooperation**. For this purpose, the FDPIC can network with foreign data protection

authorities independently of an individual case and the associated specific supervisory activity. This allows for an exchange on relevant issues arising in connection with cross-border data processing and the preparation of opinions or recommendations. Simple administrative cooperation can be based on Art. 58 para. 1 lit. b FADP.

E. Forms of cooperation

In the absence of a general law on international administrative assistance, the individual provisions on administrative assistance are scattered across various **special laws** and international treaties. They are highly heterogeneous, which makes it difficult to categorize them comprehensively. The sectoral approach, on the other hand, makes it possible to take specific account of the particularities of the subject area and the interests and needs of the authorities involved and the persons concerned. The content and scope of formal cooperation with foreign data protection authorities in the area of the FADP is therefore primarily governed by Art. 55 FADP. However, the specific forms of cooperation still need to be defined. 25

1. Forms of cooperation

Art. 55 FADP leaves the form of cooperation open. The provision merely states that the FDPIC may exchange information or personal data with foreign authorities for the purpose of fulfilling their respective statutory tasks in the area of data protection. It is therefore at the discretion of the FDPIC to decide on the intensity and form of cooperation with foreign data protection authorities. 26

The wording of Art. 55 FADP, according to which the FDPIC may exchange information and personal data with foreign authorities, makes it clear that **informational administrative assistance** is at the heart of the exchange with foreign data protection authorities. This includes the disclosure of factual and personal data for the purpose of supporting the FDPIC and, conversely, by the FDPIC to other foreign data protection authorities for the fulfillment of their respective legal tasks. This form of cooperation may be related to the investigation of suspected violations of the provisions of the respective data protection laws. 27

28 Art. 55 FADP does not expressly refer to the possibility of **conducting coordinated investigations**. Nevertheless, the FDPIC is authorized to enter into such forms of cooperation on the basis of Art. 55 FADP. The wording of Art. 55 FADP can certainly be understood to mean that the conduct of coordinated investigations is part of the exchange of information and personal data. Ultimately, cooperation in coordinated investigations is also based on the exchange of information. Furthermore, there is no indication in the materials that forms of cooperation are limited to the exchange of information. Rather, Art. 55 FADP leaves the forms of cooperation open, which argues in favor of the broadest possible understanding of international administrative assistance. In view of the purpose of international administrative assistance, which is to ensure compliance with data protection regulations in a cross-border context as effectively as possible, it stands to reason that all forms of cooperation – provided that the conditions set out in para. 1 are met – fall under international administrative assistance. As a result, the provision of investigative assistance and the conduct of coordinated investigations are also covered by Art. 55 FADP.

29 There is currently no specific legal basis for the **recognition and enforcement** of decisions by foreign data protection authorities. Even the administrative assistance measures granted by the FDPIC under Art. 55 FADP do not go so far as to include the enforcement of decisions by foreign data protection authorities – such as sanctions – in Switzerland. Given the differences between the catalog of criminal provisions in the FADP and the DSGVO, the enforcement of sanctions imposed by foreign data protection authorities would often fail due to the requirement of double criminality. This is particularly significant because controllers and processors in Switzerland are covered by the territorial scope of the DSGVO and may therefore be subject to its sanctions regime.

2. Multilateral cooperation

30 The increasingly cross-border nature of data processing has led to increased cross-border supervision, which is reflected in the networking of supervisory authorities, in which the FDPIC also participates. For example, the general cross-border exchange of information, which is intended, among other things, to promote the development of cross-border standards, often takes place in **multilateral bodies** and international networks. These have a varying degree

of institutionalization and represent a form of simple administrative cooperation (see N. 23 f.).

3. International treaties

Beyond Art. 55 FADP, the Federal Council is free to specifically regulate co- 31
operation between the FDPIC and foreign data protection authorities within the framework of international treaties. The FDPIC would have preferred Art. 55 FADP to have been supplemented to allow it to independently regulate the modalities of cooperation with foreign authorities within the framework of an agreement. However, Art. 67 lit. a FADP stipulates that the **Federal Council** may independently conclude international treaties concerning international cooperation between data protection authorities.

Art. 55 FADP already provides a sufficient basis for the exchange of personal 32
data and, for example, professional, business, and manufacturing secrets under the conditions set out in para. 1. An international treaty is not necessary for this. However, such a treaty is appropriate if **long-term cooperation** requires a higher degree of cooperation and this is to be formalized. The delimitation of the responsibilities of different data protection authorities can also be regulated within the framework of an international treaty. Finally, an international treaty is necessary if the rights and obligations of data protection authorities are to be established that go beyond Art. 55 of the FADP. Outside the scope of Convention 108+ and Directive (EU) 2016/680, this could include an obligation to provide administrative assistance or the regulation of disclosure to third parties (see N. 8 and N. 10).

F. Limitations

In the case of international administrative assistance, it must always be borne 33
in mind that two legal relationships are involved. These can sometimes be in **tension** with each other. On the one hand, there is a relationship under international law between the requesting and requested states. This relationship is primarily governed by the conditions for providing administrative assistance, as provided for in para. 1. The main question here is to what extent cooperation with the requesting state is permitted in the area of data protection on the basis of para. 1. On the other hand, there is also a legal relationship between the requested state and the person affected by the information or personal data transmitted within the framework of administrative assistance. In

this relationship, as far as personal data is concerned, the constitutional right to privacy is balanced against the state's duty to ensure compliance with data protection regulations in a cross-border context. For both relationships, the protection of fundamental rights and data protection law give rise to certain requirements that must be observed when disclosing information and personal data across borders.

34 Art. 13 para. 2 of the Federal Constitution of the Swiss Confederation (FC; SR 101) protects personal and personal data. **Informal self-determination** ensures that a person can independently decide to whom and when they disclose personal information and whether and for what purpose information about them is processed. The scope of protection is therefore not only affected when personal data is processed improperly. Processing without the consent of the persons concerned is sufficient for this. The disclosure of personal data to third parties is therefore also covered by Art. 13 para. 2 FC. The disclosure of personal data to a foreign data protection authority therefore generally constitutes an infringement of the fundamental rights of the persons concerned.

35 Interference with constitutionally protected rights is permissible under certain conditions (see Art. 36 of the FC). Art. 55 of the Federal Act on Data Protection (FADP) provides a sufficient legal basis for the disclosure of personal data to foreign data protection authorities. There is also a significant public interest in ensuring the most effective possible compliance with data protection regulations in a cross-border context, which ultimately also arises from the protection requirements of Art. 13 para. 2 of the FC itself. The disclosure of personal data to foreign data protection authorities must therefore be proportionate. The individual legal elements of the principles of administrative assistance enshrined in Art. 55 para. 1 FADP – the principles of specificity and confidentiality (see N. 54 ff. and N. 60 ff.), the principle of long arm (see N. 65 ff.) and the possibility of imposing conditions on the disclosure of personal data or anonymizing it (see N. 68 f.) – indirectly contribute to the proportionality of the disclosure in this context. Nevertheless, whenever personal data is disclosed to foreign data protection authorities, the FDPIC must check to what extent the disclosure is proportionate in the specific case. This leads Kerboas/Lennman to comment that such a **proportionality check** requires a lot of time and resources in each individual case, but sometimes leads to only a minor result.

International administrative assistance between the FDPIC and foreign data protection authorities is also subject to the **scope of the FADP**. This means, first and foremost, that the FDPIC may only disclose personal data if, according to Art. 16 FADP, an adequate level of protection exists in the country of the requesting data protection authority. In relation to the contracting parties to Convention 108+, an adequate level of protection can generally be assumed, subject to special circumstances. The reasons set out in Art. 36 para. 6 FADP also preclude the disclosure of personal data by federal bodies – and thus the FDPIC – to foreign countries. The FDPIC therefore refuses or restricts disclosure in the context of cross-border administrative assistance if this is required by essential public interests, interests of the data subject that are obviously worthy of protection (lit. a) or special data protection provisions (lit. b). With regard to the possibility of refusing or restricting disclosure on the basis of statutory confidentiality obligations, reference can be made to the following explanations (see N. 64 and N. 77). 36

- **Public interests** that preclude disclosure may include military security, national security, or policing. Such interests also exist if disclosure could compromise the position in negotiations, the opinion-forming and decision-making process of the public body, the effectiveness of investigative, security, or supervisory measures, or relations with foreign countries. Public interests may also include economic, monetary, or currency policy interests. If such interests are affected and it can be assumed with a certain degree of probability that disclosure would cause significant damage, disclosure must be refused.
- In the case of the **legitimate interests** of the person concerned, the primary consideration is the extent to which the disclosure of the information would unreasonably compromise the protection of privacy.

G. Legal protection

International administrative assistance is provided between the FDPIC and a foreign data protection authority. The disclosure of information and personal data can initially be described simply as "[...] internal administrative action [...]" or attributed to **actual administrative action**. The fact that the actual administrative action affects the legal positions of individuals is then a reflex effect of international administrative assistance that it can have on private individuals. Art. 55 FADP does not comment on whether the authorities are 37

obliged to provide administrative assistance for the implementation of an administrative procedure.

38 Effective legal protection naturally requires a suitable object of appeal and thus a decision. If the administrative assistance in the form of information is provided as an administrative act without a decision within the meaning of a **real act** of the FDPIC, a declaratory decision must first be obtained on the basis of Art. 25*a* of the Federal Act on Administrative Procedure (Administrative Procedure Act, APA; SR 172.021). In such cases, however, the person concerned will often be unaware of the administrative assistance measure, which means that they cannot actually pursue the route via Art. 25*a* APA. In the context of effective legal protection, the key question is in which cases there is a right to the issuance of a decision. It is only the decision that opens up the possibility of seeking administrative legal protection.

39 Whether a decision is required for the disclosure of information and personal data by the FDPIC is governed by the general rules of the VwVG. The FADP does not provide for any special legal deviations in this regard. The FDPIC's decision to provide administrative assistance is to be regarded as a decision if **legitimate interests** of private individuals are affected. Legitimate interests do not require legally protected interests. Purely factual, economic, or non-material interests are sufficient, provided that they appear to be worthy of protection.

40 The concept of interests worthy of protection is based on the status of a party under Art. 6 APA, which in turn is linked to Art. 48 APA. In terms of party status, every person has an interest in a decision that would be legitimate to challenge if a decision were issued. The prerequisite for this is that the person is **particularly affected**. This person must have a particularly close relationship to the subject matter to be regulated in the decision and therefore be more affected than the general public. Such an impact exists for Wyss, for example, when administrative assistance measures permanently and significantly determine rights and obligations. From this, he concludes that in cases where the legal position is irreversibly changed, a decision must be issued. Conversely, it should be noted that the transfer of personal data or information alone will often "only" constitute a preparatory measure with a view to the *subsequent* issuance of a decision. The initiation of administrative proceedings does not in itself constitute a decision. In the area of international administrative assistance, however, it is important to note that the transfer of data

abroad may in itself constitute an interference with the interests of the persons concerned that are worthy of protection, as confirmed by Art. 16 ff. FADP.

More generally, it can be said that the **disclosure of personal data** always constitutes an interference with informational self-determination. This means that there is always sufficient concern. If the FDPIC concludes that the conditions for administrative assistance under para. 1 are met, it must initiate proceedings for the disclosure of personal data and decide on the disclosure of personal data to a foreign data protection authority in a decision pursuant to Art. 5 and Art. 34 f. APA. The status of party to the proceedings allows the data subject to exercise the rights granted to parties under the APA: this includes, among other things, the right to a fair hearing, the right to inspect files, the right to representation, and the right to receive notification of the decision. Finally, participation in the administrative proceedings is also closely linked to the right to appeal. 41

In the case of the disclosure of professional, business, or manufacturing secrets, a particular interest is also readily apparent. In this context, para. 3 obliges the FDPIC to give the persons concerned the opportunity to comment before disclosing information that may contain professional, business, or manufacturing secrets to a foreign data protection authority. This already follows from the right to a fair hearing under Art. 29 APA. Art. 55 para. 3 FADP therefore does not create any recognizable procedural added value, but serves to clarify the situation. 42

The persons concerned must be involved in the administrative procedure at a **time** that allows them to effectively exercise their rights as parties. In other words, legal protection must be provided in a timely manner. Before disclosing the information or personal data to the requesting data protection authority, the FDPIC must inform the data subjects of the planned disclosure: once the information or personal data has been disclosed to the requesting data protection authority, domestic legal protection can no longer be effectively applied. Further processing of the information or personal data is determined outside the Swiss legal system. Since the use of the information and personal data abroad cannot be prevented, disclosure to the requesting data protection authority creates an irreversible situation. The Federal Supreme Court has also recognized this in the context of international administrative assistance in 43

tax matters: "Once the data has been transferred abroad, it is generally no longer possible to ensure that it will not be used."

44 With the FDPIC, a federal authority decides on cooperation with and the disclosure of information and personal data to foreign data protection authorities. If the decision to disclose is made in the form of an order pursuant to Art. 5 APA, the **appeal procedure** is also governed by the APA. Pursuant to Art. 44 APA, the orders are subject to appeal to the Federal Administrative Court. Decisions concerning international administrative assistance are generally excluded from appeal to the Federal Supreme Court in public law matters. This is intended to relieve the burden on the Federal Supreme Court and enable rapid proceedings through the shortened chain of appeal. Accordingly, the Federal Administrative Court decides in the final instance on international administrative assistance within the scope of the FADP. It is nevertheless conceivable that, with regard to other issues for which the Federal Supreme Court is responsible, a preliminary ruling on the admissibility of international administrative assistance may be necessary.

II. REQUIREMENTS (PARA. 1)

A. General

45 Art. 55 para. 1 FADP regulates the conditions under which the FDPIC may exchange information and personal data with foreign authorities for the purpose of fulfilling their respective legal duties in the area of data protection. These conditions are **characteristic elements** of cross-border administrative assistance. They have developed in the context of mutual legal assistance and are applied to the area of administrative assistance.

1. Competent authorities

46 According to Art. 55 para. 1 FADP, foreign authorities that are responsible for data protection in their country are covered. In other words, the exchange of information and personal data only takes place with **foreign data protection authorities**. The FADP does not contain any further requirements for qualification as a foreign data protection authority. In our opinion, the supervisory authority as described in Art. 15 of Convention 108+ can be used to understand the term. This provision obliges the contracting parties to establish one or more independent and impartial public supervisory and control authorities

that contribute to the protection of natural persons with regard to the processing of their personal data. These authorities may be a single data protection officer or a collegiate body. In addition to independence, it is essential that the supervisory authority has effective supervisory and control instruments at its disposal. The authority must therefore also have investigative powers.

Furthermore, a distinction must be made between the data processing bodies of the respective states – including the supervisory authorities in certain economic sectors or industries – and the specific supervisory authorities in the field of data protection. Cross-border cooperation in the context of data protection law takes place primarily at the level of the **data processing bodies**. In the course of their daily work, these bodies must assess whether the exchange of information and personal data with a foreign authority is permissible. For the data processing bodies, cooperation is governed by the relevant substantive law. Articles 16 and 36 of the FADP must always be observed. The FDPIC, on the other hand, is responsible for supervising these data processing bodies, for which purpose it can rely on the international administrative assistance provided for in Article 55 of the FADP. 47

2. Scope and content

The exchange of information and personal data relates to all **statutory tasks** of the FDPIC or the foreign data protection authority. The scope of the statutory tasks is determined by national legislation, and the permissibility of the exchange is determined by the request, which must explain to what extent the information or personal data is necessary for the fulfillment of the statutory tasks. The statutory tasks of the FDPIC are listed in Chapter 7 of the FADP. The FDPIC may take all actions to which it is authorized under the provisions of the FADP applicable to its activities in order to fulfill foreign requests for administrative assistance. 48

In addition to **information**, the FDPIC may also exchange **personal data** within the meaning of Art. 5 lit. a FADP. The FDPIC may therefore disclose any information relating to an identified or identifiable natural person. 49

3. Legal nature

Art. 55 FADP does **not contain any obligation** to provide cross-border administrative assistance. It merely authorizes the FDPIC to provide administra- 50

tive assistance or to request administrative assistance under the conditions set out in para. 1. However, in relation to foreign data protection authorities that are signatories to Convention 108+, the obligation under the convention to provide administrative assistance and the grounds for refusal must be observed (see N. 8).

B. Conditions for admissibility

51 In order for the FDPIC to exchange information and personal data with foreign data protection authorities, the following five conditions must be met **cumulatively** in accordance with Art. 55 para. 1 FADP. In practice, it is difficult to conclusively assess the extent to which the individual conditions are met. In practice, therefore, the conditions should be set out in writing in the context of granting administrative assistance and communicated to the requesting foreign data protection authority.

1. Reciprocity (lit. a)

52 Art. 55 para. 1 lit. a FADP stipulates that **reciprocity of administrative assistance** must be ensured between Switzerland and the foreign state. Reciprocity is a characteristic element of administrative assistance. Accordingly, a requesting data protection authority can only request administrative assistance in the form of information and personal data if it is also prepared to grant administrative assistance itself.

53 Such administrative assistance is guaranteed in relation to the contracting parties to Convention 108+ and to the member states of the EU on the basis of Directive (EU) 2016/680. In relation to other foreign data protection authorities, reciprocity is bindingly guaranteed if an **international treaty** provides for administrative assistance with reciprocal rights. The Federal Council may conclude such international treaties independently on the basis of Art. 67 lit. a FADP. Without an international treaty basis, the FDPIC must obtain assurance of reciprocity in each individual case, whereby it can only comply with the request for administrative assistance on the basis of such assurance.

2. Principle of speciality (lit. b)

54 Art. 55 para. 1 lit. b FADP is an expression of the principle of speciality. The principle of speciality or the principle of purpose limitation is a traditional **principle of international law** governing international administrative and

legal assistance, which derives from extradition law. It is also enshrined in Art. 19 of Convention 108+. The Federal Supreme Court attributes customary international law character to the principle, at least in the area of extradition law. However, the principle is also codified in many federal laws governing administrative assistance.

According to the principle, the information and personal data exchanged may be used by the requesting authority **only for the data protection procedure** on which the request for administrative assistance is based and for which the information or personal data was transmitted. Further use is only permitted if the laws of both states or an international treaty provide for such a possibility and the requested authority that provided the information or personal data approves the further use in the specific individual case. For subsequent and parallel use of the information and personal data in any criminal proceedings, the principles of international legal assistance in criminal matters must be observed. 55

The principle of speciality serves as a **barrier** that primarily protects the sovereignty of the requested state. At the same time, however, the purpose limitation also serves to strengthen the personal rights of the persons concerned and is intended to ensure the proportionate use of the information and personal data. Unrestricted further use by the requesting state is prohibited by the purpose limitation. 56

In addition to its barrier function, the principle of speciality also acts as a **condition of admissibility** for the disclosure of information and personal data: the requesting data protection authority must provide sufficient assurance that it will use the information or personal data only for the purpose for which it was transmitted by the requested authority. Based on the principle of good faith under international law, the Federal Supreme Court has so far taken the view that compliance with the principle of speciality by states can be taken for granted. Only if there are concrete indications of misuse in the requesting state should compliance with the principle be reviewed. Against the background of this case law, the FDPIC does not need to obtain assurances if the administrative assistance is based on an international treaty that includes the principle of speciality. Both contracting parties are directly bound to observe the principle of speciality on the basis of the principle of good faith under Art. 26 of the Vienna Convention on the Law of Treaties (SR 0.111). If, on the other hand, administrative assistance is provided exclusively on the basis 57

of Art. 55 para. 1 lit. b FADP, the FDPIC must expressly inform the requesting foreign data protection authority of the requirement of (further) use associated with the principle of speciality and remind it of the limits within which the transmitted information or personal data may be used.

58 In terms of admissibility requirements, the purpose limitation arising from the principle of speciality requires that the requesting data protection authority specify the purpose for which the requested information or personal data is needed. This principle therefore results in an **obligation to provide justification**.

59 The controllability and **enforceability** of purpose limitation are, of course, limited. If a foreign data protection authority violates the principle of speciality, the FDPIC may reject future requests for administrative assistance from that authority on the grounds that there is insufficient guarantee of compliance with the principle of speciality. Apart from that, it can be assumed that enforcement must regularly be carried out by the data subject and through individual legal protection. This applies if the personal data of the data subject is actually used in a subsequent procedure as a result of its impermissible reuse – i.e., in a procedure that is not based on the original request for administrative assistance and for which the personal data was not transferred. In such a case, the data subject would have to complain about the impermissible transfer within the framework of the procedure in question. The extent to which this option is available depends in particular on the applicable (possibly foreign) procedural law.

3. Principle of confidentiality (lit. c)

60 Art. 55 para. 1 lit. c FADP is concerned with the protection of special confidentiality interests. The provision requires the requesting authority to undertake to protect these secrets. The **scope and content** of the secrets to be protected are determined by the relevant criminal law provisions and the relevant case law. For professional secrecy, reference is made to Art. 321 SCC, and for manufacturing and business secrets to Art. 162 SCC and Art. 273 SCC.

61 **Professional secrecy** applies in particular to clergy, lawyers, doctors, dentists, pharmacists, midwives, and psychologists.

62 The concept of secrecy is generally understood broadly in connection with **business secrets**; there is no legal definition. According to Federal Supreme

Court case law, facts that are neither obvious nor generally accessible (relative obscurity) are not considered secrets if the holder of the secret has a legitimate interest in keeping them secret (objective interest in secrecy) and wishes to keep them secret for legitimate reasons (subjective interest in secrecy). Trade secrets are information that could impair the commercial success of the company or distort competition if it became known to competing companies. Trade secrets therefore include all technical, organizational, commercial, and financial facts of economic life that could influence the commercial success of the owner of the secret.

Manufacturing secrets are to be treated in the same way as trade secrets: they relate in particular to the technical side of production, i.e., knowledge that contains instructions for technical action. This refers to knowledge that is used in the manufacture of products and that is not recognizable in the product sold and is therefore capable of being kept secret. This includes, for example, information about manufacturing, production, or construction processes and instructions, as well as research results, production and construction plans, or sources of supply. 63

Legal **confidentiality obligations** do not *per se* preclude disclosure to foreign data protection authorities. Art. 55 para. 1 lit. c FADP makes it clear that such information may be disclosed provided that the requesting data protection authority maintains professional secrecy and business and manufacturing secrets (see N. 77 ff.); Art. 55 FADP therefore allows for an exception to the statutory confidentiality obligation. However, Art. 55 para. 3 FADP obliges the FDPIC to obtain the opinion of the parties concerned before disclosing information that could contain professional, business, or manufacturing secrets (see N. 78). This makes it clear that a balance must be struck between the interest in disclosing the information and the interests of confidentiality. 64

4. Principle of the long arm (lit. d)

According to Art. 55 para. 1 lit. d FADP, information and personal data may only be disclosed to **third parties** – including other authorities – if the requested data protection authority has given its prior approval for such disclosure. Third parties primarily refer to third-party authorities in the requesting country that are not involved in the exchange between the FDPIC and the foreign data protection authority. 65

66 The **approval requirement** protects the persons concerned from further disclosure of information or personal data relating to them. It also ensures that the FDPIC retains control over the information and personal data. If there is a particular interest, the data subject must be heard before the disclosure is approved; in addition, the other rights of the parties must be safeguarded. This applies in particular to the disclosure of personal data. For further information, please refer to the comments on legal protection (see N. 37 ff.).

67 The FDPIC must obtain a corresponding **assurance** from the foreign data protection authority. It may refrain from obtaining such an assurance if the prohibition of disclosure to third parties is already effectively ensured by another legal basis, such as an international treaty.

5. Compliance with conditions and restrictions (lit. e)

68 According to Art. 55 para. 1 lit. e FADP, the requesting authority must comply with the conditions and restrictions imposed by the authority that provided it with the information and personal data. This provision allows the disclosure of information and personal data in cases where, without the possibility of conditions or restrictions such as **anonymization**, a request for administrative assistance would have to be rejected.

69 Since the FDPIC is bound by Art. 36 para. 6 FADP in the context of administrative assistance and this provision already links the disclosure of personal data to the possibility of conditions and restrictions, lit. e is essentially a repetition. However, the provision makes it clear that, even in the context of international administrative assistance, the FDPIC must base the disclosure of personal data on a **case-by-case assessment** of the interest in administrative assistance and the conflicting interests under Art. 36 para. 6 FADP.

III. DISCLOSURE OF PERSONAL DATA (PARA. 2)

70 Art. 55 para. 2 FADP specifies what information the FDPIC may disclose to the foreign data protection authority in order to justify its request for administrative assistance or to comply with a request from a foreign data protection authority. The list is **not exhaustive**, as can be seen from the wording "in particular" in the introductory sentence. In other words, the FDPIC may also provide other information to justify its request for administrative assistance or

to comply with a request for administrative assistance from a foreign authority.

According to the provision, the FDPIC may provide information on the **identity** of the controller, the processor or other third parties involved (lit. a) as well as on **categories** of data subjects (lit. b). The mention of categories serves to assign persons to standardized groups that share certain common characteristics. The dispatch cites "consumers," "members of the armed forces," and "employees" as examples of such categories. 71

The FDPIC may only disclose the **identity of the data subjects** if the data subjects have given their consent (lit. c no. 1). Disclosure of identity already occurs when a person can be identified. This may be apparent from the data itself. However, the identity is already identifiable if it can be determined without disproportionate effort from the context of the data or by combining it with other data. 72

The disclosure of identity requires the **consent** of each individual data subject. Otherwise, disclosure is not permitted. The requirements of Art. 6 para. 6 and para. 7 FADP apply to legally valid consent. Consent is therefore only valid if it is given voluntarily after adequate information has been provided and in relation to the specific disclosure. Adequate information includes details of the responsible person, the objective or purpose, the manner and scope of data processing, the categories of data processed, and details of the transfer of data. Consent is not bound to any form and therefore does not require a written declaration. However, when disclosing particularly sensitive personal data to foreign data protection authorities, consent must be given explicitly. According to the message accompanying the FADP, a declaration of intent is explicit "[...] if it is made in writing or verbally or by means of a sign and the intention expressed is immediately apparent from the words or sign used." 73

Consent is central to processing by private individuals because it serves as justification for an infringement of privacy. Regardless of consent, however, the FDPIC remains the addressee of fundamental rights. The disclosure of identity to foreign data protection authorities must therefore continue to serve the public interest and be proportionate in order to be justified, due to the interference with Art. 13 para. 2 of the FC (see N. 34 f.). The consent requirement therefore does not serve as justification for the processing of data 74

by federal bodies such as the FDPIC, but as an **additional barrier** to disclosure.

75 In exceptional cases, the FDPIC may disclose the identity of the persons concerned if the disclosure of the identity of the person concerned is **indispensable** for the fulfillment of the statutory task by the FDPIC or the foreign data protection authority (lit. c no. 2). The exception is analogous to Art. 36 para. 2 lit. a and lit. b FADP, which sets out such requirements for national administrative assistance, provided that there is no specific legal basis. Indispensability means that the task cannot be fulfilled at all without the disclosure of data.

76 In addition, the FDPIC may provide information about the personal data or categories of personal data processed (lit. d), the purpose of the processing (lit. e), the recipients and categories of recipients (lit. f), and the technical and organizational measures (lit. g).

IV. DUTY TO PROVIDE INFORMATION AND STATEMENT (PARA. 3)

77 Art. 55 para. 3 FADP obliges the FDPIC, in the context of administrative assistance proceedings, to disclose information that may contain **professional, business, or manufacturing secrets** to a foreign data protection authority only if it has given the persons concerned the opportunity to comment in advance. Both natural and legal persons may be affected. Contrary to what was requested in the consultation, the legislator has not made the disclosure of business and manufacturing secrets subject to the consent of the person concerned.

78 The purpose of the provision is to protect the rights of persons who are holders of professional, business, or manufacturing secrets. To this end, para. 3 provides for a **duty to inform and a right to be heard**. Before the FDPIC discloses information to a foreign data protection authority that may contain professional, business, or manufacturing secrets, it must inform the persons concerned who are the bearers of these secrets about the possible disclosure. The FDPIC is then obliged to obtain the opinion of the persons concerned. This gives the persons concerned the opportunity to present their point of view to the FDPIC in a statement and to justify why the information relating to professional, business, or manufacturing secrets should not be disclosed to the foreign data protection authority.

By informing the persons concerned in advance and giving them the opportunity to comment, the FDPIC helps to ensure that their interests are taken into account and their secrets are protected. The comments should be taken into account in the FDPIC's decision-making process, but they are **not binding**: para. 3 does not oblige the FDPIC to comply with the comments of the persons concerned. However, it has a duty to take note of the comments and to give them considerable weight in its decision-making. The more the professional, business, or manufacturing secrets of the holder of the secret are affected, the more weight must be given to the comments of the persons concerned. 79

According to Gerschwiler, the persons concerned must be informed as soon as there is a **certain probability** that professional, business, or manufacturing secrets could be disclosed. This is to be agreed with. The protection of professional, business, and manufacturing secrets can only be effectively guaranteed if the FDPIC does not wait until it is certain that secrets protected by criminal law are affected before informing the persons concerned. In order to be able to effectively take into account the interests of the holders of secrets and to involve them in the decision-making process in a timely manner by giving them the opportunity to comment, a generous standard must be applied. This may also help to avoid subsequent complaints. 80

In exceptional cases, the FDPIC is not obliged to obtain a statement from the persons concerned. This is the case if a statement is not possible or would involve a disproportionate amount of effort. This exception has apparently been made for practical reasons and is intended to prevent the disclosure of information to foreign data protection authorities from being undermined if it is impossible to obtain a statement or only possible with disproportionate effort. Since the FDPIC's disclosure interferes with the criminal law protection of the professional, business, or manufacturing secrets of the persons concerned, it should not be hastily assumed that this is **impossible or unreasonable**. However, the permissible course of action will ultimately have to be determined by case law. 81

BIBLIOGRAPHY

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.

MATERIALS

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).

COMMENTARY ON

Art. 57 FADP

A commentary by Myriam Christ

SUGGESTED CITATION

Myriam Christ, Kommentierung zu Art. 57 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Christ, N. XXX zu Art. 57 DSG.

Art. 57 Information

[1] The FDPIC shall submit a report on his or her activities to the Federal Assembly every year. He or she shall submit the report to the Federal Council at the same time. The report shall be published.

[2] In cases of general interest, the FDPIC shall inform the public about its findings and rulings.

CONTENT

IN A NUTSHELL

The provision on the FDPIC's public relations work is one of the most important but less well-known provisions of the Data Protection Act. As early as the 1980s, international experience showed that successful implementation of the data protection provisions requires a dialogue between the supervisory authority and the other federal authorities or the civilian population (e.g., when it is a question of pointing out a need for legislative action or exerting pressure on certain data controllers who do not comply with the legal provisions).

Art. 57 para. 1 FADP obliges the FDPIC to inform the Federal Assembly - the electoral body of the FDPIC according to Art. 43 para. 1 FADP - about its activities once a year. The Federal Council is informed in writing about the activities of the FDPIC. The second paragraph is intended to enable the FDPIC to carry out his information mandate independently of the supervised federal authorities. The provision is worded very openly. Thus, the FDPIC has numerous possibilities to carry out his legal information mandate.

I. GENERAL

A. Normative purpose and background

Article 57 FADP is not one of the most well-known provisions of the FADP. Nevertheless, this legal provision on the FDPIC's public awareness activities plays a crucial role in ensuring that data protection law requirements can be implemented in practice. Indeed, awareness of data protection law in both the private and public sectors is primarily raised through the public relations work of the FDPIC (and the cantonal and municipal data protection commissioners). Successfully raising public awareness of data protection requires a dialogue between the supervisory authority and the public. Data protection considerations or measures should therefore not remain purely internal to the data-processing agencies, either in the private or public sector, but should be brought to the attention of the public in a very conscious and proactive manner. 1

The public awareness activities of the FDPIC pursue several concrete goals. On the one hand, it contributes to strengthening the effectiveness of the FDPIC's supervisory activities (Art. 49 to 53 FADP) - as part of its supervisory ac- 2

tivities, the FDPIC can sanction unlawful data processing. Based on Art. 57 FADP, it can publish its findings and thus put pressure on the offending data controller as well as encourage other data controllers not directly affected by the investigation to adapt their practices. On the other hand, the FDPIC's public relations work can decisively relieve the FDPIC in his advisory role (Art. 58 FADP). The publication of easily understandable aids, such as guidelines, sample letters or FAQs, contributes decisively to reducing the effort required for personal consultation and to preventing potential data protection violations.

3 Furthermore, based on its public relations work, the FDPIC can give an account of its activities to the electoral body (Federal Assembly pursuant to Art. 43 para. 1 FADP) and thus provide the Federal Assembly with an overview of its official conduct.

4 Public relations work within the meaning of Art. 57 FADP then offers the FDPIC the opportunity to publish information about problematic developments and to point out any need for legislative action that it deems necessary.

5 In the present case, it should be noted that the individual enforcement of rights via the civil courts provided for by the legislator (Art. 32 para. 2 FADP) plays a subordinate or (almost) no role in practice. In view of lengthy and costly proceedings with an uncertain outcome, it is extremely rare for those affected to initiate proceedings before the competent court. This is all the more true as more and more data processing is carried out by private individuals abroad. Thus, a promising proceeding before a Swiss civil court becomes (almost) impossible. As a result, fundamental questions of data protection are rarely addressed in case law, and the few court decisions have only limited significance beyond the individual case. The FDPIC therefore plays an important role in law enforcement thanks to its public relations work.

B. History of origins

Ad para. 1:

6 A provision very similar to the current para. 1 was already contained in Art. 30 aDSG. Based on international experience, which had already shown in the 1980s that awareness of data protection law is strengthened, among other things, by the public relations work of the data protection authorities, this

provision had been incorporated into Swiss law in 1988 and entered into force in 1992.

Art. 30a FADP did not give rise to any debates in Parliament - the article corresponded to the Federal Council's draft of 1988. This also applies to Art. 57 FADP. In the context of the revision, the provision was only clarified insofar as the FDPIC now has to report annually (and no longer periodically). This clarification corresponds to the practice under the old law. 7

The FDPIC reports to the Federal Assembly and thus provides the electoral body with an overview of the performance of his duties. As under the old law, the Federal Council receives only the written activity report. 8

Furthermore, the expression "as well as when necessary" has been deleted. From now on, the FDPIC will report once a year. Neither the evaluation of the consultation nor the dispatch address this deletion. In practice, the possibility to inform the public also when necessary (i.e. at any time and not only once a year) has not played a major role. Moreover, it should be pointed out in this context that the FDPIC may, if necessary, inform the public about its activities on the basis of Art. 57 para. 2 FADP. 9

Ad para. 2:

Art. 57 para. 2 FADP was shortened in the revision compared to para. 2 under the old FADP. In line with the increased independence of the FDPIC already requested in December 2011, the FDPIC can now decide for itself what it informs the public about. The publication of personal data subject to official secrecy no longer depends on the consent of the authority concerned, and an explicit distinction between personal and factual data in the context of the FDPIC's information mandate is no longer provided for. 10

The second paragraph also states that the FDPIC "informs" and not merely "may inform" about findings in the general interest. This linguistic clarification is to be welcomed, but changes little in practice. The "may" provision under the old law already established a binding information mandate. 11

C. Comparative law

Ad para. 1:

12 The regular preparation of an activity report was already provided for in Art. 28 para. 5 Directive 95/46/EC and has been regulated in Art. 59 DSGVO since 25 May 2018. In terms of content, this provision differs from Art. 57 para. 1 FADP in that the corresponding European law rule specifies a possible content of the activity report (list of reported types of breaches and types of measures taken under Art. 58 para. 2 DSGVO).

13 Art. 15 para. 7 ETS 108 states that each European supervisory authority shall regularly prepare and subsequently publish an activity report. According to the explanatory report, an activity report must be published once a year. This report must contain, in particular, information on the measures taken to enforce national data protection legislation. Except for the fact that the revised FADP does not specify any content, the Swiss legislator has adopted both the Council of Europe and EU requirements. It goes without saying, however, that measures taken to enforce data protection provisions are mentioned in the FDPIC's activity report even without a corresponding legal requirement.

Ad para. 2:

14 Art. 15 para. 2 lit. e ETS 108 sets out the framework for the awareness-raising tasks of the supervisory authorities. According to the explanatory report, the supervisory authorities must proactively make visible the measures they take, their tasks and their competences. For this purpose, they may publish regular activity reports (cf. Art. 15 para. 7 ETS 108), opinions or general recommendations. They can also raise public awareness through other, freely selectable communication channels. According to the explanatory report, public relations work also includes informing individuals and data controllers about their respective rights and obligations in appropriate, i.e. easily understandable, language (especially if the data processing concerns children or other particularly vulnerable individuals).

II. PARA. 1: ANNUAL PUBLICATION OF THE ACTIVITY REPORT

A. Annual publication

15 In the context of the revision, Art. 30 aDSG was slightly clarified: the publication must take place "annually". This specification was requested in the consultation, but changes little in practice. The law still does not contain any

specifications regarding the time of publication. Under the old law, it was customary for the report to cover the period between April 1 and March 31 of the following year and to be published at the end of June. A press conference is held on the occasion of each publication. The FDPIC presents the report in person, often accompanied by another member of the management, and takes questions from members of the media. There is nothing to indicate that this practice will not be maintained under the new law.

The report is not submitted to the Federal Council or the Federal Assembly for any adjustments, either before or after publication. In other words, the report is published in the same way as it is submitted to the Federal Assembly and the Federal Council (cf. the specifications in Art. 37 FADP in this regard). Among other things, the FDPIC also exercises supervision over the data processing carried out by the federal bodies. It is therefore conceivable that, depending on the results of the investigation, federal bodies audited under supervisory law could demand certain adjustments to the activity report. Against this background, the publication of the unchanged activity report is to be welcomed and contributes to strengthening the independence of the FDPIC. 16

A presentation of the activity report before the commission responsible for preparing the election of the FDPIC or in the councils is not envisaged, even if this is occasionally demanded in the doctrine. 17

B. Activity report

The activity report is the centerpiece of the FDPIC's public relations work (see Art. 57 para. 2 and Art. 58 FADP for other ways to raise public awareness). 18

Unlike European law - i.e., Art. 59 DSGVO and Art. 15 para. 7 ETS 108 - neither the FADP nor the DPO impose substantive requirements in Switzerland. The FDPIC is thus in principle free to decide on the content of the activity report. Pursuant to Art. 58 para. 1 lit. f FADP, the Data Protection Commissioner also performs the duties assigned to him by the Public Information Act of 17 December 2004 (FoIA, SR 152.3). According to Art. 19 FoIA, the Public Information Officer must regularly report to the Federal Council and publish this report. Since the FoIA entered into force on July 1, 2006, the FDPIC has published an activity report that tracks both his activities as data protection commissioner and his duties as public information commissioner. 19

20 The activity report follows a similar structure year after year, although the weighting of the individual topics may vary: Current Challenges, Data Protection (Digitization and Fundamental Rights; Justice, Police, Security; Tax and Finance; Commerce and Economy; Health; Labor; Insurance; Transportation; International), Public Principle (General; Access Requests; Arbitration Procedures; Legislative Procedures), the FDPIC (Tasks and Resources; Communication; Statistics; Organization of the FDPIC). Moreover, the FDPIC sets several thematic priorities per activity report. For example, it devoted its first focus in the 2020/2021 activity report to the revised FADP and its second focus to the Privacy Shield and the challenges associated with it.

21 Like all federal authorities, the FDPIC must observe the applicable legal provisions in the performance of its statutory duties, namely those relating to the protection of industrial and commercial secrets. In addition, it is subject to official secrecy under Article 22 of the Federal Personnel Act (BPG, SR 172.220.1). Consequently, it must ensure the confidential treatment of personal data to which it gains access in the exercise of its supervisory duties, namely when it publishes its activity report.

22 Due to the very brief nature of the articles in the activity report (under the old law, approximately one column per supervisory investigation), it is difficult to imagine - in contrast to the publication of rulings - that fabrication or business secrets are revealed in the activity report.

23 In practice, the FDPIC anonymizes the names of private individuals against whom supervisory proceedings have been initiated but not yet concluded. As soon as the proceedings have been concluded, the legal entity concerned is named in the subsequent activity report. The naming of the offending companies may not always be pleasant for the parties concerned, but it does not fall under the manufacturing or business secrecy. In addition, the naming of the guilty party is covered by the purpose of Art. 57 para. 1 FADP, since one of the purposes of the FDPIC's public relations work is to exert pressure on the guilty party and to encourage other data protection officers who are not directly affected by the investigation to adapt their practices.

24 The situation is different in the case of official secrets, which can also be disclosed on one line. However, in these cases, the public interest in informing the public about unlawful data processing by federal authorities - also in view

of the historical responsibility of the FDPIC after the Fiche scandal - is likely to prevail (cf. comments below regarding Art. 57 para. 2 FADP).

The law also makes no stipulations regarding the form of the activity report. 25
Design and circulation are therefore determined independently by the FDPIC. The activity report expressly does not appear in the design internal to the federal administration. The independence of the FDPIC is thus also formally expressed.

Due to the objective of the reporting, the activity report must be a publicly 26
accessible document. The FDPIC publishes the report as a free e-paper on its website; the printed report can be ordered for CHF 17.00 from the Federal Office for Buildings and Logistics.

Since 2017/2018, the report has also been published in Italian and English. Be- 27
tween 1993 and 2017, the report was published in German and French only. The lack of an Italian translation was a clear violation of Article 10 of the Federal Law on the National Languages and Communication between the Language Communities (SR 441.1). Even if this federal law does not require publication in English, it is to be welcomed that the activity report has also been published in English for several years. This newly available translation simplifies the personal consultation of the FDPIC, since English-speaking persons are increasingly asking the FDPIC for his legal advice. A reference to the English-language version of the activity report helps to make these foreign-language consultations more efficient.

The addressees of the activity report are the Federal Assembly as the elec- 28
toral body of the FDPIC, the Federal Councillors as heads of the individual departments, all of whom carry out countless data processing operations, and the general public (media professionals, legal advisors, technicians, and the general civilian population). In other words, Art. 57 para. 1 FADP applies to all activities of the FDPIC. These very heterogeneous addressees represent a challenge that should not be underestimated when writing the activity report.

In this context, it should be noted for the sake of completeness that the data 29
protection challenges that arise in the private or public sector are often of a similar nature. For this reason, it may be instructive to read the activity reports of the cantonal data protection officers, who are required by cantonal law to publish activity reports.

III. PARA. 2: PUBLICATION OF FINDINGS AND RULINGS OF GENERAL INTEREST

A. Determination

30 "Determination" is not a clearly defined legal term; it comprehensively circumscribes the legally binding information mandate of the FDPIC.

31 Facts of general interest relevant to data protection law may be brought to the attention of the FDPIC through the media, via the hotline or contact form, or in exchanges with other federal or cantonal authorities. The extent to which the FDPIC wishes to react to an identified piece of information is at his discretion, in particular with regard to timing and information channel.

32 The legally fuzzy term "determination" offers the advantage of reacting to a (possible) FADP violation more flexibly and quickly than by issuing an order. In addition, this fuzzy term offers the possibility of informing the public about a matter relevant to data protection even if the requirements for initiating an investigation under Art. 49 FADP are not met.

33 Whether and how often findings will be published in the future remains to be seen. As with all legally fuzzy terms, the interpretation of this term depends on the respective FDPIC.

B. Decree

34 The FDPIC can now issue rulings (cf. Art. 49 to 51 FADP). During the consultation process, some participants from the business community requested that the FDPIC not publish its rulings, but only the facts about which an investigation was opened. These participants were of the opinion that this was the only way to guarantee the privacy rights of the persons concerned. Individual participants, on the other hand, were of the opinion that all FDPIC rulings should be published. The rule laid down in the law thus represents a compromise and enables the FDPIC to weigh any business or official secrets against the general interest in clarifying an unlawful fact in individual cases. The general interest is likely to be interpreted broadly in principle in light of the goals of the FDPIC's public relations work.

C. General interest

Neither the revised FADP, nor the revised DPA, nor the 2017 Dispatch define "general interest." The previous dispatch on the old FADP did not define the term either. Only one example was given by the Federal Council at that time: the publication of a recommendation on an information system of nationwide importance was in the general interest. In the doctrine, further, more current examples are mentioned: the data processing in question represents a special risk situation for the fundamental rights and the personal rights of the persons concerned, it concerns the general implementation of the FADP, it has a precedent character or it is widely discussed in public. Furthermore, according to Rosenthal/Jöhri, the publication of identified grievances (without further specification) may be in the public interest. Due to today's digital market, the publication of a FADP violation by a market leader is also likely to be in the public interest. In any case, the term is to be interpreted broadly also under revised law. The FDPIC may otherwise only be able to perform its public relations work inadequately. 35

As a rule, information of general interest will have a certain urgency and will deviate from the usual reporting. If there is no urgency, this information may be published in the next activity report. 36

Which information is of general interest and consequently should be published depends, among other things, on the prioritization of pending business made on the basis of available human resources. Even if it is true that the Federal Assembly has created additional posts with the entry into force of the new FADP, the FDPIC remains chronically understaffed. Thus, it is possible that findings that would be in the general interest will continue to be published late or not at all. 37

D. Publication

As was already the case under the old law, the time of publication can be freely chosen. The question of the time of publication is not always equally important. However, if the publication of a finding is used as a means of pressure, a publication that is strategic with regard to time is crucial. 38

The FADP does not provide any formal requirements for the FDPIC's public relations activities. The communication channel is thus freely selectable also under the new law. In the past, the FDPIC has published model letters, model 39

contracts, guidelines, fact sheets and FAQs on its website. It also drafts internal administrative opinions. In addition, the FDPIC gives speeches on current topics, publishes written articles in specialized journals, and gives interviews to the media. The communications department operates a Twitter account (@derBeauftragte) and regularly writes media releases. Various employees have collaborated on the creation of a teaching aid for young people. Broader campaigns would also be conceivable. Regardless of the communication channel chosen, the FDPIC must always follow the principles of a professional communication policy with a view to effectively raising public awareness.

40 Published findings do not have the legal scope of decrees or laws. They are not legally binding. In the event of a dispute, the court seized decides independently, even if the data subject has previously turned to the FDPIC in its advisory capacity or relied on a published finding. However, the fact that the private individual followed the advice of the FDPIC may play an important role in the examination of fault in reparative actions.

41 The publication of findings, however, also knows limits set forth in Art. 36 para. 6 FADP (substantial public interests, interest of the data subject that is obviously worthy of protection, statutory secrecy obligations or special data protection provisions). Like all federal authorities, the FDPIC must comply with the applicable legal provisions, namely those relating to the protection of manufacturing and trade secrets and those protecting the confidential and private spheres (defamation [Art. 173 SCC], libel [Art. 174 SCC], insult [Art. 177 SCC]) as well as the prohibition of coercion (Art. 181 SCC). In addition, he is subject to official secrecy pursuant to Art. 22 BPG. Consequently, the FDPIC must ensure the confidential treatment of personal data to which he gains access in the exercise of his supervisory duties. There is nothing to suggest that the FDPIC will change his practice of contacting the responsible persons concerned before a planned publication and asking whether any business or official secrets should be blacked out before publication. However, this contact should not be confused with obtaining consent.

42 In addition, the principle of anonymization of personal data applies. For this reason, personal data that is to be published is always anonymized before the planned publication. Names of senior administrative staff acting in the exercise of their administrative duties or the names of private persons in charge do not enjoy any special protection in this context.

There is an important exception to the principle of anonymization. If the FDPIC is of the opinion that the publication of the unredacted finding or decision is in the public interest, he may now waive anonymization himself (under the old law, the FDPIC was allowed to publish personal data subject to official secrecy only with the consent of the authority concerned). This development is to be welcomed, as it clearly reinforces the independence of the FDPIC. With increasing public awareness of data protection issues, this revision of the law is not surprising. In summary, it can therefore be assumed that the principle of anonymization will be interpreted rather narrowly and that not all publications will be anonymized as a matter of principle. 43

With regard to anonymization, it should also be noted that effective anonymization of personal data is becoming increasingly difficult in view of technological advances. Moreover, anonymization may not be effective, especially if the publication of the finding is to be used as a means of exerting pressure. 44

Criminal law provisions, such as defamation, libel, insult, coercion or abuse of authority, are of course reserved. The FDPIC does not enjoy any immunity under criminal law and must observe these criminal law provisions in the context of its public relations work. 45

Finally, it should be noted in this context that the FADP applies only to disclosures or publications of personal data (cf. Art. 1 FADP or Art. 36 FADP). However, it is conceivable that the FDPIC will come across factual data within the meaning of Art. 5 lit. a a contrario in the course of its supervisory activities. The disclosure of factual data is not subject to the FADP, but these data may be protected by official secrecy and their disclosure may therefore be subject to the provisions of the FPG (e.g. strategies, plans or measures in the cybersecurity area). In these cases, the explanations regarding the disclosure of personal data (Art. 36 et seq. FADP) probably apply by analogy. The FADP does not contain a provision on the release from official secrecy of factual data. It must therefore be assumed that the FDPIC can also release himself from official secrecy in such constellations. Whether this actually corresponds to the legislative will is questionable, especially in view of the politically tense situation in Europe. 46

BIBLIOGRAPHY

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 Daten-

schutzrechts/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).

MATERIALS

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).

COMMENTARY ON

Art. 58 FADP

A commentary by Myriam Christ

SUGGESTED CITATION

Myriam Christ, Kommentierung zu Art. 58 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Christ, N. XXX zu Art. 58 DSG.

Art. 58 Further tasks

[1] The FDPIC shall also carry out the following tasks in particular:

a. It shall inform, train and advise federal bodies and private persons on data protection matters.

b. It shall support the cantonal bodies and work with Swiss and foreign authorities that are responsible for data protection.

c. It shall raise public awareness, and in particular that of persons in need of protection, in relation to data protection.

d.I t shall provide data subjects on request with information on how they may exercise their rights.

e. It shall comment on draft federal legislation and measures that involve data processing.

f. It shall carry out the duties assigned to it under the Freedom of Information Act of 17 December 2004[21] or other federal acts.

g. It shall develop working instruments as recommendations of good practice for use by controllers, processors and data subjects; for this purpose, it shall take into account the specifics of the field concerned and the need to protect vulnerable persons.

[2] It may also advise federal bodies that are not subject to his or her supervision in accordance with Articles 2 and 4. The federal bodies may allow him or her to inspect files.

[3] The FDPIC has the power to declare to foreign authorities that are responsible for data protection that direct service is permitted in relation to data protection in Switzerland, provided Switzerland is granted reciprocal rights.

CONTENT

IN A NUTSHELL

The list of tasks set out in Art. 58 FADP supplements the tasks of the FDPIC already provided for in Art. 57 FADP. For example, this provision stipulates that the FDPIC raises awareness among the public about data protection, comments on draft federal decrees, or publishes recommendations of good practice. However, the list of tasks in Art. 58 FADP is not exhaustive. Other, non-specifically defined tasks may thus be assumed by the FDPIC, provided that they are consistent with the fundamental objectives of the FADP.

I. GENERAL

A. Purpose of the norm and background

1 According to the wording of the ingress ("In addition, the FDPIC shall in particular perform the following tasks"), Art. 58 FADP is to be understood as a supplement or catch-all provision to Art. 57 FADP. Art. 58 FADP specifies the scope of the FDPIC's advisory and information activities pursuant to Art. 57 FADP, which the FDPIC largely determines himself due to his legally enshrined independence.

2 The list of tasks of the FDPIC is also not exhaustive under the revised law ("in particular"). Thus, there is still some leeway for additional tasks under the new law, as long as they do not contradict the purpose of the FADP. In this context, it should also be noted that further tasks of the FDPIC are set forth in other parts of the FADP, e.g. in Art. 11 FADP (opinions on codes of conduct), Art. 12 para. 4 FADP (notification of lists of processing activities), Art. 16 para. 2 FADP (data disclosure abroad), Art. 23 FADP (consultation of the FDPIC in the context of data protection impact assessments) or Art. 24 FADP (notification of data security breaches). Yet other tasks of the FDPIC are laid down in various special laws, such as Art. 84b KVG (ensuring data protection by insurers) or Art. 63 para. 3 in conjunction with. Art. 64 NDG (examination by the FDPIC as to whether the FIS has lawfully processed the personal data of the person making the request).

3 For further information on the purpose of the norm and its background, please refer to the general information on Art. 57 FADP.

B. History of origins

As part of the revision, Art. 31 aDSG was adapted to EU law and to the requirements of the Council of Europe. For this reason, the list of tasks of the FDPIC was slightly adapted or supplemented. 4

Art. 31 para. 1 lit. d aDSG (adequate protection of data protection legislation abroad), Art. 31 para. 1 lit. e aDSG (examination of guarantees for data transfers to non-equivalent states) and Art. 31 para. 1 lit. f aDSG (certification procedure) were not included in the revised Art. 58 FADP. Now, it is no longer the FDPIC but the Federal Council or the FOJ that clarifies whether the legislation of a state in question guarantees adequate protection (Art. 16 para. 1 FADP). The list of states, territories, specific sectors in a state and international organizations with adequate data protection according to the Federal Council are now included in Appendix 1 of the FADP. The examination of the guarantees for a data transfer to a non-equivalent state is now regulated in detail in Art. 16 para. 2 FADP and is also adopted in principle by the FDPIC under the new law. Certification is now regulated in Art. 13 FADP. Under current law, the FDPIC can no longer examine certification procedures itself (Art. 31 para. 1 lit. f aDSG). A supervisory procedure within the meaning of Art. 49 ff. FADP are reserved in this context. 5

For further information on the history of the development of the advisory and information activities of supervisory authorities under data protection law, please refer to the comments on Art. 57 FADP. 6

C. Comparative law

In European law, the tasks of the respective data protection authorities are set out in Art. 57 DSGVO, without prejudice to other tasks set out in individual places in the DSGVO. 7

Art. 58 DSGVO sets out the specific powers by which the supervisory authorities can achieve the objectives set out in Art. 57 DSGVO. 8

In terms of the level of detail, Art. 57 and 58 DSGVO clearly go beyond the "sister regulations" in Art. 57 and 58 FADP. This attention to detail in European data protection law aims to improve legal certainty and the protection of fundamental rights, after the predecessor provision (Art. 28 Directive 95/46/EC) only provided a rough framework that had been filled out very differently 9

by national provisions under the old law. Apart from the formal differences (level of detail and structure), no fundamental differences in content between the European provisions and the Swiss provisions can be discerned. This finding is not surprising: the old list of tasks in Art. 31 aDSG was supplemented with the express aim of implementing the European law requirements pursuant to Art. 46 para. 1 lit. d and e Directive (EU) 2016/680 and the requirements of Art. 12bis no. 2 lit. e E-SEV.

II. PARA. 1: SPECIFIC TASKS OF THE FDPIC

A. Lit. a: Information mandate

10 Art. 58 para. 1 lit. a FADP was added to the FADP as part of the revision. This new provision is intended to clarify the FDPIC's information mandate set forth in Art. 57 FADP.

11 This new provision expressly provides that the FDPIC shall exercise his advisory and informational mandate not only vis-à-vis public bodies, but also vis-à-vis private persons. This linguistic clarification, which corresponds to the practice of the FDPIC under the old law, is to be welcomed.

12 In view of both the wording of the law and the message, the FDPIC has a wide margin of discretion as to how he wishes to implement this information mandate in practice. In principle, it is free to decide which decision-makers from the administration, politics, science and business it informs, trains or advises. However, the discretion of the FDPIC is not without limits: The independence of the FDPIC must always be preserved, even when implementing the information mandate as defined in Art. 58 para. 1 lit. a FADP. In practice, it may lead to problematic constellations if the FDPIC himself or members of his management maintain too close personal contact with certain decision-makers and this contact or exchange creates the appearance of bias on the part of the FDPIC for third parties or influences the FDPIC in a possible downstream supervisory procedure.

13 Within the framework of its information mandate, the FDPIC participates, for example, in the annual data protection law conference of the University of Fribourg, publishes guidelines, sample letters and FAQs concerning data processing carried out by federal bodies or private individuals, advises private individuals both by telephone and in writing, or regularly exchanges information

with the Association for Corporate Data Protection (VUD). It can also organize information events or further training for those responsible in the public sector. Under the heading of "training", cooperation with the various law faculties would also be conceivable. At present, data protection law is not a compulsory course at any Swiss university. As things stand today, future lawyers are not at all or only insufficiently prepared for the challenges in legal practice with regard to the cross-sectional subject of "data protection".

The FDPIC can now charge fees for advising private individuals on data protection issues pursuant to Art. 58 para. 1 FADP on the basis of Art. 59 para. 1 e FADP in conjunction with Art. 44 DPA. Art. 44 FADP. These fees are calculated on the basis of time spent, with an hourly rate of CHF 150.00 to 250.00. 14

With a view to efficient, Switzerland-wide implementation of this legally standardized information mandate, it is also crucial under the new law that the FDPIC and his or her deputy do not come from the same language region. In principle, the FDPIC and his or her deputy should therefore continue to be responsible for the implementation of the information mandate in their respective regions of origin (e.g., handling interview requests). 15

The more often the FDPIC fulfills its information mandate through various channels, the more likely it is that a broad public will be informed about the current challenges in data protection law. However, the actual implementation of the information mandate depends on the available human resources, which remain modest. 16

B. Lit. b: Support for cantonal and international authorities

Art. 58 para. 1 FADP lit. b is derived from Art. 31 para. 1 lit. a and lit. c aDSG. According to the explicit wording of the law, the support of cantonal and international authorities is not a special case of the FDPIC's advisory activities. The FDPIC may "only" support the cantonal authorities and not "advise" them. Due to the division of competences between the Confederation and the cantons, the FDPIC is not entitled to advise cantonal bodies to the extent that the cantonal data protection authorities are competent to do so. Under the old law, the wording of the law ("bodies of the cantons") excluded the FDPIC from also supporting municipalities. Now, due to the slightly adapted wording of the law ("Swiss authorities"), it is conceivable that the FDPIC may also support municipal bodies. However, due to the division of competences in the 17

area of data protection, it should remain the case in practice that the municipal bodies must contact the competent cantonal data protection authority in the event of questions or ambiguities.

18 Under the old law, it was also unclear from the wording of the law whether the relevant provision applied only to public bodies or also covered data protection bodies of private companies. In view of the current wording of Art. 58 para. 1 lit. b FADP, it is clear that the scope of this provision is limited to public bodies.

19 It follows from the foregoing that the consultations of the FDPIC must be limited to areas for which the cantons are not competent (consultations of private persons and of federal bodies, cf. Art. 58 para. 1 lit. a FADP) as well as to clarifications regarding delimitations of competence between the Confederation and the cantons. Actual cooperation in specific individual cases does not take place due to the division of competences between the Confederation and the cantons. In this sense, the wording chosen ("cooperates with Swiss authorities") is misleading.

20 The assistance provided by the FDPIC within the meaning of Art. 58 para. 1 lit. b FADP is still not bound to any form and remains free of charge under the new law.

21 In view of the increasingly transnational problems, assistance from foreign authorities is becoming more and more important. In view of Art. 58 para. 1 lit. b FADP, the FDPIC not only exchanges information with representatives of the cantonal authorities, but also has a seat in various international organizations and, in this context, supports foreign or international authorities in implementing globally effective data protection.

22 Due to its statutory independence, the FDPIC must always be able to decide for itself whether and to what extent it wishes to support another authority. A binding mandate to provide assistance would not be compatible with the independence of the FDPIC .

23 With regard to the limits of this assistance offered by the FDPIC, it should also be noted that Art. 58 para. 1 lit. b FADP is neither a basis for a federal competence in the area of data protection nor a basis for an exchange of information with other authorities (neither national nor international). This provision should only allow for a professional exchange between authorities and

thus allow the other public bodies to benefit from the legal and technical knowledge of the FDPIC.

Since the foundation of "privatim", the exchange with the cantonal authorities has been organized by representatives of this association or by certain working groups. In practice, it has repeatedly been shown that exchanges between federal and cantonal representatives are enriching in areas where their respective competences overlap, in particular during the Covid 19 pandemic, which raised various data protection issues in the health sector not only at the cantonal level but also at the national (and international) level. Recently, the FDPIC and "privatim" jointly revised their guide "Elections and Voting" with a view to the 2023 federal elections: Elections and Voting take place at all federal levels and are subject to similar challenges at all federal levels. 24

C. Lit. c: Awareness-raising mandate

Art. 58 para. 1 lit. c FADP specifies the awareness-raising mandate of the FDPIC set forth in Art. 57 FADP. 25

The sensitization of people in need of protection was newly included in the FADP in accordance with European law (Art. 57 para. 1 lit. b DSGVO). However, the term "vulnerable people" is not defined in either Art. 58 FADP or Art. 5 FADP (terms). The message lists minors and the elderly as people in need of protection. Due to the choice of words ("in particular"), this list is not exhaustive. Sick persons and refugees, for example, may also be considered to be people in need of special protection within the meaning of Art. 58 para. 1 lit. c FADP, especially if one considers that in these constellations, personal data requiring special protection within the meaning of Art. 5 lit. c no. 1, 2 and 5 FADP are often processed. For example, the FDPIC intervenes year after year regarding the processing of personal data in the health sector. 26

The FDPIC has already made efforts under the old law to sensitize young people to data protection. For example, it has designed seven lessons for pupils at secondary level I and II, each of which is devoted to a specific topic that is relevant to young people in their everyday lives. He has also published tips for new parents on his website. The interactive service for raising awareness of data protection and transparency in organizations "Think Data", which is supported by the FDPIC, is also explicitly aimed at female and male students, among others. However, the sensitization of children and young people 27

also knows its limits. According to Art. 62 para. 1 FC, education is the responsibility of the cantons. It is therefore primarily up to the cantonal directors of education to raise awareness of data protection during compulsory schooling.

28 With regard to the sensitization of older people, there is currently no known specific cooperation with an organization active in this area or a project aimed specifically at this social group. Cooperation with "pro senectute" or other associations or interest groups would be conceivable or desirable on the basis of Art. 58 para. 1 lit. c FADP.

29 The awarding of prizes and awards along the lines of, for example, the Rodotà Award of the Council of Europe or the Big Brother Awards of the Chaos Computer Club Switzerland would be one way of raising awareness among the civilian population in a somewhat different way.

30 When implementing the FDPIC's awareness-raising mandate, however, it must always be borne in mind that - as, for example, in the context of combating climate change - it is a matter of sensitizing the general public to a danger whose consequences will only become noticeable or tangible at a later point in time. This makes awareness-raising work significantly more difficult.

D. Lit. d: Advisory mandate

31 The FDPIC's advisory mandate was expressly included in the FADP as part of the revision. Thus, the law also reflects a change observed in practice: contrary to what the 1988 legislator had envisaged, the focus of the FDPIC's activities is not on supervision, but on advising private individuals:

32 Individual legal enforcement via the civil courts (Art. 32 para. 2 FADP), as envisaged by the legislator, plays a subordinate or (almost) no role in practice. In view of lengthy and costly proceedings with an uncertain outcome, it is extremely rare for those affected to initiate proceedings before the competent court. This is all the more true as more and more data processing is carried out by private individuals based abroad and leads to a violation of privacy in Switzerland. Promising proceedings before a Swiss civil court thus become (almost) impossible or more difficult. Consequently, fundamental questions of data protection are hardly an issue in case law, and the few court decisions have only limited significance beyond the individual case. The FDPIC, with its advisory mandate, therefore has an important role to play in law enforcement.

The FDPIC is free as to the form. It fulfills its advisory mandate both orally (hotline) and in writing (contact form, sample letters or sample complaints, guidelines, FAQ, media releases, Twitter). 33

Unlike consultations with "private persons on data protection issues" under Art. 58 para. 1 lit. a FADP, "information on how a private person can exercise his or her rights" under Art. 58 para. 1 lit. d FADP in conjunction with. Art. 59 para. 1 lit. e a contrario FADP free of charge. It goes without saying that the demarcation between the scope of application of lit. a and that of lit. d FADP is likely to be difficult in practice. In the interest of legal equality, it is to be hoped that the FDPIC will make generous use of the exception provided for in Art. 59 para. 3 FADP (waiver of the charging of fees) in this context. 34

In the course of its consultations, the FDPIC learns firsthand in which areas or in which companies there may be data protection problems. Implementing the advisory mandate as broadly as possible thus contributes, among other things, to the FDPIC being able to efficiently implement its supervisory mandate pursuant to Art. 49 et seq. FADP can be implemented efficiently. 35

E. Lit. e: Consultation of the FDPIC in the federal legislative process

Consultation of the FDPIC in the federal legislative process is a special case of the FDPIC's advisory mandate. 36

According to the new wording of the law, the Commissioner must be consulted on all bills concerning federal decrees and measures that affect data processing (and not only on bills that affect data protection to a significant extent). This linguistic clarification reflects the practice under the old law and is to be welcomed in terms of legal certainty. 37

In Art. 38 para. 2 FADP, this obligation of all federal bodies has been further specified: The federal bodies shall submit to the FDPIC all draft legislation concerning the processing of personal data, data protection and access to official documents. 38

The (unofficial) internal deadline for comments in the context of office consultations is three weeks. In practice, however, not every federal office adheres to this unofficial arrangement. In certain cases, the very short deadline for comments may lead to a reduction in the quality of the FDPIC's opinion. It 39

is to be hoped that after the end of the Corona pandemic, this deadline will be respected again to a greater extent. A return to the "courant normal" would allow the FDPIC to prepare his opinions carefully and - where he deems it necessary - to seek dialogue with the competent federal office and to find a solution that is feasible for all agencies involved.

40 If the FDPIC has been ignored in the legislative procedure and considers that there is a public interest in this information, he may address the public directly on the basis of Art. 57 para. 2 FADP (in conjunction with Art. 39 lit. i FADP).

41 The term "measures" is a fuzzy concept. This linguistic vagueness enables the FDPIC to have a seat in various bodies or working groups. The FDPIC can therefore be involved in the first phase of a new data protection project on the basis of Art. 58 para. 1 lit. e FADP. For example, the FDPIC was consulted at an early stage in the context of the cloud strategy of the federal administration. Or, for example, SECO also sought the advice of the FDPIC when revising the guidelines on Art. 26 ArGV 3, which were published in February 2023. However, it should be pointed out in this context that consultation with the FDPIC at the beginning of a new project does not exclude the possibility that the FDPIC, in the context of its supervisory activities within the meaning of Art. 49 et seq. of the FADP, may subsequently review the project in question. FADP, the FDPIC may subsequently review the project in question. In other words, the consultation of the FDPIC should not be confused with a kind of "certification procedure".

F. Lit. f: Tasks according to FoIA

42 The mention of the tasks of the FDPIC according to the FoIA is purely declaratory. The tasks of the FDPIC with regard to the principle of public access derive directly from Art. 18 FoIA (management of the conciliation procedure, public relations, consultation in the legislative procedure) and Art. 19 FoIA (evaluation).

43 Coordination between the FADP and the FoIA is governed by Art. 7 para. 2 and Art. 9 of the FoIA and Art. 36 para. 3 of the FADP, respectively.

44 It is debatable whether data protection or the principle of public access is served if the same authority has to advocate efficient data protection on the one hand and grant the greatest possible access to official documents on the other. The Swiss solution also applies in some other countries, such as Ger-

many (at the federal level) or the United Kingdom. France, on the other hand, has entrusted these two tasks to two different authorities. At the European level, the compromise in this regard is regulated in Art. 86 DSGVO.

G. Lit. g: Recommendations of Good Practice

Art. 58 para. 1 lit. g FADP was newly introduced into the FADP as part of the revision. However, the FDPIC already performed this task intensively as part of its advisory activities under the old law by publishing numerous guides, sample letters and FAQs on its website. 45

The publication of the recommendations of good practice is, like the consultation of the FDPIC in the context of the legislative procedure at the federal level (Art. 58 para. 1 lit. e FADP), a special case of the advisory activity of the FDPIC. Also with regard to the recommendations of good practice, it must be pointed out that an implementation of the recommendations does not exclude any supervisory procedure. In other words, the recommendations are not legally binding. The FDPIC cannot take legislative action on the basis of Art. 58 para. 1 lit. g FADP. Any court called upon to decide whether or not a FADP violation has occurred in an individual case is independent of any recommendations made by the FDPIC. However, the fact that a private individual has followed the recommendations of the FDPIC may play an important role in the examination of fault in the context of reparative actions. 46

Regarding the notion of vulnerable individuals, reference can be made to the preceding comments on Art. 58 para. 1 lit. c FADP. 47

III. PARA. 2: EXTENDED MANDATE TO PROVIDE ADVICE

In terms of content, Art. 58 para. 2 FADP corresponds to Art. 31 para. 2 aDSG. 48

Certain data processing operations are excluded from the scope of the FADP pursuant to Art. 2 para. 2, 3 and 4 FADP and Art. 4 para. 2 FADP. Art. 58 para. 2 FADP allows the FDPIC, if desired, to comment on issues that are excluded from the scope of the FADP according to the text of the law. The linguistic clarification in the second sentence clarifies that the federal bodies that may be affected can grant the FDPIC access to their files. In other words, official secrecy is lifted in these cases. 49

50 Art. 58 para. 2 FADP is a so-called "optional provision". Unlike for the tasks specified in para. 1, there is no entitlement for the advisory tasks mentioned in para. 2.

51 The list set out in Art. 58 para. 1 FADP is not exhaustive. It is therefore permissible for the FDPIC to also advise on data processing that does not fall within the scope of the FADP (cf. Art. 2 para. 2 lit. a FADP). This possibility is an expression of the fact that Art. 13 FC has comprehensive validity and does not only apply in those areas in which the FADP is applicable.

52 Due to the continued scarcity of resources at the FDPIC, Article 58 para. 2 FADP, like its predecessor provision, will probably rarely be applied.

53 For the sake of completeness, it must also be pointed out in this context that in areas where the FADP is not applicable, any supervisory activity of the FDPIC is excluded, e.g. in pending civil proceedings.

IV. PARA. 3: INTERNATIONAL LEGAL ASSISTANCE

54 Art. 58 para. 3 FADP was newly inserted into the FADP as part of the revision. The purpose of this provision is to simplify the transmission of official documents to private data protection officers who are domiciled abroad but are required to designate a representation in Switzerland pursuant to Art. 14 FADP.

BIBLIOGRAPHY

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).

MATERIALS

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).

COMMENTARY ON

Art. 60 FADP

A commentary by Jonas D. Gassmann

SUGGESTED CITATION

Jonas D. Gassmann, Kommentierung zu Art. 60 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Gassmann, N. XXX zu Art. 60 DSG.

Chapter 8 Criminal Provisions

Art. 60 Violation of obligations to provide access and information or to cooperate

[1] On complaint, a fine not exceeding 250,000 francs shall be imposed on private persons who:

a. violate their duties under Articles 19, 21 and 25–27, in that they wilfully provide false or incomplete information;

b. fail wilfully:

to provide information to the data subject in accordance with Articles 19 paragraph 1 and 21 paragraph 1, or

to provide the data subject with the information specified in Article 19 paragraph 2.

[2] A fine not exceeding 250,000 francs shall be imposed on private persons who, in violation of Article 49 paragraph 3, wilfully provide the FDPIC with false information or wilfully fail to cooperate in the course of an investigation.

CONTENT

IN A NUTSHELL

The provision of Art. 60 criminalizes (i) the intentional violation of the duty to provide information, (ii) the intentional violation of the duty to provide information, and (iii) the intentional lack of cooperation with the FDPIC in the course of an investigation. A fine of up to 250,000 Swiss francs may be imposed for the fulfillment of any of these offenses.

I. GENERAL

1 Art. 60 incorporates the regulatory content already contained in Art. 34 aDSG. Art. 34 para. 2 lit. a aDSG is not taken over, as the corresponding reporting obligations are no longer included in the revised FADP. Newly and additionally, the penal norm also extends to the duty to inform in the case of an automated individual decision according to Art. 21. In contrast to Art. 34 aDSG i.V.m. Art. 14 aDSG, the duty to inform no longer applies only to personal data and personality profiles requiring special protection, but now, according to Art. 60 in conjunction with. Art. 19 for all personal data. This further expands the provision. In the preliminary draft, a very comprehensive article was created for this purpose. A penalty was envisaged for the intentional violation of information, disclosure and cooperation obligations and also an element of negligence. In the consultation process, the punishability of negligent violations was criticized in some cases. As a result, the element of negligence was dispensed with in Art. 54 FADP.

2 The penal provision of Art. 60 para. 1 is an application offense, and that of Art. 60 para. 2 is an official offense.

3 The provision of Art. 60 is intended, on the one hand, to protect persons who may be affected from the endangerment of their personality and, on the other hand, to protect the supervisory function of the FDPIC (and thus its ability to function) in the private sphere. This is an abstract endangerment offense; the offense is completed with the provision of false or incomplete information or failure to provide information/details in breach of duty or with refusal to cooperate with the FDPIC. There need not be a violation of personality rights or the FDPIC's investigation procedure need not have been impaired.

Art. 60 para. 2 is to be distinguished from the provision of Art. 63 in that, in contrast to Art. 63, Art. 60 para. 2 does not require the existence of an order in the formal sense. 4

The penalty provision continues to be structured as an infraction, but the upper limit of the fine provided for it has been raised significantly. Art. 50 VE-FADP still provided for a fine of up to 500,000 Swiss francs. The Federal Council justified this amount with "the lack of control of the persons concerned over their data, the lack of transparency in data processing and the increasingly powerful economic actors". Comparisons were also drawn with other criminal provisions of ancillary criminal law (such as Art. 49 of the Banking Act) and the importance of high fines in deciding whether Swiss legislation still offers a "sufficient level of protection" in relation to the EU. This upper limit on fines provided for in the preliminary draft caused criticism in the consultation process. In some cases the fines were considered too low, in others too high. It was also criticized that the sanctions are only directed against private individuals. In response to this, the upper fine limit in Art. 54 of the FADP was set at 250,000 Swiss francs, which corresponds to 25 times the previous fine. The actual fine is determined taking into account the economic circumstances of the offender (Art. 106 para. 3 SCC in conjunction with Art. 47 SCC). Art. 54 FADP has been taken over as Art. 60 with a few editorial changes. 5

II. OBJECTIVE ELEMENTS OF THE OFFENSE

A. Circle of offenders

Art. 60 is a special offense, because only those who are obliged to provide information or to cooperate (Art. 60 para. 1) or those who are requested by the FDPIC to provide information or to cooperate in any other way within the framework of an investigation (Art. 60 para. 2) can be considered as perpetrators. Anyone who cannot be a perpetrator under Art. 60 and therefore does not respond to a request for information or provides false information remains unpunished. If the conditions are met, it is possible to be punished as an instigator. 6

The orientation of the criminal provision is in contrast to the DSGVO, in which the respective company is held responsible. In Switzerland, the natural persons who actually act on behalf of the company and culpably fulfill the of- 7

fense are held liable. This is justified by the rejection of the attribution of third-party culpability in corporate criminal liability by Art. 102 StGB. In addition, there would not yet be sufficient criminal procedural guarantees in administrative procedural law, which would lead to legal uncertainty. In order to counteract the lack of corporate criminal liability, the Federal Council envisages a tightening of the criminal liability of governing bodies through the application of Art. 6 VStR in addition to Art. 29 StGB.

8 Prosecutions can be brought against management personnel, but also against other persons who are responsible for relevant operations. At the same time, however, the obligated persons are not only responsible for the false information they themselves provide, but also, for example, for the case in which an employee provides false information in accordance with his instructions.

B. Penalty-bearing conduct

9 Art. 60 provides for three different offenses. Penalties are imposed for breach of the duty to provide information (Art. 60 para. 1 lit. a; below, n. 10 ff.), breach of the duty to provide information (Art. 60 para. 1 lit. b; below, n. 17 ff.) and failure to cooperate with the FDPIC in the course of an investigation (Art. 60 para. 2; below, n. 19 ff.).

1. provision of false or incomplete information (Art. 60 para. 1 lit. a)

10 Art. 60 para. 1 lit. a criminalizes the provision of false or incomplete information and thus refers to the violation of Art. 19, Art. 21 and Art. 25-27.

11 The objective elements of the offense include the existence of an obligation to provide information and the absence of a reason to waive or limit this obligation (Arts. 19, 21 and 25-27). A distinction can be made between the duty to provide information under Arts. 19 and 21 and the duty to provide information under Arts. 25-27.

12 Under the duty to provide information (Art. 25), only those who provide false or incomplete information are liable to prosecution, but not those who, for example, assert a false ground for refusal under Art. 26. Information is false if it does not correspond to the true facts (e.g. if the person requesting information is provided with data other than that which was actually processed, or if it is untruthfully claimed that no data is being processed from him/her). In addition, information is also false if it is misleading, i.e. if it creates a false impres-

sion of the true facts. Information is incomplete if not all the details listed in Art. 25 are provided (e.g. if the retention period of the personal data is not disclosed, although this would be possible). Information may also be cumulatively false and incomplete.

However, it is not a criminal offense if someone discloses that the information is incomplete by blacking it out or in some other way, since this does not create the appearance of completeness. The reason for this is that in the case of refused disclosure, action is easily possible via Art. 32, whereby the civil court can order the provision of the information under penalty of Art. 292 SCC. Furthermore, Art. 60 para. 1 lit. a does not apply in cases where information is provided but a fee is charged in violation of the law. In such a case, however, Art. 146 SCC (fraud) is sometimes applicable if the false impression is created that the fee is the fee normally owed. 13

Likewise, Art. 60 para. 1 lit. a does not apply if (e.g. because the existence of a situation requiring information is denied) no information is provided at all or only with delay. However, in the case of a refusal to provide information, criminal liability under Art. 60 para. 1 lit. b is possible. 14

In the context of the duty to provide information (Art. 19 and 21), the provision of false or incomplete information is also punishable. 15

In Art. 21, the duty to provide information no longer relates only to the acquisition of personal data and personality profiles requiring special protection, as in Art. 14 aDSG, but now to the acquisition of all personal data. The duty to inform has thus become more comprehensive in terms of content and the risk of criminal liability has been expanded. 16

2. Failure to provide information (Art. 60 para. 1 lit. b)

Art. 60 para. 1 lit. b covers those cases in which a private person fails to (i) inform the data subject that personal data about him or her have been obtained (Art. 19 para. 1) or that an automated individual decision has been taken (Art. 21 para. 1) or (ii) provide the data subject with the information he or she needs to assert his or her rights under the FADP (Art. 19 para. 2). The objective elements of Art. 61 lit. b would be fulfilled, for example, if a company fails to provide information in a legally adequate privacy statement about which personal data it processes. 17

18 It is also a criminal offense if a company gives a reason for not providing the information. In this respect, criminal liability is broader than in the case of Art. 60 para. 1 lit. a.

3. Providing false information or refusing to cooperate in an investigation by the FDPIC (Art. 60 para. 2).

19 The penal provision of Art. 60 para. 2 takes over the regulatory content of Art. 34 para. 2 lit. b aDSG, which declared the provision of false information or refusal to cooperate in the context of an investigation by the FDPIC to be punishable. It refers to the duty to cooperate set forth in Art. 49 para. 3, according to which private persons are obliged to provide the FDPIC with all information and documents necessary for the investigation. The offense of "providing false information" is a crime of activity, and the offense of "refusing to cooperate" is a true offense of omission.

20 The objective elements of the offense presuppose a formal investigation by the FDPIC pursuant to Art. 49, which has been opened because of a possible violation of data protection provisions. Any false information or refusal to cooperate in the context of investigations carried out by the FDPIC outside of a formal investigation are not covered by Art. 60 para. 2. Another prerequisite is that (i) the FDPIC unambiguously requested the perpetrator to provide information or to cooperate in any other way within the framework of the opened investigation, (ii) the FDPIC was entitled to make this request, (iii) the perpetrator either provided false information or refused to cooperate as requested, and (iv) the perpetrator was not entitled to provide false information or to refuse to cooperate (e.g. based on the right to refuse information mentioned in Art. 49 para. 3). False information is not punishable if the FDPIC had not requested any information at all.

21 The criminal court may not limit itself to examining the act or omission of the accused person, but must also examine whether the request by the FDPIC to provide information or to cooperate was lawful.

22 The request of the FDPIC does not have to be made with reference to criminal liability (in contrast to Art. 63 and of Art. 292 SCC), but it must be clear to the requested person that his cooperation is not voluntary. In cases where the FDPIC requests a potentially punishable person to cooperate, it must be re-

quired that he explicitly informs this person of the right to refuse to provide information.

III. SUBJECTIVE ELEMENTS OF THE OFFENCE

From a subjective point of view, intent is required. It is sufficient to have contingent intent, i.e. to consider it possible that the offense will be committed and to accept that it will be. At the time of the commission of the crime, the offender must have been aware of the circumstances of the case on the basis of which the objective facts must be regarded as having been established, and he must have understood the subsequent legal evaluations at least in layman's terms (so-called parallel evaluation in layman's terms). 23

In practice, it is probably not uncommon for the acting person to be aware of the possibility that information could be incomplete and to accept this because he or she prefers to provide such information rather than no information at all. If the person concerned is given a declaration of completeness, intent is regularly assumed if the information is not complete after all. The party obliged to provide information acts negligently and is thus not liable to prosecution if it has relied on the fact that the supplied, non-verified data is complete. The distinction from the existence of contingent intent must be made on the basis of circumstantial evidence in each individual case. 24

If the perpetrator is mistaken about the facts relevant to the facts of the case, there is an error of fact pursuant to Art. 13 SCC. In this case, the court judges the offense according to the perpetrator's conception of the facts. This is particularly relevant if the person obliged to provide information provides incomplete information because he or she believes it to have been provided in full. An error of fact can also exist with regard to normative elements of the offense, such as the question of whether there is a corresponding duty to provide information or to report. In this case, the opinion of an average third party is decisive. 25

IV. ILLEGALITY AND CULPABILITY

According to Art. 333 para. 1 SCC, the general rules of the SCC apply with regard to unlawfulness. Conduct in accordance with the offence may exceptionally be permitted on the basis of legal or supra-legal grounds for justification. 26

27 With regard to guilt, the general rules also apply under Art. 333 para. 1 SCC. Criminal liability may be hindered by a mistake as to prohibition according to Art. 21 StGB. However, this is only the case if the person who comes into question as the perpetrator could not have known that he was acting unlawfully. In this case, he or she believes that he or she has done nothing wrong. If the error of law could have been avoided, the penalty is only reduced.

BIBLIOGRAPHY

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.

MATERIALS

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

COMMENTARY ON

Art. 61 FADP

A commentary by Jonas D. Gassmann

SUGGESTED CITATION

Jonas D. Gassmann, Kommentierung zu Art. 61 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Gassmann, N. XXX zu Art. 61 DSG.

Art. 61 Violation of duties of care

On complaint, a fine not exceeding 250,000 francs shall be imposed on private persons who wilfully:

a. disclose personal data abroad in violation of Article 16 paragraphs 1 and 2 without satisfying the requirements of Article 17;

b. assign the data processing to a processor without satisfying the requirements of Article 9 paragraphs 1 and 2;

c. fail to comply with the minimum requirements for data security stipulated by the Federal Council in Article 8 paragraph 3.

CONTENT

IN A NUTSHELL

The provision of Art. 61 criminalizes (i) the intentional violation of the specifications during data export, (ii) the intentional violation of the specifications during the transfer of data processing to a commissioned processor, and (iii) the intentional non-compliance with minimum data security requirements. A fine of up to 250,000 Swiss francs may be imposed if one of these offences is committed. In the case of the criminal variant of intentional non-compliance with minimum data security requirements (Art. 61 lit. c), there are justified doubts as to its justiciability.

I. GENERAL

The provision of Art. 61 is new. The Federal Council justified the introduction of this provision in the dispatch by stating that the totally revised Data Protection Act provides for "new elementary obligations" that are "not covered by the existing penal provisions". This is an abstract endangerment offense; the offense is completed when the act is committed, so criminal liability does not require unauthorized third parties to have knowledge of the personal data concerned. 1

The criminal provision of Art. 61 is an application offense. 2

The purpose of Art. 61 is to enforce the obligations of data controllers and processors laid down by law (Art. 16 para. 1 and 2 in conjunction with Art. 17; Art. 9 para. 1 and 2; Art. 8 para. 3) by making their violation punishable. According to the dispatch, the punishment should ultimately contribute to the effective protection of the personality of the persons concerned. Art. 61 lit. a should also be read in the context of the objective of the revision of the FADP, as mentioned by the Federal Council in its report on the evaluation of the FADP of December 9, 2011: the revision should address the increase in data processing, the increasingly international dimension of data processing, and the growing difficulty of continuing to be able to control data once it has been disclosed. 3

The offense of Art. 61 is a special offense: Only those who are responsible for ensuring compliance with the obligations set forth in Art. 61 are eligible as offenders; in the case of legal entities, these are their managers pursuant to Art. 4

29 SCC. By its nature, the provision of Art. 61 is thus primarily directed at persons authorized to give instructions, since they must ensure the fulfillment of the duties in question. Anyone who does not prevent infringements by subordinate employees or does not reverse their effects also qualifies as an offender (Art. 6 para. 2 and 3 of the Criminal Code in conjunction with Art. 64 para. 1 of the FADP).

5 As far as the criminal element of Art. 61 lit. c is concerned, this was repeatedly criticized in the legislative process as being too vague. However, the request for deletion was ultimately not granted. Meyle/Morand/Vasella rightly question the justiciability of the "minimum data security requirements" regulated in the DPA (see below, n. 17 ff.).

II. OBJECTIVE FACTS

6 Art. 61 FADP lists three facts, the fulfillment of which is considered a breach of due diligence obligations. The consequence of a violation on the part of private persons is a fine of up to 250,000 Swiss francs. In particular, the violation of the following three facts is subject to criminal prosecution upon request: Violation of the requirements for data export (Art. 61 lit. a, below n. 7 ff.), violation of the requirements for handing over data processing to a contract processor (Art. 61 lit. b, below n. 12 ff.) and non-compliance with minimum data security requirements (Art. 61 lit. c, below n. 15 ff.).

A. Violation of data export requirements (Art. 61 lit. a)

1. General

7 Under the previous law, anyone who disregarded the legal requirements in the context of a data disclosure to countries without adequate legal data protection remained unpunished. Pursuant to Art. 34 para. 2 lit. a aDSG, only those who took care of protection in the form of a contract but intentionally failed to report this contract to the FDPIC pursuant to Art. 6 para. 3 aDSG or intentionally provided false information in doing so were liable to prosecution.

8 Pursuant to Art. 61 lit. a, anyone who intentionally exports data to a state without adequate data protection and who can neither demonstrate an adequate data protection guarantee nor rely on an exception pursuant to Art. 17 is now liable to prosecution. If the Federal Council has not issued an "adequacy

decision" based on Art. 16 para. 1, personal data may only be disclosed to the state in question under the conditions mentioned in Art. 16 para. 2, with the greatest practical relevance being the conclusion of standard contractual clauses ("standard data protection clauses", lit. d).

Within the scope of the DSGVO, the European Commission repealed the previous standard contractual clauses with effect from September 27, 2021, by implementing Decision (EU) 2021/914 of June 4, 2021, and replaced them with new standard contractual clauses. The FDPIC approved these new standard contractual clauses on August 27, 2021, with the proviso that they be adapted and/or supplemented as necessary in specific cases of application. However, anyone who discloses data to a country that does not have adequate legal data protection cannot be content with merely concluding recognized standard contractual clauses. Rather, the wording of Art. 16 para. 2 lit. d requires that these standard contractual clauses actually ensure "adequate" data protection. The new standard contractual clauses require the parties to (i) additionally ensure that they can comply with the standard contractual clauses regardless of the national law of the importer and (ii) document their assessment in this regard. A transfer impact assessment (TIA) must therefore be carried out and data may only be transferred if this TIA is satisfactory. 9

Art. 10 para. 1 DPA specifies or relativizes that the data exporter must take "appropriate measures" in the case of data disclosure by means of standard contractual clauses to ensure that the data importer complies with the clauses in question. It follows that (under the risk-based approach) a residual risk that the local law of the importer undermines the importer's compliance with the standard contractual clauses may be accepted, as long as measures have been taken to adequately reduce this risk. Cf. the commentary on Art. 16 and 17. 10

2. No criminal liability of the importer

Anyone who (as an exporter) discloses personal data abroad despite knowing that the recipient (importer) of the data does not ensure appropriate data protection despite the contract exposes himself to the risk of criminal liability under Art. 61 lit. a. In contrast, the importer who accepts personal data or uses it in violation of the contract or data protection is not subject to the risk of criminal liability - the only criminal offense under Art. 61 lit. a is the disclosure of personal data. 11

B. Violation of the requirements when transferring data processing to a processor (Art. 61 lit. b)

1. General

12 Pursuant to Art. 61 lit. b, anyone who intentionally hands over data processing to a processor without the requirements of Art. 9 para. 1 and 2 being met is liable to prosecution. According to Art. 9 para. 1, the processing of personal data may be transferred to a processor by contract or by law if (a) the data are processed in the same way as the controller would be permitted to do himself and (b) no legal or contractual obligation of secrecy prohibits the transfer. According to Art. 9 para. 2, the controller must in particular ensure "that the processor is able to guarantee data security". The objective elements of Art. 61 lit. b would be fulfilled, for example, if a company, as the data controller, used a data processor (e.g., a cloud service provider) without having concluded a legally sufficient data processing contract with the data processor.

13 Art. 7 DPA specifies these requirements for commissioned processing: the controller must approve the commissioning of subcontracted processors in advance in a general or specific manner (Art. 7 para. 1 DPA). In the case of a general authorization, the data controller must be informed of any intended change regarding the involvement or substitution of other third parties, and the data controller may object (Art. 7 para. 2 DPA). See the commentary on Art. 9 for more details.

2. No Criminal Liability of the Data Processor (or the Persons Acting on His or Her Behalf)

14 Violation of Art. 9 para. 3, i.e. the order processor's obligation to obtain prior approval from the controller for new subcontractors, is not punishable. Even in the case of a violation of Art. 9 para. 1 or 2, according to the wording of Art. 61 lit. b, the order processor (or the persons acting on his behalf) is not liable to punishment: only the person responsible (or the persons acting on his behalf) can be punished. The same must also apply in the event that the commissioned processor in turn transfers the data processing to a subcontracted processor: norms justifying punishment must be interpreted narrowly.

C. Violation of minimum data security requirements (Art. 61 lit. c)

1. General

According to Art. 61 lit. c, anyone who intentionally fails to comply with the minimum data security requirements issued by the Federal Council pursuant to Art. 8 para. 3 is liable to prosecution. Reference is made here to the first section ("Data security", Art. 1 ff.) of the first chapter of the DPA. 15

The provision of Art. 61 lit. c is an abstract endangerment offense designed as a blanket standard (cf. already above, n. 1); a "data breach" need not have occurred. And conversely, not every "data breach" results in criminal liability - if there is a "data breach" but the "minimum data security requirements" have been met, there is no criminal liability. 16

2. Violation of the principles of Art. 1 DPA

The provision of Art. 1 DPA contains principles that the controller and the processor must observe when determining the appropriate level of protection and the measures suitable for it. These are general guidelines, and not concrete (minimum) data security requirements. According to the correct opinion of Meyle/Morand/Vasella, this very general provision regarding the procedure of the controller in determining security measures is not justiciable - it is not apparent which "minimum requirements" for data security within the meaning of Art. 8 para. 3 should result from Art. 1 DPA. 17

If the controller does not adhere to the principles of Art. 1 DPA, for example, if he does not determine the need for protection of personal data according to the criteria provided for in para. 1 or if he does not take relevant criteria into account in the risk assessment as provided for in para. 2 or if he does not review his measures "over the entire processing period" as provided for in para. 5, this does not indicate a violation of "minimum requirements" for data security: on the one hand, Art. 1 DPA does not define such requirements, but only contains guidelines on how to achieve them, and on the other hand, a controller may also implement effective measures to ensure adequate data security without strictly following Art. 1 DPA. 18

3. Violation of the objectives of Art. 2 DPA.

19 The provision of Art. 2 DPA defines data security protection objectives that the controller and the processor must achieve by means of technical and organizational measures: Confidentiality (lit. a), Availability (lit. b), Integrity (lit. c) and Traceability (lit. d).

20 These protection goals are identical to those pursuant to Art. 6 para. 2 of the Federal Act of 18 December 2020 on Information Security at the Confederation (Information Security Act). Like the principles pursuant to Art. 1 DPA, the objectives pursuant to Art. 2 DPA are also very general (which is evident from the heading "Objectives" alone) and no "minimum requirements" for data security within the meaning of Art. 8 para. 3 can be derived from them. What concrete technical and organizational measures would have to be implemented is not clear from this. Meyle/Morand/Vasella rightly question the justiciability of this provision as well.

4. Violation of the provision on technical and organizational measures (Art. 3 DPA)

21 The provision of Art. 3 DPO contains specifications for technical and organizational measures and thus concretizes data security. However, it does not contain any "minimum requirements" for data security within the meaning of Art. 8 para. 3 (either); instead, Art. 3 DPO merely concretizes the protection goals contained in Art. 2 DPO.

22 In a broad interpretation, Art. DPO could be interpreted as containing "minimum requirements" to the extent that, according to this provision, the protection goals as defined in Art. 2 DPO must be "ensured". However, such an interpretation would mean that every violation of a protection goal would be evidence that a suitable measure was lacking. This in turn would not be compatible with the risk-based approach recognized in the area of data security. In this respect, the word "ensure" should be interpreted as "strive for".

23 Art. 3 DPA, together with Art. 1 and 2 DPA, is to be read as a concretization of the concept of data security, without "minimum requirements" for data security being derived from it. In addition, the controller and the processor do not necessarily have to take into account all the protection objectives pursuant to Art. 3 DPA for their technical and organizational measures. The justiciability of this provision is also rightly questioned by Meyle/Morand/Vasella.

5. Omission of logging in accordance with Art. 4 DPA

The provision of Art. 4 DPA takes over the previous Art. 10 DPA. The purpose of logging is to ensure purpose limitation. 24

As a rule, logging is not a "minimum requirement for data security" as mentioned in Art. 61 lit. c (even though Art. 4 DPA is listed under the first section of the DPA, "Data Security"), and failure to log cannot be punishable in this respect. Criminal liability would be conceivable by way of exception if a prosecuting authority could prove in an individual case that logging as a measure of traceability was also indirectly intended to serve data security and that the accused person was aware of this at least in broad outline. 25

6. Failure to draw up processing regulations in accordance with Art. 5 et seq. DPA

The provisions of Art. 5 f. FADP take over the previous Art. 11 FADP and Art. 21 FADP. In the explanatory report FADP, the Federal Council itself states that the creation of processing regulations is about accountability - i.e. not about data security. This is not altered by the fact that an obligation to draw up such regulations only exists in the case of increased risk. 26

A "minimum requirement for data security", as mentioned in Art. 61 lit. c, is the creation of "processing regulations" (even though Art. 5 f. DPA are listed under the first section "data security" of the DPA) is not and the omission of this preparation can in this respect also not be punishable. 27

7. Consideration of costs in determining appropriate data security and appropriate measures

Pursuant to Art. 1 para. 1 DPA, in order to ensure adequate data security, the controller and the processor must determine the need for protection of the personal data and establish "the appropriate technical and organizational measures in view of the risk." Art. 1 para. 2 FADP circumscribes criteria for assessing the need for protection of the personal data and Art. 1 para. 3 FADP circumscribes criteria for assessing the risk to the personality or fundamental rights of the data subject. The higher the need for protection of the personal data and/or the higher the risk mentioned, the stricter the requirements for the measures. According to Art. 1 para. 4 DPA, the "implementation costs" 28

must also be taken into account when determining the technical and organizational measures.

29 According to the Federal Council, implementation costs should be understood broadly and include not only necessary financial resources, but also personnel and time resources. The costs are already to be taken into account when determining which measures are "appropriate" and which are not. Meyle/Morand/Vasella rightly point out that the view taken by the Federal Council, according to which data controllers and processors "cannot exempt themselves from the obligation of adequate data security on the grounds that excessive costs are involved", would render the provision of Art. 1 para. 4 DPA meaningless: "only" "adequate" security is required, and costs must be included as a criterion in determining adequacy.

30 The "minimum requirements for data security" are thus not violated (and it is not punishable) if the controller or the processor also take the costs, among other things, into account when determining the appropriate data security and the appropriate measures.

III. SUBJECTIVE ELEMENTS OF THE OFFENCE

31 From a subjective point of view, the elements of the offense under Art. 61 require intent, with contingent intent being sufficient. The offender acts with contingent intent if, although he does not know with certainty that his conduct will violate the requirements for data export (Art. 16 para. 1 and 2; Art. 17) or for the transfer of data processing to a processor (Art. 9 para. 1 and 2) or if he does not comply with the minimum requirements for data security (Art. 8 para. 3 in conjunction with Art. 1 et seq. FADP), he accepts or accepts that he may commit a violation.

32 In the case of the criminal offense under Art. 61 lit. b, there is contingent intent if, when transferring data processing to a processor, the perpetrator at least accepts that the processor will (i) process the data in violation of the law or (ii) fail to ensure data security. Decisive for the answer to the question of whether such an acceptance exists are the circumstances under which the order processor in question was "examined" and ultimately selected. The provisions of Art. 9 are very open and vaguely formulated (especially in comparison to the parallel provision of Art. 28 DSGVO), which in practice is likely to make it more difficult for the criminal authorities to prove criminal conduct in indi-

vidual cases (apart from the fact that with regard to the justiciability of the criminal variant of intentional non-compliance with minimum data security requirements, there are in any case well-founded doubts, see above n. 17 ff.). In contrast, merely (unpunished) negligent conduct would be assumed, for example, if the perpetrator assumed, based on external legal advice obtained (about which no doubts had to arise), that a certain commissioned data processing contract was legally sufficient, but this turned out to be insufficient.

IV. ILLEGALITY AND CULPABILITY

Cf. OC-Gassmann on Art. 60, n. 26 f.

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 62 FADP

A commentary by Jonas D. Gassmann

SUGGESTED CITATION

Jonas D. Gassmann, Kommentierung zu Art. 62 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Gassmann, N. XXX zu Art. 62 DSG.

Art. 62 Violation of the professional duty of confidentiality

[1] Any person who, while practising his or her profession, acquires knowledge of secret personal data for the purpose of that profession but thereafter wilfully discloses such data shall on complaint be liable to a fine not exceeding 250,000 francs.

[2] The same penalty shall apply to any person who wilfully discloses secret personal data that has come to his or her knowledge while carrying on an activity for or while training with a person subject to a duty of confidentiality.

[3] The disclosure of secret personal data after ceasing to practise a profession or after completing training is also a criminal offence.

CONTENT

IN A NUTSHELL

The provision of Art. 62 deals with the so-called "minor professional secrecy". It criminalizes the intentional disclosure of secret personal data learned during the exercise of a profession. Compared to the previous law, the offense of "breach of professional secrecy" is considerably expanded. A fine of up to 250,000 Swiss francs may be imposed if this offense is committed.

I. GENERAL

The provision of Art. 62 builds on Art. 35 aDSG, but considerably expands the elements of the offense of "breach of professional secrecy". It is no longer merely a matter of disclosing "secret personal data or personality profiles requiring special protection", but rather "secret personal data" in general. The Federal Council has justified this extension of the protection of secrets to all types of personal data with the further development of information and communication technology and the accompanying massive expansion of the collection of data. Art. 62 aims to protect the secrecy of those persons who entrust their personal data to third parties. 1

The penal provision of Art. 62 is an application offense. 2

According to the Federal Council, Art. 62 is intended to close gaps "that arise due to the restricted circle of offenders under Articles 320 and 321 SCC (special offences)". The duty of confidentiality should also apply to persons who do not fall under Art. 320 or 321 SCC. The legislator preferred this solution to an expansion of the (general) criminal law provisions, as he did not consider it expedient to also expand the right to refuse to testify, which the procedural laws generally provide for the professions mentioned in Art. 321 SCC. Terminologically, however, the "minor professional secrecy" is based on the "major" professional secrecy pursuant to Art. 321 StGB (which applies in particular to doctors, lawyers, clergy, etc.) and on banking secrecy pursuant to Art. 47 BankG. 3

The Federal Council already refrained from mentioning the disclosure of data processed for commercial purposes in the preparation of the draft. This was retained by the parliamentary chambers. 4

5 The preliminary draft still provided for a prison sentence of up to three years or a fine in the event of a breach of professional secrecy (Art. 52 VE-FADP). According to the explanatory report VE-FADP, the tightening was intended because a fine would no longer correspond to the severity of possible infringements, especially with regard to Art. 321 SCC. In the consultation, however, various participants found the penalty to be too high, which is why a fine of 250,000 Swiss francs was introduced. The maximum fine of 250,000 Swiss francs was ultimately retained, as this amount was considered by the majority to be proportionate and sufficiently deterrent.

6 Overall, it is astonishing that the provision of Art. 62, which is unusually harsh in view of the broad scope of application and the range of fines, especially in international comparison, was hardly discussed (in terms of content) in the parliamentary deliberations.

II. VIOLATION OF PROFESSIONAL CONFIDENTIALITY

A. Circle of Offenders

7 Art. 62 FADP does not cover all persons who disclose secret personal data of another. According to the wording, it covers persons who exercise a profession that requires the disclosure of secret personal data. Art. 62 FADP is thus designed as a special offense. In contrast to Art. 321 StGB, however, no specific professional affiliation is required. In order to be subject to a duty of confidentiality (which goes beyond business and manufacturing secrets within the meaning of Art. 321a para. 4 of the Swiss Code of Obligations), since the introduction of Art. 62 employees no longer have to have a special status such as that of lawyers, doctors, bank employees or civil servants: it is sufficient that they have gained knowledge of "secret personal data" in the course of their professional activities. By virtue of Art. 2 para. 1, the penal provision of Art. 62 also covers members of federal authorities.

8 According to Art. 62 para. 3, not only the current exercise of the profession is covered, but the protection of the secret also lasts if the obligated persons have given up the profession or have completed their corresponding training. This corresponds to the provision of Art. 35 para. 3 aDSG. It can be assumed that this means (by analogy with Art. 321 SCC) that the professional duty of confidentiality continues to exist until the death of the person bound to secrecy, irrespective of the continuation of the business relationship.

According to Art. 62 para. 2, auxiliary persons (employees; commissioned data processors) and trainees (including interns) are also subject to criminal liability. This extension corresponds to the provision of Art. 35 para. 2 aDSG. Third parties who act in place of the primary holder of secrets are, according to the view expressed here, subject to the obligation to maintain secrecy as auxiliary persons. 9

Not liable to prosecution under Art. 62 is anyone who discloses secret personal data that the person holding the secret or an auxiliary person has disclosed to him or her in violation of Art. 62. 10

Art. 62 FADP does not provide for direct criminal liability of the company. In order to counteract this, the criminal liability of the governing bodies was increased by applying Art. 6 of the Criminal Code in addition to Art. 29 of the Penal Code. 11

B. Objective elements of the offence

According to Art. 62 para. 1, "[w]hoever intentionally discloses secret personal data of which he or she has become aware in the exercise of his or her profession which requires knowledge of such data" is liable to prosecution. The objective element of the offense first requires that it be "secret" personal data. Personal data is any information relating to an identified or identifiable natural person (Art. 5 lit. a). Art. 62 itself does not define which personal data is considered "secret", but the message refers to the material concept of secrecy in criminal law. A secret protected by criminal law exists if (i) the fact is not generally known or accessible, (ii) the person keeping the secret has an interest worthy of protection in the limited knowledge, and (iii) he also has the will to do so. 12

Furthermore, the perpetrator must have gained knowledge of the personal data in the course of exercising his profession. This includes, on the one hand, data that the client/secret owner has entrusted to the person holding the secret and, on the other hand, data that the person holding the secret has obtained himself in the course of exercising his profession. 13

The concept of "disclosure" of secret personal data corresponds to that in Art. 320 and 321 SCC: A disclosure occurs if the person who holds the secret brings secret personal data to the attention of a third party who is not authorized to do so or enables the third party to take note of the data, whereby it is 14

irrelevant how this occurs (e.g. direct forwarding of secret personal data or insufficient file storage so that the third party is enabled to take note). If the data has been effectively anonymized, pseudonymized or encrypted prior to forwarding so that the third party cannot take note of the data, there is no disclosure in accordance with the offence.

On the other hand, disclosure is also deemed to have occurred if secret personal data is passed on to an internal employee or to an external service provider. Situations in which third parties disclose personal data to an employee in connection with a request for strict confidentiality can be problematic. One might think of an employee in the HR department of a company who is informed by another employee of a grievance within the company, with the latter demanding that his identity be kept secret. On the one hand, the employee in the HR department may be liable to prosecution if he (nevertheless) discloses the identity internally; on the other hand, the company will have to accept credit for the knowledge of certain employees. Here, clear regulations are needed in practice as to how such reports are handled and what is communicated, to whom, when and how.

15 It is not clear from the wording of Art. 62 or from the dispatch who is the owner of the secret protected by this provision. According to the dispatch, however, the provision of Art. 62 is explicitly linked to the professional secrecy of Art. 321 SCC, which is why it is justified to understand Art. 62 as "professional secrecy" and not as a purely data protection law norm: The owner of the secret is the person who has entrusted the professional person with his secret for the exercise of his profession. Accordingly, the trust of the owner of the secret in the confidentiality of the communication to the professional person is protected, and only the breach of this trust (i.e. not every data protection violation) is punishable. Article 62 protects the trust placed in a professional person that he or she will keep the secret entrusted to him or her for the purpose of exercising his or her profession - regardless of the existence of a direct contractual relationship with the person to whom the secret is entrusted. According to the view expressed here, only a disclosure of personal data that takes place in disappointment of a justified expectation of the owner of the secret that the same will be treated confidentially can constitute a criminal offense. A company can manage the customer's/secret owner's expectation by listing in its privacy policy the categories of third parties to whom the company discloses personal data. Provided that the reference in the privacy

statement is "sufficiently clear," the secrecy owner will no longer be able to claim a "legitimate expectation" that the personal data in question will be treated confidentially.

Even if Art. 62 is understood in this narrower sense, this provision is still very broad and indeterminate: When a trust in confidentiality protected by criminal law can be assumed is not (and was not under Art. 35 aDSG) clarified. What is clear, however, is that not every fact disclosed to a professional person that is not generally known deserves this protection. With Rosenthal/Gubler (p. 61), it must be required (in view of the requirements for a criminal provision arising from the requirement of certainty under Art. 1 StGB) that (i) a justified expectation has been created in the owner of the secret that his will to keep the secret will be respected and (ii) the secret has been disclosed to the owner of the secret or his organization within this framework. Thus, an at least tacit agreement of confidentiality is required. 16

C. Subjective Elements of the Crime

From a subjective point of view, intent on the part of the perpetrator is required, i.e. the perpetrator must be aware of the duty of confidentiality, the secret nature of the personal data and the disclosure. It is sufficient if the perpetrator considers it possible that third parties could gain knowledge of the personal data, but nevertheless acts because he accepts this (contingent intent). In practice, it is not uncommon for criminal liability to fail because knowledge of the obligation to maintain secrecy and the confidential nature of the personal data cannot be proven, namely if there are no indications that the company in question has imparted the relevant knowledge to its employees. 17

III. ILLEGALITY AND CULPABILITY

Cf. OC-Gassmann on Art. 60, n. 26 f. In particular, the disclosure may be justified by the consent of the owner of the secret, whereby the principles developed by case law and dogmatics in Art. 321 no. 2 SCC apply mutatis mutandis. Legal regulations that permit disclosure (Art. 14 StGB) or even make it obligatory may also be considered. One might think here of procedural duties to cooperate. 18

IV. DELIMITATION AND COMPETITION

20 In addition to Art. 320 SCC (violation of official secrecy) and Art. 321 SCC (violation of professional secrecy), Art. 62 also protects the owner of a secret from unlawful disclosure of secret data to third parties. However, Art. 62 closes the loophole created by the limited perpetration and consequently is in unreal ideal competition with the two provisions of the Criminal Code. Analogous to Art. 35 aDSG, the violation of data secrecy is absorbed into Art. 320 and 321 SCC (consumption).

21 If the facts of Art. 47 BankG are also fulfilled, this takes precedence as a special norm.

The author would like to express his sincere thanks to MLaw Antonia Straden for her assistance in commenting on this article.

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 63 FADP

A commentary by Jonas D. Gassmann

SUGGESTED CITATION

Jonas D. Gassmann, Kommentierung zu Art. 63 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Gassmann, N. XXX zu Art. 63 DSG.

Art. 63 Disregard of decisions

Any private person who wilfully fails to comply with a ruling issued by the FDPIC or a decision of the appeal courts that refers to the penalty under this Article shall be liable to a fine not exceeding 250,000 francs.

CONTENT

IN A NUTSHELL

The provision of Art. 63 makes it a criminal offense to intentionally fail to comply with an order of the FDPIC or a decision of an appellate body. To be punishable, the order or decision must be accompanied by a corresponding threat of punishment and it must be sufficiently clear to the addressee from the order or decision what he must do or refrain from doing. If this requirement is met, a fine of up to 250,000 Swiss francs may be imposed.

I. GENERAL

Art. 63 is a disobedience offence designed as a blanket provision. Comparable penal provisions are frequently found in secondary criminal law, albeit with massively lower penalties. As a lex specialis, the provision of Art. 63 takes precedence over the provision of Art. 292 StGB (disobedience of official orders) contained in the core criminal law. 1

The provision of Art. 63 was added to the law only after the consultation. In the opinion of the legislator, recourse to Art. 292 StGB would not have been sufficient because the threat of punishment was too low. In the consultation process, there were various criticisms that the new penal provisions were formulated too openly. Art. 63 now allows the FDPIC to order compliance with obligations under the FADP and to combine this with a threat of punishment. The obligation can thus be specified in the order to the extent that it is sufficiently clear to the addressee what he must do or refrain from doing. 2

The criminal provision of Art. 63 is an official offence. 3

The purpose of the provision of Art. 63 is, on the one hand, to compensate for the omitted penal provisions (concerning reports to the FDPIC) in comparison to the VE-FADP and, on the other hand, to take into account "the questions regarding the principle nulla poena sine lege, as they were frequently raised in the consultation". 4

According to the Federal Council, the solution created by Art. 63 "allows the relevant provisions of the FADP to continue to be drafted in a sufficiently general form without at the same time coming into conflict with the criminal law requirements for the precision of a legal regulation." In addition, according to the Federal Council, it facilitates the work of the competent law enforce- 5

ment authorities, which would take into account the concerns partially expressed in the consultation.

6 This provision is aimed at the enforcement of orders of the FDPIC within the meaning of Art. 51, which the FDPIC issues after an investigation has been carried out, and the enforcement of decisions of appeal bodies. In contrast, the threat of a fine under Art. 60 para. 2 concerns the intentional provision of false information and the intentional refusal to cooperate in an investigation by the FDPIC.

7 The criminal offence of Art. 63 is a special offence: only those who are the addressee of a decision of the FDPIC or of a decision of an appellate authority can be considered as perpetrators. Other persons can at most be considered as instigators. If the order of the FDPIC or the decision of an appellate body is addressed to a company, criminal liability arises on the basis of Art. 29 SCC for a management person: The duty incumbent on the company that gives rise to the penalty is attributed to the natural person. Anyone who does not prevent violations by subordinate employees or who does not reverse the effects of such violations also qualifies as a perpetrator (Art. 6 para. 2 and 3 of the Criminal Code in conjunction with Art. 64 para. 1 of the FADP).

II. DISREGARD OF AN ORDER OF THE FDPIC OR A DECISION OF AN APPELLATE AUTHORITY

A. Objective facts

1. Order of the FDPIC or decision of an appeal body

8 A punishment under Art. 63 presupposes that a specific person is prescribed a sufficiently concretely described course of conduct in a validly issued and served order or decision, with the threat of a sanction under this provision in the event of non-compliance. There is no obligation on the part of the FDPIC or the appellate bodies to attach the threat of sanctions pursuant to Art. 63 to their orders or decisions. However, in order to make compliance with the rulings or decisions more likely, the FDPIC or the appeal bodies should make regular use of this possibility.

9 An order of the FDPIC means a sovereign act addressed by the FDPIC to a specific person on the basis of Art. 51, by which a specific legal relationship

under administrative law is regulated in a legally binding and enforceable manner. It is required - as in the case of Art. 292 StGB - that the order contains a concrete instruction of conduct (to do, to tolerate or to refrain from doing something); a mere declaratory order does not satisfy this requirement. A general order is also not a suitable object of crime. A specific instruction to act includes, for example, an order to adapt or stop a certain processing of personal data or to refrain from disclosing personal data abroad (cf. on the whole OK-Fanger/Oehri on Art. 51 FADP). The order must be "legally existent" (i.e. it must not contain any serious defect that would render it null and void), must have been effectively received by the addressee and must be formally final.

A decision of an appellate authority means a judgment of a court that decides on an appeal against an order of the FDPIC, i.e. a judgment of the Federal Administrative Court (Art. 33 lit. d VGG) or of the Federal Supreme Court (Art. 86 para. 1 lit. a BGG). 10

According to Art. 1 SCC, punishment can only be considered if the applicable penal provision satisfies the requirement of certainty. Since Art. 63 itself does not describe the offence, but refers to the order of the FDPIC or the decision of an appellate body, the order or decision that is subject to the penalty must also meet the requirements of the principle of certainty. The principle of legality requires that the obligation imposed in the order or decision is "sufficiently clearly circumscribed" (cf. already above, n. 9); in other words, it must be clear to the addressee of the order or decision what specific conduct is required of him. 11

2. Non-compliance

As an act, the offense under Article 63 requires that the addressee of the order or decision does not comply with the order or decision. What is meant by non-compliance is determined by the content of the order or decision. If, for example, the FDPIC orders a ban on the disclosure of personal data abroad, the disclosure in question constitutes a "failure to comply"; if the perpetrator discloses personal data abroad several times despite the ban, he or she fulfills the elements of the crime under Art. 63 several times. 12

B. Subjective Elements of the Offence

13 From a subjective point of view, the offense under Art. 63 requires intent, although contingent intent is sufficient. The offender acts with contingent intent if, although he does not know with certainty that his conduct will violate the order or decision, he accepts or accepts that he may commit a violation.

III. UNLAWFULNESS AND CULPABILITY

Cf. OK-Gassmann, Art. 60 FADP, n. 26 f.

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 64 FADP

A commentary by Jonas D. Gassmann

SUGGESTED CITATION

Jonas D. Gassmann, Kommentierung zu Art. 64 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Gassmann, N. XXX zu Art. 64 DSG.

Art. 64 Corporate criminal liability

[1] The criminal liability of businesses is governed by Articles 6 and 7 of the Federal Act of 22 March 1974 on Administrative Criminal Law (ACLA).

[2] If a fine not exceeding 50,000 francs is under consideration and if the identification of the perpetrators in accordance with Article 6 ACLA requires measures that would be disproportionate in view of the potential penalty, the authority may decide not to pursue these persons but instead to order the business to pay the fine (Art. 7 ACLA).

CONTENT

IN A NUTSHELL

By referring to two isolated provisions of the Federal Law on Administrative Criminal Law (VStrR), the business owner liability is introduced in the FADP. Art. 64 makes it possible, in the case of an infringement in a business establishment, under certain circumstances to pass on a fine actually to be imposed on the responsible natural person to the business establishment, if this fine amounts to a maximum of 50,000 Swiss francs.

I. GENERAL

Because it is the responsibility of the cantons to prosecute and judge criminal acts within the meaning of Chapter 8 (Art. 65 para. 1), the Federal Act of 22 March 1974 on Administrative Criminal Law (VStrR) is in principle not applicable (Art. 1 VStrR e contrario). However, Art. 64 para. 1 now expressly refers to Art. 6 and 7 of the Criminal Procedure Code with regard to offences in business establishments. 1

With the reference to Art. 6 of the Criminal Procedure Code (determination of the person responsible for an infringement in a business establishment) and Art. 7 of the Criminal Procedure Code (subsidiary responsibility of the business establishment), the liability of the principal is introduced in the FADP. This is intended to enable "an appropriate allocation of criminal responsibility in companies", i.e. to its management level (management persons with decision-making and directive powers). 2

The maximum amount of the fine pursuant to para. 2 (which modifies the provision of Art. 7 FADP), up to which the business enterprise (instead of the natural person) may be ordered to pay the fine, was still set at 100,000 Swiss francs in Art. 53 VE-FADP. Controversial statements in the consultation process led to the maximum fine ultimately being set at 50,000 francs. The substantially higher maximum fine compared to Art. 7 FADP can be explained by the fact that the range of fines for violations of the FADP (fines of up to 250,000 Swiss francs) far exceeds the amount provided for in Art. 7 FADP (5,000 Swiss francs), and the maximum fine had to be increased so that in practice there would still be room for application of the provision of Art. 64 para. 2. 3

II. OFFENSES IN BUSINESS ESTABLISHMENTS

A. Applicability of Art. 6 and 7 CCC (para. 1)

4 Art. 64 para. 1 refers to Art. 6 and 7 of the Criminal Code for "offences in business establishments", and thus to two isolated articles within the Criminal Code. The assessment of the fine, for example, is therefore not based on Art. 8 CCC, but on Art. 106 para. 3 SCC. Since, according to Art. 1 of the Criminal Code, the Criminal Code does not apply to criminal violations of the FADP, this explicit reference is necessary if a kind of "principal's liability" is to be introduced into the FADP (see also above, n. 1 ff.).

5 Any entrepreneurial activity in which capital and labor are actively used to participate in economic life is considered a "business operation". It is therefore a matter of criminal acts committed in the course of economic activities in a company. Art. 6 para. 1 of the Criminal Code does not cover acts that are committed merely on the occasion of carrying out business activities.

6 Art. 6 para. 1 ICC establishes the so-called perpetrator principle: the perpetrator is the one who has committed the act. For example, an employee who uses a tool of an online service provider without being asked and authorized to do so by a superior for the performance of his or her duties, in the course of which personal data is processed, but the employee has not taken care to conclude a legally sufficient data processing contract (criminal liability under Art. 61 para. 1 lit. b). Another example would be the unauthorized disclosure of secret personal data by an employee to a third party in the exercise of her profession (criminal liability under Art. 62).

7 The prerequisite for the principal's liability (principal's liability within the meaning of Art. 6 para. 2 VStrR) is, from an objective point of view, the existence of a guarantor's duty, whereby this cannot be derived from Art. 6 para. 2 VStrR, but follows "from the responsibility for the business as a source of danger and/or from the responsibility for the conduct of subordinates". One might think here, for example, of a compliance officer who is contractually responsible for ensuring compliance with the requirements of data protection law in the company or of the personnel officer who is contractually responsible for the processing of personnel data. Delegation of responsibility is permitted by law, whereby the delegating person remains responsible for the selection, instruction and supervision of the person concerned. Another prerequisite is

the existence of authority on the part of the principal: In order for the principal's liability to apply, it must have been possible for the principal to prevent the act or to nullify its effects. From a subjective point of view, Art. 6 para. 2 VStrR requires intent or negligence. In the case of offences which (like the criminal provisions of Chapter 8 of the FADP) are structured as intentional offences, however, it is disputed whether it is sufficient for the applicability of the principal's liability and thus for the principal's criminal liability that the latter merely negligently failed to prevent the infringement or to nullify its effects. According to the opinion expressed here, it is required for the applicability of the principal's liability that the principal has violated the guarantor's obligation at least possibly intentionally. If the directly acting perpetrator (who committed the infringement) acted merely negligently, the principal's liability is excluded from the outset in the case of such incidental acts.

If the principal, employer, client or person represented is a legal entity, a general or limited partnership, a sole proprietorship or a group of persons without legal personality, Art. 6 para. 2 Criminal Code applies "to the guilty organs, members of organs, managing partners, persons actually in charge or liquidators" (Art. 6 para. 3 Criminal Code; cf. also Art. 29 SCC). 8

B. Sentencing of the business to a fine (para. 2)

1. General

Art. 64 para. 2 is based on the provision of Art. 7 para. 1 VStrR, but adapts the scope of application to the maximum fine provided for in the FADP and speaks more generically of the "business establishment" instead of the "legal person", "collective or limited partnership" and the "sole proprietorship" (cf. also above, n. 3 and n. 5). 9

Pursuant to Art. 64 para. 2, a fine may be imposed on a business establishment (instead of the criminal natural persons) in the event of a criminal offence in 10

the business establishment (committed by one or more natural persons; see below, n. 11 f.) if

- a fine of no more than 50,000 Swiss francs is eligible (see below, n. 13 f.) and (cumulatively)
- the investigation of the persons liable to prosecution under Art. 6 CCC would require investigative measures that would be disproportionate to the penalty imposed (see below, n. 15 f.).

2. Offence in the course of business

11 In order to impose a fine on a business operation, it is first of all necessary that there is an "infringement in the course of business". All objective and subjective elements of the offense for which the business operation is to be fined must be fulfilled, and there must be no grounds for justification or exclusion of guilt. For the concept of "business operation" see above, n. 5.

12 In practice, however, the subjective elements of the offense will not be provable, since the offending natural persons are precisely not identifiable. In order to overcome this hurdle and not exclude the application of Art. 64 from the outset, culpability must be "objectified" or the requirements for proving the subjective elements of the offense must be relaxed, for example by the criminal authority being content with the finding "that the intention clearly results from the act committed." In any case, however, there is no room for the application of Art. 64 if it is established that the subjective elements of the offense are not fulfilled in the case of the persons alleged to have committed the offense within the business operations.

3. Fine of a maximum of 50,000 francs

13 According to Art. 7 para. 1 ICC, the upper limit of the amount of the fine up to which it is possible to order a company instead of a natural person to pay a fine is 5,000 francs. This upper limit corresponds to half of the maximum fine of 10,000 francs provided for in Art. 106 para. 1 SCC. In deviation from Art. 106 para. 1 SCC, the maximum amount of the fine in the scope of application of the FADP (pursuant to Arts. 60-63) is 250,000 francs. In view of this substantially higher maximum amount, an increase also in the upper limit of the fine amount up to which a conviction of a business operation is possible was

imperative. According to Art. 64 para. 2, this upper limit is 50,000 francs, which corresponds to 1/5 of the maximum fine amount of 250,000 francs.

According to Art. 106 para. 3 SCC, in determining the amount of the fine, the court shall take into account the circumstances of the offender "so that he suffers the penalty appropriate to his fault." Because the perpetrator of the offense precisely cannot be located, the fine is to be assessed on the basis of objective fault. The circumstances of the specific violation, such as the lack of a company-internal division into individual areas of responsibility, are decisive. 14

4. Investigative measures to identify the offending persons would be disproportionate

The circumstances of the individual case are also relevant when examining whether investigative measures to identify the offending persons would be disproportionate with regard to the forfeited penalty. Because Art. 64 para. 2 is an "optional provision", the criminal authorities have a relatively considerable discretion in determining whether this provision should be applied (and thus also in answering the question of whether investigative measures to identify the offending persons would be disproportionate). There is no entitlement to the application of Art. 64 para. 2, nor can the criminal authority simply choose between action against the offending natural persons and against the business operation. Before the competent criminal authority can consider punishing the business operation on the basis of Art. 64, it must conduct "a minimum of investigative measures" to identify the offending natural persons; it is not acceptable for the criminal authority to rely on Art. 64 out of sheer convenience. When (further) investigative measures would be disproportionate must also be assessed with a view to the amount of the (potentially) forfeited fine, for which the investigations must in any case have gone so far that the amount can at least be roughly estimated. 15

In the case of FADP violations subject to penalties, it will often be clearly determined from an organizational point of view or at least relatively easy to determine in the specific case who performed the actions in question (e.g., response to a request for information or release of the privacy statement). In this respect, the practical relevance of the provision of Art. 64 is likely to be rather low; convictions of business entities to pay a fine are likely to remain the exception. 16

5. Passing on the Fine

17 If the above-mentioned conditions are met, the competent criminal authority may pass on the fine to the business enterprise. In determining the amount of the fine, the culpability and the financial circumstances of the natural person(s) who actually committed the offence are decisive, and not those of the business operation.

18 If only certain natural persons responsible for the infringement can be identified, but not others, it is debatable whether it is possible to pass on the fine applicable to the persons not identified. It is correct to require that passing on is also possible in this constellation.

BIBLIOGRAPHY

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.

MATERIALIS

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 Än-

derung 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.

COMMENTARY ON

Art. 65 FADP

A commentary by Jonas D. Gassmann

SUGGESTED CITATION

Jonas D. Gassmann, Kommentierung zu Art. 65 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Gassmann, N. XXX zu Art. 65 DSG.

Art. 65 Jurisdiction

[1] The prosecution and the adjudication of criminal acts is a matter for the cantons.

[2] The FDPIC may file a complaint with the competent prosecution authority and exercise the rights of a private claimant in the proceedings.

CONTENT

IN A NUTSHELL

As already standardized in the Federal Constitution and the Code of Criminal Procedure, the prosecution and adjudication of criminal acts are the responsibility of the cantons according to Chapter 8 of the Data Protection Act. The FDPIC has the right to file a complaint and may constitute itself as a private plaintiff in criminal proceedings.

I. GENERAL

The provision of Art. 65 para. 1 is derived from Art. 123 para. 2 FC, according to which jurisdiction in criminal matters and for the execution of sentences and measures lies primarily and principally with the cantons. It coincides with the provision of Art. 22 Code of Criminal Procedure. Art. 65 para. 1 is of a purely declaratory nature in that this provision does not establish federal competence and thus no departure from the cantonal competence already provided for under the aforementioned provisions. In other words, even without an explicit norm, the cantons would be responsible for prosecuting and adjudicating criminal acts under Chapter 8. 1

The provision of Art. 65 para. 1 was already envisaged in this way in the preliminary draft. In the consultation procedure, the majority of the cantons opposed the idea that the prosecution and adjudication of punishable acts should continue to be the responsibility of the cantons. The reason given for this opposition was the fear that criminal proceedings could increase due to the higher number of unlawful acts and the harsher sanctions, which would require the employment of specialized staff. It was also argued that cantonal jurisdiction would make uniform enforcement of data protection law more difficult. 2

Art. 65 para. 2 strengthens the position of the FDPIC by expressly granting it the right to file criminal charges and to constitute itself in criminal proceedings as a private plaintiff within the meaning of Art. 118 CPC et seq. 3

The provision of Art. 65 para. 2 was not yet included in the preliminary draft, but only in the draft. In the consultation process, there were several calls for the FDPIC to be empowered to impose administrative sanctions. In contrast to European law, however, it was decided against a sanctioning possibility by 4

the FDPIC. Instead, the lack of authority to impose administrative sanctions was compensated for by the introduction of other provisions in the FADP. These include, in particular, Art. 65 para. 2, whereby the FDPIC can file a complaint with the cantonal criminal authority and exercise the rights of a private plaintiff in criminal proceedings, or the penalty provisions of Art. 60 para. 2 and of Art. 63.

II. COMPETENCE FOR CRIMINAL PROSECUTION AND JURISDICTION

A. Cantonal jurisdiction (para. 1)

5 Both the prosecution and the adjudication of criminal acts under Chapter 8 fall within the jurisdiction of the cantons (so-called original cantonal jurisdiction).

6 In principle, the Federal Act of 22 March 1974 on Administrative Criminal Law (VStrR) is therefore not applicable (for its applicability, it would be a prerequisite that the aforementioned jurisdiction would lie with an administrative authority of the Confederation, Art. 1 VStrR). However, by virtue of an explicit reference in Art. 64 para. 1, Articles 6 and 7 of the Criminal Procedure Code apply to offences committed in business establishments. This reference does not change the aforementioned cantonal jurisdiction.

7 The local jurisdiction is governed by the general rules of jurisdiction of Art. 31 et seq. Code of Criminal Procedure.

B. Multiple jurisdiction

8 Art. 65 does not comment on the situation where both cantonal and federal jurisdiction exists in a criminal case. In this case, an offender who violates not only one or more elements of the offences in Chapter 8, but also one or more elements of the offences that are subject to federal jurisdiction, is to be considered.

9 In the absence of an explicit provision, reference must be made here to Article 26 para. 2 of the Code of Criminal Procedure: According to this provision, the Office of the Attorney General of the Confederation "may order the unifi-

cation of proceedings in the hands of the federal authorities or the cantonal authorities."

III. RIGHTS OF THE FDPIC (PARA. 2)

A. Right of notification

The FDPIC has the right (but not the obligation) to file a complaint with the competent prosecuting authority. However, he does not have the right to file a criminal complaint. The right to file a criminal complaint belongs solely to the data subject whose rights (such as the right to information, the right of access, the right to secure transfer of one's personal data to third parties) have been violated. 10

It is up to the competent criminal authority to initiate a criminal investigation if it has concrete indications that a criminal offence may have been committed (Art. 7 para. 1 Criminal Procedure Code). Within the framework of Art. 8 CCP, the public prosecutor's office may refrain from prosecution and, in particular, discontinue criminal proceedings that have already been opened, for example, if the case is a minor one or the offender has made good the damage caused and there are no interests that conflict with discontinuing the criminal proceedings. 11

B. Constitution as a private prosecutor

The FDPIC is also entitled to participate in the cantonal criminal proceedings as a private plaintiff (and thus as a party, Art. 104 para. 1 lit. b CCP) within the meaning of Art. 118 CCP. If it deems it necessary in the interest of a uniform application of the FADP, the FDPIC may, for instance 12

- challenge discontinuation orders (Art. 322 para. 2 CCP) and appeal against cantonal judgments (Art. 382 para. 1 CCP);
- request inspection of files (Art. 101 para. 1 Criminal Procedure Code);
- participate in procedural acts (Art. 107 para. 1 lit. b CCP) and in the taking of evidence (Art. 147 ff. CCP); and
- submit requests for evidence (Art. 107 para. 1 lit. e CCP).

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 66 FADP

A commentary by Jonas D. Gassmann

SUGGESTED CITATION

Jonas D. Gassmann, Kommentierung zu Art. 66 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Gassmann, N. XXX zu Art. 66 DSG.

Art. 66 Statute of limitations for prosecution

Prosecution is subject to a statute of limitations of five years.

CONTENT

IN A NUTSHELL

Criminal violations of the Data Protection Act are misdemeanors. In deviation from the general provision of Art. 109 SCC, the statute of limitations for criminal prosecution does not expire after three years, but only after five years. This is because investigations into possible violations of data protection law are regularly technically complex, require corresponding specialized knowledge, and the criminal proceedings should not fail because the statute of limitations is too short. A distinction must be made between the statute of limitations for prosecution and the statute of limitations for enforcement, which is three years.

I. GENERAL

Art. 66 establishes a special limitation period for prosecution for violations of the Data Protection Act. The provision applies to violations of the Data Protection Act punishable under Chapter 8 (Arts. 60-63). Compared to "ordinary" violations, this is two years longer. This is intended to take into account the technical nature of these violations and the regularly limited experience of the competent cantonal law enforcement authorities in data protection law. 1

Art. 66 is new. Under the previous law, criminal prosecution by virtue of Art. 333 para. 1 SCC became time-barred after three years in accordance with the relevant provision of general criminal law (Art. 109 SCC). In the consultation process, individual participants opposed an extension of the statute of limitations. The wording according to the preliminary draft remained unchanged after the parliamentary deliberations. 2

II. STATUTE OF LIMITATIONS FOR PROSECUTION

A. Duration

The violations of the Data Protection Act, which are punishable under Chapter 8, provide for fines as a penalty and therefore qualify as misdemeanors under Art. 333 para. 3 SCC. 3

Pursuant to Art. 109 SCC, the statute of limitations for criminal prosecution in the case of transgressions is three years. Investigations into possible violations 4

of the Data Protection Act regularly require knowledge of the underlying technical processes, and such investigations will not infrequently be complex. The cantonal law enforcement authorities responsible for enforcing the criminal provisions under Art. 65 para. 1 (unlike, for example, the data protection supervisory authorities responsible for imposing fines under the DSGVO) regularly have little or no experience with data protection law issues (see also above, n. 1). To ensure that corresponding criminal proceedings do not fail due to excessively short statutes of limitations, the statute of limitations for criminal prosecution was increased by two years to five years compared to the general provision of Art. 109 SCC.

B. Commencement

5 Pursuant to Art. 104 SCC, the commencement of the limitation period for prosecution is governed by Art. 98 SCC: If the offense is an active offense, the statute of limitations begins to run on the day on which the offense was committed or on the last day on which the offense was committed. If the offense is a continuing offense, the statute of limitations begins to run on the day on which the criminal conduct ends. In the case of criminal offences designed as omissions, the statute of limitations does not begin as long as the omission continues; the decisive date is the date on which the obligation to act ends. If more than one person is involved in an offense, the statute of limitations begins to run uniformly for all participants with the last partial act.

C. Repeated Offences

6 Repeated offenses that are directed against the same legal entity must be distinguished from continuing offenses. These become time-barred individually after the expiry of the five-year limitation period. For example, if a perpetrator repeatedly entrusts data processing to a processor within the meaning of Art. 61 lit. b FADP without fulfilling the requirements of Art. 9 para. 1 and 2 FADP, the individual violations become time-barred independently of each other, one after the other.

III. LIMITATION OF ENFORCEMENT

7 Art. 66 governs only the limitation period for prosecution, not also the limitation period for enforcement. The latter is governed by the general provision of Art. 109 SCC. It is three years from the day on which the fine decision be-

comes enforceable (Art. 333 para. 1 in conjunction with Art. 109 in conjunction with Art. 100 SCC), i.e. from the day on which the decision becomes final. An appeal against the fine decision to the Federal Supreme Court does not have a suspensive effect (cf. Art. 103 BGG), so that the fine decision becomes legally binding as soon as it is handed down by the last cantonal instance.

BIBLIOGRAPHY

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.

MATERIALS

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.

COMMENTARY ON

Art. 67 FADP

A commentary by Nula Katharina Frei

SUGGESTED CITATION

Nula Frei, Kommentierung zu Art. 67 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Frei, N. XXX zu Art. 67 DSG.

Chapter 9 Conclusion of International Treaties

Art. 67

The Federal Council may conclude international treaties relating to:

a. international cooperation between data protection authorities;

b. the mutual acknowledgement of an adequate level of protection for the disclosure of personal data abroad.

CONTENT

IN A NUTSHELL

In view of increasingly international data flows, effective data protection must also regulate cross-border issues. This may require agreements with other states or international organizations. To facilitate the conclusion of such agreements, Art. 67 FADP grants the Federal Council authority to conclude international treaties without parliamentary approval for two specific subject areas, namely for the purpose of cooperation between data protection authorities and the mutual recognition of an adequate level of data protection. The delegation norm is to be interpreted narrowly.

I. GENERAL

A. Purpose of Art. 67 FADP

In the age of ubiquitous electronic networking, the cross-border processing of personal data has become part of everyday life. For a long time, therefore, data protection has also had an international dimension and, to that extent, has also become an object of foreign policy. 1

Switzerland has concluded numerous bilateral and multilateral agreements in the area of data protection. A distinction can be made between general agreements, which standardize or constitutionalize data protection across all areas of law, and subject-specific agreements, which establish regulations for individual areas of cooperation. The first category currently includes only the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), the modernized version of which (ETS 108+) Switzerland will soon ratify. Subject-specific data protection regulations can be found in numerous agreements in the areas of police cooperation and mutual legal assistance in criminal matters, visa issuance, migration management and readmission of foreign nationals, cooperation in asylum matters, and the exchange of air passenger data. 2

An important player in data protection is the European Union. Its data protection law has a significant influence on Swiss law. Apart from indirect influences and the extraterritorial effect of the General Data Protection Regulation (GDPR), which will not be discussed in depth here, there are also several agreements between Switzerland and the EU with data protection content. Of 3

greatest practical relevance is the Schengen Association, under which Switzerland adopts certain legal acts of the EU, in this case namely Directive 2016/680 on data protection in the areas of police and justice, which must be implemented by the federal government and the cantons.

4 Compared to the general regulation on the conclusion of international treaties in Switzerland (below n. 10 ff.), Art. 67 DPA facilitates the conclusion of international treaties by conferring on the Federal Council the competence to conclude treaties independently without the approval of the Federal Assembly in two specific subject areas, namely for the purpose of cooperation between data protection authorities as well as the mutual recognition of an adequate level of data protection.

B. History of origins

5 Art. 67 DPA replaces Art. 36 para. 5 aDSG, which was considered too vague under the existing principles of delegation of authority, namely the prohibition of blank delegations. Art. 36 para. 5 aDSG provided that the Federal Council may conclude international treaties on data protection if they comply with the principles of the FADP.

6 The remaining paragraphs of Art. 36 aDSG, which authorized the Federal Council to issue implementing provisions both of a general nature and relating to specific subject areas, are not continued in the new FADP.

7 In the legislative process, Art. 67 DPA was uncontroversial. The suggestion that the Federal Council's authority to conclude treaties should be limited to the effect that it may not conclude any treaties under international law on the enforcement in Switzerland of sanctions imposed by foreign supervisory authorities, which was put forward in some cases during the consultation process, was not heard either in the dispatch or in the parliamentary deliberations. Compared to the preliminary draft and the draft of the Federal Council, Art. 67 (with the exception of the numbering) did not undergo any changes in the parliamentary deliberations and, according to the Council minutes, was not discussed.

II. COMPETENCE OF THE FEDERAL COUNCIL TO CONCLUDE INTERNATIONAL TREATIES

An international treaty is an agreement concluded in writing between two or more subjects of international law within the meaning of Article 38(1)(a) of the ICJ Statute and Article 2(1)(a) of the Vienna Convention on the Law of Treaties. 8

While Art. 67 DPA uses the term "international treaty", à Art. 16 para. 2 lit. a DPA speaks of "international treaty". Despite the different terminology, the same is meant. 9

In principle, the Federal Council and the Federal Assembly are jointly responsible for concluding international treaties in Switzerland. While the Federal Council, within the scope of its foreign policy competences, negotiates and signs international treaties (Art. 184 para. 1 and 2 BV), the Parliament approves the treaties by means of a federal decree (Art. 166 para. 2 sentence 1 BV) before the Federal Council can ratify them (Art. 184 para. 2 BV). This is explained by the fact that international treaties, just like federal laws, contain law-making provisions and thus require at least subsequent democratic legitimation. In certain cases, the optional or obligatory referendum on international treaties is provided for in addition to parliamentary approval. If an international treaty is subject to a referendum, if it concerns essential interests of the cantons, or if it is of great political, financial, economic, ecological, social or cultural significance, a consultation must be carried out in advance. 10

Parliament may, however, dispense with this competence by means of delegation. Accordingly, the approval requirement does not apply to treaties whose conclusion has been delegated to the Federal Council by Parliament by means of a federal law or an international treaty approved by it. The idea behind this is to relieve the Federal Assembly from approving treaties that are "not worthy of parliamentary approval" and to concern it only with issues that require greater democratic legitimacy. 11

This independent treaty-making competence is elaborated in more detail in Art. 7a RVOG, which lists three constellations in which the Federal Council may ratify a treaty without prior parliamentary approval. 12

- First, on the basis of an authorization in a specific federal law (Art. 7a para. 1 RVOG). Art. 67 DPA is such an authorization. Here, parallel principles as

in the area of legislative delegations to the Federal Council are authoritative: the essential legal policy evaluations must be made with sufficient definiteness in the parliamentary law. So-called "blank delegations" are not compatible with the principle of legality, because they could have the effect of removing an unforeseeable number of international treaties of varying content from the requirement for approval.

- Second, an authorization in an international treaty approved by the Federal Assembly (Art. 7a para. 1 RVOG). Essentially parallel principles of delegation apply to this as to delegations of competence in a federal act.
- Thirdly, the Federal Council may ratify so-called treaties of limited scope without prior parliamentary approval (Art. 7a para. 2 RVOG). This is a subsidiary general clause because it applies to all treaties of limited scope, regardless of the area in question. According to Art. 7a para. 3 RVOG, contracts of limited scope include contracts that do not create new obligations or do not entail a waiver of existing rights (Art. 7a para. 3 lit. a RVOG), contracts that merely serve to execute contracts that have been approved by the Federal Assembly and merely flesh out the rights, obligations or organizational principles already stipulated in the basic contract (lit. b), and contracts that are addressed to the authorities and regulate administrative-technical issues (lit. c). This list is exemplary: whether a contract actually has a limited scope is to be determined by interpretation. The law also specifies which contracts are in principle not considered to be of limited scope (Art. 7a para. 4 RVOG). This is the case, in particular, if the treaty is subject to the optional referendum on the state treaty pursuant to Art. 141 para. 1 lit. d of the Federal Constitution (lit. a), contains provisions which fall within cantonal competences (lit. b), or involves high expenditure (lit. c). Further criteria are whether a treaty interferes with the legally protected interests of private individuals, requires a change in the law, or whether it fits "smoothly" into the general domestic and foreign policy environment as well as the economic environment.

13 In purely quantitative terms, the vast majority (over 90%) of treaties entered into by Switzerland are concluded independently by the Federal Council. The Federal Council submits an annual report to the Federal Assembly on the treaties it has concluded independently (Art. 48a para. 2 RVOG). In this form, there is subsequent parliamentary control.

The Federal Council may also delegate the competence to conclude international treaties to a department. If the treaty is of limited scope within the meaning of Art. 7a para. 2 RVOG, it may further delegate this competence to a group or to a federal office (Art. 48a para. 1 RVOG). 14

The predecessor provision, Art. 36 para. 5 aDSG, stipulated that the Federal Council may independently conclude international treaties "provided that they comply with the principles of the law." This was interpreted in the doctrine in such a way that the international treaties had to comply with the general data protection principles, namely the principles of legality, good faith, recognizability, proportionality, purpose limitation, data accuracy, data security, protection of the rights of the data subjects, as well as the prohibition of data disclosure abroad in the event of a risk of serious personality violations. Although this requirement has not been incorporated into the new provision, it still arises for Art. 67 DPA from the nature of the delegation and ultimately from the principle of separation of powers: in the absence of an explicit provision, the Federal Council is not authorized to conclude agreements that contradict the general provisions of the law without the approval of Parliament. Since the data protection principles derive directly from the Constitution (Arts. 5, 13, 36 BV) and the international law requirements of the data protection convention (Art. 5 ETS 108+), even parliamentary approval would not change the fact that international treaties contradicting the data protection principles may not be concluded in principle. 15

A. International Cooperation between Data Protection Authorities (lit. a)

According to Art. 67 lit. a FADP, the Federal Council may conclude international treaties regulating international cooperation between data protection authorities. Questions of delimitation arise with regard to the term "cooperation" (a) as well as the circle of authorities involved (b). 16

1. Cooperation

The increasingly cross-border nature of data processing makes international cooperation between data protection authorities essential. Cooperation is therefore one of the cornerstones of the modernized Council of Europe Convention ETS 108+, which in Chapter V obliges the contracting states to cooperate and provide mutual assistance (cf. Art. 16 para. 1 ETS 108+). Similarly, in 17

its modernized data protection law, the European Union places great emphasis on institutionalized cooperation between national data protection authorities (cf. Art. 60 et seq. GDPR as well as the - for Switzerland in the area of police and law enforcement binding - Art. 50 et seq. DIRECTIVE 2016/680).

18 Cooperation between data protection authorities can take various forms. Art. 17 of the ETS 108+ Convention lists the following forms of cooperation as examples: Providing mutual assistance, namely in the form of exchange of information, coordinating investigations or operations or carrying out joint measures, and providing each other with information and documentation on national law and administrative practice.

19 The ETS 108+ Convention obliges the Parties to form a network of supervisory authorities to organize their cooperation (Art. 17 para. 3). Further details of the cooperation, in particular with regard to the forms and procedures as well as the languages to be used, are to be determined directly between the Contracting Parties concerned (Art. 21 para. 3). The conclusion of international treaties is necessary for the regulation of these issues. Art. 67 lit. a FADP enables the Federal Council to conclude such treaties in a simplified manner and thus also implements this obligation under Convention ETS 108+.

20 In terms of domestic law, it is one of the statutory duties of the FDPIC to cooperate with foreign authorities responsible for data protection (à Art. 58 para. 1 lit. b FADP). In practice, the FDPIC cooperates in particular with individual national and supranational data protection authorities, especially the data protection authorities of the Schengen member states and the European Data Protection Committee (EDSA). It is also involved in international bodies such as the Council of Europe, the European and International Conferences of Data Protection Commissioners, the French-speaking Association of Data Protection Authorities, and the OECD.

21 The FDPIC also has the authority to provide administrative assistance to foreign data protection authorities, provided that the requirements of à Art. 55 FADP are met. For this purpose, too, an international treaty may be necessary, which the Federal Council can facilitate pursuant to Art. 67 lit. a.

22 In relation to the aforementioned statutory competences of the FDPIC, Art. 67 lit. a FADP provides the legal basis in cases where international cooperation goes beyond purely informal cooperation (e.g., the exchange of best practices) and must therefore be placed on a formal footing. The conclusion of an

international treaty is particularly necessary if mutual rights and obligations are to be established on a permanent basis and if personal data or otherwise protected data (such as trade secrets) are to be exchanged with other states. For the transfer of personal data, the requirements of à Art. 16 FADP must also be observed.

So far, no such cooperation agreements have been concluded in the area of data protection. As a model for a cooperation agreement, the dispatch also mentions an agreement from another legal area, namely the agreement of 17 May 2013 between the Swiss Confederation and the European Union on cooperation in the application of their competition law. The contents of this agreement provide a preview of possible contents of future cooperation agreements in the area of data protection: for example, in it, the parties undertake that their competition authorities may inform each other of enforcement measures that they consider may affect important interests of the other party (Art. 3), that they may coordinate enforcement measures with respect to related transactions (Art. 4), or that they may request each other to initiate enforcement measures (Art. 6). 23

Also within the scope of Art. 67 lit. a FADP are agreements that delimit the responsibilities of the various data protection authorities. Such an agreement would have practical relevance with respect to the delimitation of responsibilities between Swiss and European data protection authorities, since the GDPR also applies to controllers or processors not established in the EU, which means that the responsibilities of the supervisory authorities of the EU member states extend to controllers in Switzerland, but they cannot take any enforcement action in Switzerland. A parliamentary motion calling for the conclusion of a corresponding coordination agreement with the EU was already adopted by the Councils in 2017, but has not yet been implemented, which is probably mainly due to the fact that no new agreements can currently be concluded with the EU before the institutional issues have been clarified. In any case, the Federal Council could conclude a corresponding coordination agreement based on Art. 67 DPA without the approval of Parliament. 24

2. Data protection authorities

The authorization of the facilitated conclusion of cooperation agreements under international law pursuant to Art. 67 DPA relates exclusively to cooperation between "data protection authorities." Both the ETS 108 Convention (Art. 25

1 Additional Protocol of 2001 or Art. 12bis ETS 108+) and the EU Directive 2016/180 (Art. 41 RL 2016/680), which is binding on Switzerland, oblige the contracting states to establish one or more independent data protection supervisory authorities.

26 Inversely, this means that the enabling basis of Art. 67 lit. a DPA does not extend to contracts on data protection-related cooperation between other authorities, such as the exchange of personal data between judicial, police or migration authorities. Such contracts require parliamentary approval unless authorized in another federal law.

27 The competence to conclude the cooperation agreement is reserved to the Federal Council. According to the wording of the law, even if the FDPIC is the party directly affected by such contracts, it has no competence to conclude them independently. Although the Federal Council would have the possibility to subdelegate its competence to conclude international treaties independently to the FDPIC (cf. Art. 48a para. 1 RVOG and above, n. 14), it has not done so to date. In this respect, the FDPIC is dependent for its activities on the Federal Council concluding corresponding contracts, which is in a certain tension with its institutional independence (à Art. 43 para. 4 FADP).

B. Mutual recognition of an adequate level of protection (lit. b)

28 The second purpose for which the Federal Council may conclude state treaties without prior approval of Parliament is the mutual recognition of an adequate level of protection pursuant to Art. 67 lit. b FADP.

29 This provision is to be understood in connection with à Art. 16 FADP, which regulates the conditions for the disclosure of personal data abroad. One of these possibilities is the existence of an international treaty: according to Art. 16 para. 2 lit. a, disclosure abroad is possible if an international treaty ensures appropriate data protection.

30 The modernized data protection convention of the Council of Europe also recognizes the possibility of ensuring the existence of an adequate level of protection in a third country by means of an international agreement (cf. Art. 12 para. 3 lit. b ETS 108+). Similarly, EU law provides for corresponding regulations (cf. Art. 46 para. 2 lit. a GDPR and Art. 37 para. 2 lit. a of Directive 2016/680, which is binding on Switzerland).

An international treaty within the meaning of Art. 16(2)(a) DPA may be a general data protection convention such as the ETS 108+ Convention, or any other sectoral agreement in a specific area that regulates the transfer of personal data between the contracting parties. It should be noted that an international treaty is only covered by the authorization in Art. 67 lit. b DPA if it is limited to the purpose of mutual recognition of an adequate level of protection; if it goes beyond that, the Federal Council may not conclude the treaty independently or needs a different basis for authorization. 31

The possibility of recognizing an adequate level of protection by means of an international treaty is relevant if the legislation of the state or international body concerned does not provide adequate protection within the meaning of Art. 16(1) FADP and there is therefore no corresponding declaratory decision by the Federal Council. By means of an agreement, the states involved can agree on an international treaty data protection system that compensates for the deficiencies in the national legal system so that mutual recognition of an adequate level of protection becomes possible. 32

The most important example of application is the agreements with the United States, whose level of data protection is not considered adequate within the meaning of Art. 16(1) FADP, among other things because of the far-reaching access rights of both the U.S. President and the domestic intelligence service to data held by U.S. companies and the limited legal protection available to non-U.S. nationals. At the same time, however, the agreements with the United States illustrate the limits of international treaty agreements on data protection standards, namely the difficulty in realpolitik of modifying the distribution of domestic competences by means of international law: The U.S.-Swiss Safe Harbor Framework (which was modeled on the EU-US Safe Harbor, which had to be replaced due to the ECJ ruling in the Schrems case), which was still cited as an example in the explanatory report on the preliminary draft of the DPA (but no longer in the dispatch), was no longer recognized by the FDPIC as a basis for data transfers to the United States following the Schrems ruling. After the subsequent EU-US Privacy Shield was also deemed insufficient by the ECJ in the Schrems II case, the Swiss-US Privacy Shield remains formally in force, but is also deemed insufficient by the FDPIC. The EU and the USA announced in March 2022 that they had agreed on a Trans-Atlantic Data Privacy Framework; however, Switzerland would first have to agree on a parallel agreement with the USA. It remains to be seen 33

whether the Trans-Atlantic Data Privacy Framework will really overcome the aforementioned realpolitik difficulties.

34 Mutual recognition of an adequate level of data protection is also possible in sectoral agreements. For example, in the context of double taxation agreements with countries that do not have adequate data protection, the contracting parties can state that data protection in connection with the granting of administrative assistance in tax matters is considered adequate, at least with regard to tax-relevant data, on the basis of the state treaty assurances given. The same applies to the transfer of personal data in the context of cooperation between police, customs, law enforcement or migration authorities, where Switzerland has concluded numerous agreements. As already mentioned, the enabling basis of Art. 67 lit. b FADP is limited to the question of mutual recognition of an equivalent level of protection. Consequently, cooperation agreements, which in practice usually regulate further, more far-reaching issues, require prior approval by Parliament - unless another federal law provides an enabling basis.

C. State treaties for other purposes

35 The basis for authorization in Art. 67 FADP is limited to the two purposes of lit. a and b. The delegation norm must be interpreted narrowly. The delegation norm must be interpreted narrowly.

36 For other purposes in the area of data protection, the Federal Council may also conclude treaties under international law, but the competence is then not based on this article but on the general provisions (see above n. 10 ff.). This means that if the treaty is of limited scope, or if there is an enabling provision in a federal law other than the DPA, the Federal Council may also ratify it without parliamentary approval. In all other cases, parliamentary approval is required prior to ratification.

37 In my opinion, treaties that involve the transfer of personal data to foreign authorities are not of limited scope, since they interfere with the legally protected interests of private individuals. These include the numerous cooperation agreements in the areas of police, justice, mutual legal assistance, migration and taxation that Switzerland has concluded with other states and which contain provisions on the exchange of data. State treaties or exchanges of notes for the implementation of the further development of the Schengen acquis

(insofar as they regulate more than mere technical details) as well as agreements with other states on access to passenger name records (PNR) also fall under this category. Since Art. 67 does not provide any authorization for such agreements, a delegation in a sectoral federal law or parliamentary approval is always required. Correctly, the Federal Council also obtained the prior approval of the Federal Assembly before ratifying the ETS 108+ Convention as well as the adoption of Directive 2016/680. Both legal acts are instruments of great scope within the meaning of the exemplary list in Art. 7a para. 4 RVOG.

38 It should be noted that the basis for authorization in Art. 67 FADP empowers the Federal Council to conclude agreements of limited as well as broader scope within the framework of the stated purposes. In my opinion, the legal opinion expressed in the doctrine on the old delegation norm in Art. 36 Para. 5 aDSG, according to which this only covers contracts of limited scope, fails to take into account the relationship between the various bases of authorization in Art. 7a RVOG. A sectoral delegation in a federal law constitutes a lex specialis and enables a fortiori both the conclusion of treaties of limited scope and those of broader scope.

39 The Federal Council decides whether a treaty of limited scope exists or whether it falls under the delegation of Art. 67 lit. a and b. The Federal Council has the power to decide on the scope of the treaty. In order to check that it does not exceed its powers, Art. 48a para. 2 RVOG requires the Federal Council to report annually to the Federal Assembly on the contracts concluded, amended and terminated by it, by the departments, by the groupings or by the offices. If the Federal Assembly does not agree with the division made by the Federal Council, it may request by way of motion that the Federal Council submit the contract for subsequent approval.

BIBLIOGRAPHY

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.

MATERIALS

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+).

COMMENTARY ON

Art. 69 FADP

A commentary by Rehana C. Harasgama / Dario Haux

SUGGESTED CITATION

Rehana C. Harasgama/Dario Haux, Kommentierung zu Art. 69 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Harasgama/Haux, N. XXX zu Art. 69 DSG.

Art. 69 Transitional provisions relating to ongoing instances of processing

Articles 7, 22 and 23 do not apply to data processing that began before this Act comes into force, provided the purpose of processing remains unchanged and no new data are collected.

CONTENT

IN A NUTSHELL

The totally revised FADP will enter into force on September 1, 2023 without a general transition period. However, Art. 69 states that some selected articles are not applicable to certain data processing operations. The standard stipulates that this only applies, however, if these data processing operations began before the entry into force of the totally revised FADP and neither the purpose of the processing was changed nor new data was obtained after its entry into force. In this sense, the article excludes the preventive measures of Art. 7, 22 and 23 in certain cases. In this way, the legislator wanted to avoid the possibility that data controllers could be held liable after the fact, thereby incurring additional effort and costs.

I. GENERAL

A. Overview

The totally revised FADP does not contain any transition periods that would have to be taken into account by data controllers or other data subjects. In this respect, it applies in principle as of September 1, 2023. However, in the 10th chapter, the final provisions, there are some relevant transitional provisions. These are specifically contained in Art. 69 to 72. The present Art. 69 specifically provides that Art. 7, 22 and 23 are not applicable to data processing in certain cases. This applies to those processing operations that were started before the revised FADP entered into force on September 1, 2023, and whose processing purpose was neither changed nor new data added to the data processing process after the entry into force. 1

B. History of origins

When the totally revised FADP enters into force on September 1, 2023, the standards will apply throughout Switzerland and will thus be applicable, provided that Articles 2 and 3 para. 1 are fulfilled. However, as is common in other laws, there are exceptions to this principle or at least transitional provisions which are intended to simplify the transition between the old and new catalog of standards. The latter was provided for in an Art. 64 FADP. This provided for three exceptions, namely a retroactive effect of the data subjects' right to in- 2

formation in the case of already completed data processing (para. 1), a transitional period for the adaptation of continuing data processing (para. 2) and the non-applicability of certain provisions in the case of unchanged continuing data processing (para. 3). In paragraph 4, the principle of application of the provisions upon entry into force was established. Finally, however, all paragraphs were deleted - except for the aforementioned paragraph 3, which is now found in the present Art. 69.

C. Purpose of the Norm

3 Art. 69 ensures that a retroactive application of Art. 7, 22 and 23 is prevented if specific conditions are met. In this way, the legislator facilitates the transition between the existing and the totally revised FADP and saves the responsible parties additional effort and costs. In addition, the article ensures that no obligations are subsequently imposed on data controllers. A retroactive effect of the law, which may be problematic in individual cases, is thus avoided. At the same time, the significance of this article is limited, especially since the FADP generally does not provide for any relevant transition periods.

II. CONTENT

A. Requirements

4 In terms of content, Art. 69 refers to Art. 7, 22 and 23. While Art. 7 enshrines the principles of privacy by design (data protection by design) and privacy by default (data protection by default) (see in detail the OC Clause on Art. 7 FADP), Art. 22 and 23 refer to the data protection impact assessment (DSFA) (see OC Harasgama/Haux on Art. 22 FADP). Art. 22 sets out the basis for conducting the DIA and 23 sets out some requirements for consulting the FDPIC if a DIA reveals that there is a high risk to the personality or fundamental rights of the data subject despite risk mitigating measures taken.

5 These obligations must in principle be taken into account prior to the respective processing of the data and are not to be imposed retroactively on the data controller by means of this transitional provision. In terms of this prohibition of retroactivity, the norm requires that the data processing has begun before the effective date. It must therefore have started before September 1, 2023 and must neither have been planned (as defined in Art. 7 para. 1 FADP) nor already completed. While the distinction between the mere planning and the

actual implementation of data processing can be determined in individual cases, the question arises as to how implementation is to be distinguished from the termination of data processing. It must be taken into account here that termination can only be assumed when the purpose of the processing has been achieved. The situation in which the purpose is de facto no longer achievable is equated.

As a second prerequisite, the previously defined processing purpose must continue unchanged. This means that the purpose was sufficiently determined and specified at the beginning of the data processing and continues to exist unchanged at the time of the entry into force of the totally revised FADP (cf. in detail the commentary on Art. 6 para. 3 FADP on the determination of the processing purpose). In this context, the question arises as to what applies if only some processing purposes are continued, but others are abandoned. This would be the case if, for example, a database with patient data from clinical trials is initially processed for further clinical trials in the same field of research (purpose 1) and for the training of a prognosis tool based on artificial intelligence (AI) (purpose 2), and after the entry into force of the totally revised FADP, data processing only takes place for clinical trials, i.e. for purpose 1. The assumption that this is covered by the wording of Art. 69 is supported by the fact that in any case there is no expansion of the processing purposes. Rather, the existing ones are pursued further - albeit in a reduced form. 6

Thirdly, the data stock of the data processing in question must continue to exist unchanged. According to the wording of the law, therefore, "no new data may have been obtained". The process of "obtaining" is "an active, targeted and deliberate act of collecting the personal data in question". The decisive factor is the targeted, active act. Passively obtaining data, on the other hand, is not included. Other authors come to a similar conclusion by focusing on the planned nature of the act. 7

However, it is unclear how the phrase "no new data" should be interpreted. A narrow interpretation would lead to the fact that for a constant data processing process with fixed data categories, the transitional provision would not apply insofar as additional data (points) about additional persons are obtained with constant data categories. This would be the case regardless of how these additional data (points) affect the processing process or purpose. This assessment could be justified by the fact that the data set or the scope of the existing data would be changed or increased. As an example, consider an AI-based HR 8

tool at a company that processes additional data (points) from new applicants or employees after September 1, 2023. The data stock or the scope of this stock would thus be changed or increased, so that if the other requirements of Art. 69 are met, a data protection impact assessment would have to be carried out again according to this narrow interpretation. While the message certainly suggests such an interpretation, such a narrow interpretation does not correspond to the sense and purpose of the provision. In fact, this would mean that all continuing data processing operations in which it is possible that data on additional individuals will be obtained after September 1, 2023, would not be covered by the provision. The scope of application of Art. 69 would thus be negligibly narrow. This narrow interpretation is not followed in the present case. Against this background, two possible interpretations are possible: (1) Art. 69 only applies if new data categories are procured, but not in the case of a mere change or expansion of the scope of the same data categories or data points. This would be the case, for example, if an online form provided for a sweepstakes after September 1, 2023, no longer collects only name, contact information and answer to the sweepstakes question, but asks for more extensive information about interests and hobbies. Or: (2) Art. 69 is not applicable to any data processing operations if - according to the Message, narrowly interpreted - the data stock or the data volume per se is increased or changed, even though the categories of data procured remain unchanged and a resulting change in the processing purpose or the process cannot be ruled out.

9 There is also discussion as to whether data that has already been procured in advance, but is subsequently added, precludes the applicability of Art. 69 FADP. Based on the wording, some authors argue that the processing of these data falls under the exception, at least if they were obtained for the same purpose. However, this is contradicted by the fact that the environment of data processing is so deeply affected by technological innovations that the exception of Art. 69 FADP should only apply under narrow conditions and should therefore be interpreted restrictively. If new data is added to the data stock, the data stock can hardly be described as "unchanged", i.e. as remaining the same, if this data has already been obtained in the context of another data processing purpose. Whether this question will gain in importance and contour in practical application, however, seems questionable, especially since overall the practical relevance of this standard can be assumed to be rather low. This is especially true since the principle of Art. 7 was already partially established before the entry into force of Art. 4 and 7 of the aDSG, and data

controllers were also partially obligated to do so due to the DSGVO. The same applies to Art. 22 and 23 (see in detail the commentary by Harasgama/Haux on Art. 22 FADP).

B. Challenges

With the entry into force of the totally revised FADP, data controllers face numerous challenges. Although the wording of Article 69 of the FADP is brief and may be lost sight of, it should be given the necessary attention in this context. While data processing that was in progress before the entry into force and meets the other requirements is unquestionably covered by the exemption, legal advice must always be sought on detailed questions and on the application of new technologies in data processing processes that were already planned and/or tested before the entry into force of the totally revised FADP. In this case, it is important to determine precisely whether the data stock or processing purpose has actually remained unchanged or whether changes have been made or must be made. If this is the case, it must be assumed in case of doubt that the standard is not applicable. 10

BIBLIOGRAPHY

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).

MATERIALS

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.

COMMENTARY ON

Art. 72 FADP

A commentary by Danielle Schneider / Carl Jauslin

SUGGESTED CITATION

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 72 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Schneider/Jauslin, N. XXX zu Art. 72 DSG.

Art. 72 Transitional provision relating to the Commissioner`s election and termination of office

[1] The election of the Commissioner and the termination of his or her term of office shall be governed by the previous law until the end of the legislature period in which this Act comes into force.

[2] If the incumbent is elected in the first vote of the United Federal Assembly to elect the Commissioner, the Commissioner`s new term of office begins on the day after the election.

CONTENT

IN A NUTSHELL

The new data protection law will come into force on September 1, 2023. However, the previous law will continue to apply to the election and termination of the term of office of the Commissioner until the end of the 51st legislative term. According to this, the United Federal Assembly is the electoral body and responsible for the most important employer decisions.

I. GENERAL

The total revision of the FADP amends the procedure for appointing the Commissioner. The United Federal Assembly is now the sole electoral body and responsible for the most important employer decisions. In this way, the independence and democratic legitimacy of the Commissioner are to be strengthened. Transitional provisions are therefore necessary for the election and termination of the term of office of the Commissioner. 1

Art. 72 para. 1 FADP was introduced as part of the parliamentary deliberations on the total revision of the FADP. The provision was not yet included in the Federal Council's draft, as the Federal Council had retained the previous procedure for appointing the Commissioner (election by the Federal Council and approval by the Federal Assembly in accordance with Art. 26 para. 1 aFADP) as well as the previous responsibilities for employer decisions (in particular Art. 26a para. 3 concerning removal from office by the Federal Council). 2

Art. 72 para. 2 FADP was only included in the totally revised FADP in the course of the work on the parliamentary initiative SPK-N 21.443. This was necessary to close an unintentional loophole regarding the possible re-election of the previous commissioner (cf. n. 6 f.). 3

II. TRANSITIONAL RIGHT REGARDING ELECTION AND TERMINATION OF THE TERM OF OFFICE (PARA. 1)

Art. 72 para. 1 FADP provides that the election of the Commissioner and the termination of his or her term of office shall continue to be governed by the previous law until the end of the legislative period in which the totally revised FADP enters into force. 4

5 The Federal Council has set the new data protection law to come into force on September 1, 2023. This means that the Commissioner can be elected by the United Federal Assembly for the first time as of the 2023 winter session. The Judicial Commission has announced that it plans to elect the Commissioner for the next term of office in the winter session of 2023. In this case, the new term of office of the Commissioner would in principle begin on 1 January 2024 (cf. Art. 44 para. 1, second sentence FADP).

III. TRANSITIONAL RIGHT REGARDING THE POSSIBLE RE-ELECTION OF THE CURRENT APPOINTEE (PARA. 2)

6 The current Commissioner was confirmed by the Federal Council on 10 April 2019 for a second term of office until the end of the 51st legislative term on 4 December 2023. He is running for a third (and final) term. The election is to be held by the United Federal Assembly (Art. 43 para. 1 FADP). In the event of a re-election, a start of office on 1 January 2024 would lead to an unintended gap (in particular from a personnel law perspective). This is because between December 4, 2023 and January 1, 2024, the current office holder would not have an employment relationship as an appointee. Consequently, he would in principle also have no rights or obligations arising from the employment relationship (namely no salary entitlement).

7 For the first election by the United Federal Assembly, Art. 72 para. 2 FADP therefore exceptionally advances the start of the term of office to the day after the election. However, this only applies in the case of a re-election of the current incumbent. Admittedly, even this solution does not achieve a seamless transition. However, the current appointee could at least resume his employment as soon as possible. During the transition period, the FDPIC would be headed by the deputy of the appointee.

The opinion expressed reflects the personal opinion of the authorship and does not bind the Federal Office of Justice.

MATERIALS

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).

COMMENTARY ON

Art. 72a FADP

A commentary by Danielle Schneider / Carl Jauslin

SUGGESTED CITATION

Danielle Schneider/Carl Jauslin, Kommentierung zu Art. 72a DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz

Short citation: OK-Schneider/Jauslin, N. XXX zu Art. 72a DSG.

Art. 72a Transitional provision relating to the Commissioner's employment contract

If the Commissioner's employment contract was based on the previous law, the previous law continues to apply.

CONTENT

IN A NUTSHELL

With the total revision of the FADP, the Federal Assembly becomes the electoral body and employer of the Commissioner. This has implications for the employment relationship. The new provisions on the employment relationship of the Commissioner will only apply after the first election by the United Federal Assembly. After the new data protection law comes into force on September 1, 2023, the previous law shall therefore continue to apply to the employment relationship until the Commissioner is elected by the United Federal Assembly.

I. GENERAL

With the total revision of the FADP, the Federal Assembly becomes the electing body and employer of the Commissioner. It is therefore responsible for regulating the Commissioner's employment relationship (cf. Art. 43 para. 3bis FADP). As part of the parliamentary initiative SPK-N 21.443, it has issued corresponding implementing provisions. In addition, the FADP also contains various provisions on the employment relationship of the appointee, namely regarding the term of office and its termination (Art. 44 FADP), disciplinary law (Art. 44a FADP) or secondary employment (Art. 47 FADP). Art. 72a FADP clarifies from when these new provisions apply to the appointee. 1

II. TRANSITIONAL PROVISION CONCERNING THE EMPLOYMENT RELATIONSHIP OF THE APPOINTEE

The election of the Commissioner and the termination of his or her term of office are still subject to the previous law until the end of the legislative period in which the FADP enters into force (Art. 72 para. 1 FADP). Only when the appointee is elected by the United Federal Assembly can his or her employment relationship be governed by the new law. Art. 72a FADP therefore provides that the employment relationship of the appointee established under the previous law shall be governed by the previous law. 2

This means that after the new data protection law comes into force on 1 September 2023, the previous law will continue to apply to the employment relationship of the Commissioner until the first election by the United Federal As- 3

sembly. Thereafter, the totally revised or newly created provisions on the employment relationship of the Commissioner shall apply.

The opinion expressed reflects the personal opinion of the authorship and does not bind the Federal Office of Justice.

MATERIALS

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).