Contents

Global Privacy and Security Law - Gilbert, Switzerland,SWITZERLAND Sylvain Métille

Global Privacy and Security Law - Gilbert
Global Privacy and Security Law - Gilbert
SWITZERLAND Sylvain Métille

Click to open document in a browser

Sylvain Métille

Global Privacy and Security Law - Gilbert, § SWI.00, Switzerland,COUNTRY OVERVIEW

Francoise Gilbert, Global Privacy and Security Law § SWI.00 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

Capital	*Bern*
Official Language	*German, French, Italian, Romansch*
Political System	*Federal Republic; Confederation of 26 cantons*
Population	*8.6 million*
Currency	*Swiss Franc*

[A] Location

Switzerland, officially the Swiss Confederation, is a landlocked country located in the South-Western part of the European continent. It is bordered by France to the West, Germany to the North, Austria and Liechtenstein to the East, and Italy to the South. The Swiss Confederation consists of 26 cantons. Its largest urban centers include Zurich, Geneva, Basel, Lausanne and Bern, the capital. [1]

[B] Constitution and Government

The Swiss Confederation was founded in the late 13th century as a defensive alliance among three cantons. One of these cantons was named Schwyz. Today the Swiss Confederation consists of 26 cantons. The federal authorities are based in the city of Bern.

Switzerland adopted its first constitution in 1848. The current Constitution entered into effect in January 2000.

[C] Executive Branch

The Federal Council, which is composed of seven federal councilors, constitutes the federal government. The Federal Council serves for four years and is elected by the Federal Assembly.

The President of the Swiss Confederation is elected for a one-year term and is regarded during that time as “Primus inter pares,” or first among equals.

[D] Legislative Branch

The legislative branch, named the Federal Assembly, is bicameral. The Federal Assembly consists of the Council of States, which has 46 members, and the National Council, which has 200 members. Members of both houses are elected every four years.

[E] Judicial Branch

The highest court is the Swiss Federal Supreme Court, which consists of 38 justices and 19 deputy justices, organized in seven divisions. Judges are selected by the Federal Assembly, for six-year terms. They are affiliated with political parties and are elected according to linguistic and regional criteria in approximate proportion to the level of party representation in the Federal Assembly.

Subordinate courts include the Federal Criminal Court, the Federal Administrative Court and the Federal Patent Court. In addition, each of the 26 cantons has its own courts with its own judicial organization.

[F] Legal System

The legal system is based on a written civil law structure.

[G] Membership in International Organizations

Switzerland maintains a tradition of political and military neutrality. It hosts numerous international organizations, such as the United Nations and became a full member of the United Nations in 2002. It is also a founding member of the Organization for Economic Cooperation and Development (OECD) (1960) and it joined the Council of Europe in 1963.

Switzerland is a member of the Euro-Atlantic Partnership Council (EAPC), the Organization for Security and Cooperation in Europe (OSCE), the International Monetary Fund (IMF), the World Bank and the World Trade Organization (WTO). It is an observer to the Organization of American States.

Switzerland is not a member of the European Union (EU) or of the European Economic Area (EEA), but it is a founding member of the European Free Trade Association (EFTA). In this context, and in an effort to lay the grounds for easy commercial integration with its immediate neighbors, Switzerland and the EU are bound by several bilateral agreements. As a member of EFTA, Switzerland is also part of the border-free Schengen Area, which guarantees the free movement to more than 400 million people within the Schengen area.

[H] Economy

Switzerland is widely known internationally as a banking and financial hub. Its banking, insurance, tourism, international trading, logistics, pharmaceuticals, and chemicals industries are very important sectors in Switzerland. Watch making, biological science industries, and the manufacture of precision instruments for engineering are also prominent. Small and medium-sized enterprises also play an important role in the Swiss economy. [2]

Footnotes

1 Maps of Switzerland are available at: https://map.geo.admin.ch. Country maps of Switzerland showing the major cities available from the World Factbook 2021, Washington DC, Central Intelligence Agency at: https://www.cia.gov/the-world-factbook/countries/switzerland/map ; locator map available at: https://www.cia.gov/the-world-factbook/countries/switzerland/map.

2 Sources for this section include: http://www.oecd.org/switzerland/ ; www.state.gov ; www.seco.admin.ch ; www.kmu.admin.ch ; www.bfs.admin.ch ; and www.cia.gov.

Global Privacy and Security Law - Gilbert, § SWI.01, Switzerland,INTERNATIONAL TREATIES AND AGREEMENTS

Francoise Gilbert, Global Privacy and Security Law § SWI.01 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

[A] United Nations

Switzerland is a member of the United Nations, and it adheres to the Universal Declaration of Human Rights. [3] Article 12 of the Universal Declaration of Human Rights provides:

- *No one shall be subjected to arbitrary interference with his/her privacy, family, home, or correspondence, nor to attacks upon his/her honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

Other declarations and conventions issued by the United Nations have significant privacy or data protection components. This includes, for example, the Convention on the Rights of the Child (adopted in 1989, entered into force on September 2, 1990), which provides in its Art. 16:

- *No child shall be subjected to arbitrary or unlawful interference with his or her* privacy *, family, home, or correspondence, nor to unlawful attacks on his or her honor and reputation.*
- *The* child *has the right to the protection of the law against such interference or attacks.*

Further, Article 40 provides in relevant parts:

- *States Parties recognize the right of every child alleged as, accused of, or recognized as having infringed the penal law to be treated in a manner consistent with the promotion of the child's sense of dignity and worth, which reinforces the child's respect for the human rights and fundamental freedoms of others and which takes into account the child's age and the desirability of promoting the child's reintegration and the child's assuming a constructive role in society.*
- *To this end, and having regard to the relevant provisions of international instruments, States Parties shall, in particular, ensure …: (* vii *) To have his or her privacy fully respected at all stages of the proceedings.*

[B] Organization for Economic Cooperation and Development (OECD)

Switzerland is a founding member of the Organization for Economic Cooperation and Development (OECD). The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines), which were originally published in 1980, may have influenced the development of the first federal privacy law of Switzerland which was adopted in 1992. [4] The 1980 OECD Privacy Guidelines were updated in 2013. [5]

In the past 25 years, the OECD has published additional recommendations and guidelines, that may be relevant to Swiss entities:

- Recommendation on Digital Security Risk Management for Economic and Social Prosperity (2015); [6]
- Recommendation on Digital Security of Critical Activities (2019); [7]
- Recommendation on Artificial Intelligence (2019); [8]
- Guidelines for Cryptography Policy (1997-2017). [9]

[C] European Union

[1] General Relations

Even though it is not a member of the European Union (EU) or the European Economic Area (EEA), Switzerland enjoys shared values with the EU and EEA with respect to data protection matters.

[2] Adequacy Decision

In July 2000, the European Commission formally determined that the data protection laws of Switzerland provide an adequate level of protection to personal information and privacy rights. [10] Following the entry into force of the EU General Data Protection Regulation (GDPR), the European Commission is reviewing the adequacy decisions that were adopted under Directive 95/46/EC. The Commission services have engaged in an intense dialogue with each of the 11 concerned third countries and territories to assess how their data protection systems have evolved since the adoption of the adequacy decision and whether they meet the standard set by the GDPR. Switzerland is one of them and the Commission's assessment is expected to be published soon.

[D] Council of Europe

As a member of the Council of Europe (COE) since 1963, Switzerland is subject to the numerous conventions and protocols developed by the Council of Europe, including, for example, the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950).

[1] Council of Europe Convention on Human Rights and Fundamental Freedoms

The European Convention on Human Rights (ECHR), [11] in its Article 8, sets forth a right to respect for every one's "private and family life, his home and his correspondence," subject to certain restrictions. Specifically:

> *(1) Everyone has the right to respect for his private and family life, his home, and his correspondence.*
>
> *(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

[2] Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

Switzerland has also adhered to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108. [12] A first protocol amending the Convention 108 was adopted in November 2001 (Protocol CETS No. 181), with the aim of strengthening the implementation of its principles. [13] Switzerland ratified the protocol in December 2007.

In 2018, the Council of Europe completed its process of updating Convention 108 in order to deal with the challenges resulting from the use of new information and communication technologies. A protocol amending Convention 108 was adopted in October 2018 (Protocol CETS No. 223). [14] The Swiss Parliament adopted the Federal Decree on the Approval of the Protocol of Amendment, clearing the way for the Federal Council to deposit the instruments of ratification. [15] The updated Convention, known as "Convention 108+," is currently open for ratification. [16] Switzerland has signed but not yet ratified Protocol CETS No. 223. This is expected with the entry into force of the revised Swiss Federal Act on Data Protection (FADP 2020).

[3] Council of Europe Convention on Cybercrime

In 2011, Switzerland ratified the Convention on Cybercrime, which is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with violation of network security, as well as computer related fraud, child pornography, and infringement of copyright. [17]

Footnotes

3 Universal Declaration of Human Rights *available at* : https://www.ohchr.org/en/professionalinterest/pages/crc.aspx ; https://www.unicef.org/child-rights-convention/what-is-the-convention.

4 Text of the 1980 OECD Privacy Guidelines, *available at* https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

5 Text of the 2013 Amended OECD Guidelines, *available at* https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

6 Text available at: https://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm.

7 Text available at: https://www.oecd.org/sti/ieconomy/recommendation-on-digital-security-of-critical-activities.htm.

8 Text available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

9 Text available at: https://www.oecd.org/digital/ieconomy/cryptography.htm

10 Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (Decision 2000/518/EC).

11 European Convention on Human Rights (as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13, and 16), *available at* https://www.echr.coe.int/Documents/Convention_ENG.pdf.

12 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), *available at* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

13 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, *available at* https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/181

14 Text available at: https://rm.coe.int/16808ac918.

15 FF 2020 5559.

16 The text of Convention 108+, which incorporates all of the amendments resulting from Protocol CETS No. 223 is available at https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. *See also* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223.

17 Website *available at* https://www.coe.int/en/web/cybercrime/home ; also *available at* https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#.

Global Privacy and Security Law - Gilbert, § SWI.02, Switzerland,CONSTITUTION

Francoise Gilbert, Global Privacy and Security Law § SWI.02 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

The current federal constitution of Switzerland entered into force on January 1, 2000. [18] This constitution addresses the right to privacy in its Article 13. Article 13 par. 2 of the Federal Constitution of the Swiss Confederation provides:

> *Everyone has the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications. Everyone has the right to be protected against the misuse of their personal data.*

Footnotes

18 Unofficial translation of the Swiss constitution, *available at* http://www.admin.ch/ch/e/rs/c101.html.

Global Privacy and Security Law - Gilbert, § SWI.03, Switzerland,DATA PROTECTION LAW (2020)—HISTORICAL BACKGROUND AND OVERVIEW

Francoise Gilbert, Global Privacy and Security Law § SWI.03 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

Switzerland is in the midst of updating its privacy and data protection framework. At the federal level, the first Federal Data Protection Act was adopted on June 19, 1992 and entered in force on July 1, 1993 (FADP 1992). This law is being phased out. A new Federal Act on Data Protection (2020) was adopted in 2020, and is expected to enter into force in September 2023. At the local level, the cantons have laws that govern the processing of personal data by cantonal governments and bodies such as schools or hospitals. These laws are also being updated.

[A] Federal Act on Data Protection (1992)

In Switzerland, data protection is governed by a Federal Act on Data Protection (FADP), [19] which applies to the processing of personal data:

- By federal bodies, that is, federal authorities and services, and organizations and companies entrusted with federal public tasks (e.g., insurers in the context of compulsory health insurance) and;
- By private entities (natural and legal persons).

In addition, the Ordinance on the Federal Act on Data Protection (OFADP) contains implementing provisions. The FADP (1992) establishes the Federal Data Protection and Information Commissioner (FDPIC), which is the Swiss data protection supervisory authority. [20]

[B] Revision of the FADP (1992)

Since its adoption, the FADP 1992 has undergone two partial revisions, in 2006 and 2010, resulting in minor changes.

In September 2017, the Federal Council submitted to the Federal Assembly a general proposal on the total revision of the FADP 1992 that would:

- Bring the FADP 1992 in line with the European General Data Protection Regulation (GDPR); and
- Implement Directive EU 2016/680 on the protection of natural persons with regard to the processing of personal data in the area of criminal law.

The Federal Assembly decided to divide the review of the Federal Council's draft into two stages to ensure the implementation of EU Directive 2016/680 for the criminal law area as promptly as possible by the deadline

for implementation. The implementation period expired on August 1, 2018, two years after the EU notified Switzerland of the Directive on August 1, 2016.

In its Fall session of 2018, the Federal Assembly approved the necessary amendments to the data protection legislation for the implementation of EU Directive 2016/680, the Schengen FADP (SFADP).

After the approval of the SFADP, the Federal Assembly worked on the revision of the FADP 1992, and on September 25, 2020, approved the final draft of the Federal Act on Data Protection 2020 (FADP 2020). [21]

[C] Federal Act on Data Protection (2020)

The FADP 2020 and its ordinances (to be adopted by the Federal Council and the Federal Assembly) are expected to enter into force in September 2023. Its entry into force will repeal the FADP 1992 and the SFADP.

The FADP 2020 makes several significant changes to the previous law and has numerous similarities with the EU General Data Protection Regulation (GDPR). For example, the FADP 2020 no longer governs the processing of data of a legal person. It includes new categories of sensitive personal information: genetic data and biometric data that uniquely identify an individual. Further, it grants two additional rights for data subjects: the right to data portability and right to object to automated decisions making.

In the same way as GDPR increased the obligations of entities processing personal data, the FADP 2020 also increases the obligations of data controllers as well as those of data processors. Among these new obligations, organizations should note:

- Enhanced information obligations;
- Obligation to maintain records of processing;
- Obligation to conduct Data Protection Impact Assessment where the processing is likely to cause a high risk to an individual;
- Mandatory breach notification obligations; and
- Designation of a local representative established in Switzerland for entities established outside Switzerland that are subject to the FADP 2020 because of their interaction with Swiss data subjects.

Finally, the FADP 2020 will increase the amount of criminal fines for violations. Among other things of note, the criminal provisions of the FADP 2020 are aimed primarily at natural persons, especially those in managerial positions.

However, some particularities remain. Unlike the GDPR, the FADP 2020 does not allow the FDPIC, the Federal Data Protection and Information Commissioner, to issue administrative fines.

[D] Schengen Federal Act on Data Protection (Schengen FADP)

The Schengen Federal Act on Data Protection (Schengen FADP) aims to implement Directive EU 2016/680 on the protection of natural persons with regard to the processing of personal data in the area of criminal law, in accordance with the Schengen Association Agreement between Switzerland and Europe. [22]

The Schengen FADP lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent federal authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of threats to, public security.

In force since March 1, 2019, the Schengen FADP is a temporary law. It will be repealed with the entry into force of the FADP 2020.

[E] Cantonal Law

The Federal State does not have legislative competence over the processing of personal data by cantonal governments and bodies. Accordingly, each canton has its own statutory data protection rules. For example, cantonal law covers data protection processed by public hospitals and public schools.

The cantons must also update their own legislation concerning cantonal bodies in order to keep up with the changes necessitated by the implementation of Directive EU 2016/680. Work on these updates to cantonal laws has reached varying degrees of progress among the cantons.

Footnotes

19 Unofficial English translation of the Swiss FADP 1992, *available at:* http://www.admin.ch/ch/e/rs/c235_1.html.

20 The website of the Swiss Data Protection and Information Commissioner is available at http://www.edoeb.admin.ch/index.html?lang=en.

21 Text of the FADP 2020 available in French at: https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2020/1998/fr/pdf-x/fedlex-data-admin-ch-eli-fga-2020-1998-fr-pdf-x.pdf ; *see also* https://www.parlament.ch/centers/eparl/curia/2017/20170059/Texte%20pour%20le%20vote%20final%203%20NS%20F.pdf.

22 Text available at: https://www.fedlex.admin.ch/eli/cc/2008/113/fr.

Global Privacy and Security Law - Gilbert, § SWI.04, Switzerland,DATA PROTECTION LAW—DEFINITIONS AND KEY CONCEPTS

Francoise Gilbert, Global Privacy and Security Law § SWI.04 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

The text of the FADP 2020 relies on several key terms. Their definitions are found primarily in its Article 5.

[A] Data Subject

The FADP 2020 has restricted the definition of data subjects to natural persons only. Pursuant to its Article 5(b), a data subject is now defined as “the natural person whose personal data is being processed.”

[B] Data to Be Protected

[1] Personal Data

Pursuant to Article 5(a) of the FADP 2020, “all information about an identified or identifiable individual” are deemed to be protected.

Occasionally, the decision whether certain data relates to an identifiable person or not may be difficult. This is illustrated by the decision of the Swiss Federal Supreme Court in the *Logistep* case (1C_285/2009 of September 8, 2010). [23] *Logistep*, a Swiss-based company, specialized in automated searches for offers of unauthorized copies of copyrighted works in peer-to-peer networks by means of its specially developed software. As soon as the software had found such an offer, it would download a copy of the work. While downloading, the software would record information such as the supplier’s IP address, the date and time of the download, and name of the copyrighted work; and it would save this information. The company then would send the recorded data to its clients, the copyright holders of the works concerned.

According to the Court’s decision, the IP addresses collected by *Logistep* are personal data within the meaning of the FADP. This is also the case for so-called “dynamic” IP addresses, which are assigned to changing

customers by Internet providers for each period during which the customers use the Internet access. The owner of the Internet connection for which an IP address was used at a particular time can only be established with the aid of information from the provider. Due to telecommunications secrecy, providers may only give criminal investigation authorities this information under the conditions set by the Federal Act on the Surveillance of Post and Telecommunications (SPTA). Despite these restrictions regarding the identification of the owners of Internet connections, dynamic IP addresses relate, according to the Federal Supreme Court, to data about identifiable people within the meaning of the FADP.

[2] Sensitive Data

Several categories of data, generally known as “sensitive” data, receive special protection. Article 5(c) of the FADP 2020 defines as sensitive personal data the following: [24]

- Data on religious, philosophical, political, or trade union opinions or activities;
- Data on health, intimacy, or racial or ethnic origin;
- Genetic data;
- Biometric data that uniquely identify a natural person;
- Data on criminal and administrative proceedings or sanctions;
- Data on social welfare measures.

[3] Children’s Data

The FADP 2020 does not contain specific provisions for personal data of a child.

[4] Deceased Persons’ Data

The FADP 2020 does not contain specific provisions for personal data of a deceased person. The FADP only applies to the processing of data concerning a living person.

[C] Data Controllers and Processors

[1] Data Controller

Pursuant to Article 5(j) of the FADP 2020, “a data controller is the private person or federal body that, alone or jointly with others, decides on the purposes and means of the processing.”

[2] Data Processor

Pursuant to Article 5(k) of the FADP 2020, “a processor is the private person or federal body that processes personal data for a data controller.”

[D] Processing; Disclosure

[1] Processing

The protection extends to every type of processing of personal data, with “processing” being understood, under Article 5(d) of the FADP 2020, as “any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, recording, storage, use, modification, disclosure, archiving, deletion or destruction of data.”

[2] Disclosure

Article 5(e) of the FADP 2020 defines “disclosure” of data, as transmitting personal data or making them accessible. This may include, for example, granting of access, transmission, or publication.

[E] Data Protection Officer

Article 10 of the FADP 2020 allows private data controllers to appoint a “data protection officer.” [25] Its appointment is not mandatory for private data controllers.

Among his/her duties the data protection officer participates in the implementation of data protection regulation, trains, and advises the data controller in matters of data protection, and serves as the contact point for the data subjects and the data protection authorities in Switzerland.

[F] Key Government Data Supervisory Authorities

The Swiss Confederation is comprised of 26 cantons. Supervision of data processing is allocated between federal and local authorities.

[1] Federal Data Protection Authority

The Federal data protection authority is the Federal Data Protection and Information Commissioner (FDPIC). [26] The FDPIC is responsible for supervising the proper application of the federal data protection regulation. It is the competent authority for data processing for federal bodies and private persons. [27]

[2] Cantonal Data Protection Authorities

Data processing by cantonal and communal bodies is subject to cantonal law. The supervision of processing activities of cantonal authorities is performed by the cantonal data protection commissioners. [28] Several cities have local commissioners.

Footnotes

23 Decision on this issue in the *Logistep* case, *available at* http://jumpcgi.bger.ch/cgi-bin/JumpCGI?id=08.09.2010_1C_285/2009 (only German).

24 The FADP 2020 adds genetic and biometric data to the definition of sensitive data meeting the definition of special category of data is the EU's GDPP.

25 FADP 2020, Article 10(1).

26 FADP 2020, Article 4(1).

27 The website of the FDPIC is available in English at https://www.edoeb.admin.ch/edoeb/en/home.html. It is also available in German, French and Italian.

28 The website of the association of the Cantonal data protection commissioners is available at https://www.privatim.ch/fr/privatim-2/. The list of the cantonal data protection commissioners is available at https://www.edoeb.admin.ch/edoeb/en/home/documentation/datenschutz/schweiz.html.

Global Privacy and Security Law - Gilbert, § SWI.05, Switzerland,DATA PROTECTION LAW—SCOPE OF FADP 2020

Francoise Gilbert, Global Privacy and Security Law § SWI.05 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

[A] Material Scope

The FADP 2020 regulates the processing of personal data by both private persons and federal bodies. [29] It does not apply to:

- The processing of personal data carried out by a natural person for his/her exclusively personal use;
- The processing of personal data carried out by the Federal Assembly and parliamentary committees in the course of their deliberations;
- The processing of personal data by institutional beneficiaries within the meaning of Article 2(3) of the Federal Act of 22 June 2007 on the Privileges, Immunities and Facilities and the Financial Subsidies granted by Switzerland as a Host State who enjoy immunity from jurisdiction in Switzerland.

Article 2 also specifies that the processing of personal data in court proceedings or in federal proceedings, and the rights of the persons concerned, shall be governed by the applicable procedural law and that public registers relating to private law relationships (e.g., a land register) shall be in principle governed by the special provisions of the applicable federal law.

[B] Territorial Scope

Pursuant to Article 3(1) FADP 2020, the FADP applies to processing that have effects in Switzerland, even if they occurred abroad. [30]

Article 3(2) FADP 2020 specifies that private law claims are governed by the Swiss Federal Act of 18 December 1987 on Private International Law. Further the provisions governing the territorial scope of application of the Swiss Criminal Code are also reserved.

Footnotes

29 FADP 2020 Article 2(1).

30 The law thus has a theoretically broader territorial scope than the GDPR, since it covers any fact that has effects in Switzerland without specification.

Global Privacy and Security Law - Gilbert, § SWI.06, Switzerland,DATA PROTECTION LAW—PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

Francoise Gilbert, Global Privacy and Security Law § SWI.06 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

The general principles that apply to the processing of personal data are set forth in Articles 6 and 8 of the FADP 2020. Both data controllers and data processors must meet these principles. The principles are: [31]

- Lawfulness;
- Good faith;
- Proportionality;
- Transparency;
- Purpose limitation;
- Accuracy;
- Security.

[A] Lawfulness of the Processing

Under Article 6(1), personal data must only be collected and processed in accordance with the law. [32] An example of unlawful processing is the procurement of personal data in violation of provisions of the criminal code (unauthorized obtaining of data). [33] For federal bodies, this principle is specificality linked with the obligation to rely on a legal basis to process personal data. [34]

[B] Good Faith and Proportionality

Article 6(2) of the FADP requires that the processing be carried out in good faith and be proportionate.

[1] Good Faith

The principle of good faith requires that the entity processing the data be honest and not misleading. The good faith principle, for example, may be infringed (even if this does not contravene an explicit statutory prohibition) when personal data are collected by stating a false identity or false purpose. [35] Under the FADP 1992, the obligation to inform the data subjects in case of a data security breach was derived from the principle of good faith. [36]

[2] Proportionality

[a] *Proportionality Principle*

The principle of proportionality requires that data processing take place only to the extent necessary to achieve the stated purpose(s) of the processing. [37] In addition, there must be an appropriate relationship between the purpose of the processing of personal data and the intrusion on personal rights associated with the data processing. The principle of proportionality is violated, for example, when personal data are stored for longer than required.

[b] *Example of Application of the Proportionality Principle*

The application of the principle of proportionality was crucial in the decision of the Swiss Federal Supreme Court in the Google Street View case (138 II 346 of May 31, 2012). [38] The Swiss Federal Supreme Court determined that it was not necessary for Google to take further steps in addition to the automated anonymization of faces and vehicle number plates to ensure complete anonymization of all images before uploading them to its Street View service. This was what the FDPIC had requested Google to do because its software for automated anonymization was not 100 percent reliable. The Federal Administrative Court was likewise of this opinion in its decision of April 2011. The Swiss Federal Supreme Court considers it reasonable that the automated anonymization does not fully cover all persons and vehicle number plates, provided that the error quota of inadequately anonymized images is not more than approximately 1 percent.

In addition, the Swiss Federal Supreme Court defined stringent requirements for Google Street View.

For instance, when taking pictures of sensitive establishments, such as schools, hospitals, retirement homes, women’s refuges, courts, and prisons, it deemed it necessary that complete anonymization be carried out before uploading images in the Street View Service. In this case merely pixelating faces and car number plates is not sufficient. It must also be impossible to identify persons by features such as skin color, clothing, walkers, or other aids for disabled persons. Since automated anonymization is not sufficient for this purpose, such photographs must be anonymized by Google manually.

The Court also ruled that, where automated anonymization is sufficient, Google must enable those affected, to report inadequately anonymized images, electronically or by mail and free of charge. Such subsequent reports

must be processed quickly and efficiently, and the inadequate anonymization must be rectified by manual processing. In addition, Google must provide information about this reporting facility both on its website and in the media.

Except with the consent of those concerned, photographs of private areas, e.g., enclosed gardens and yards that are normally concealed from view of passersby, are prohibited. Google is therefore not allowed, without the consent of those concerned, to take photographs from a camera height of more than two meters, as was previously the case. Google was given a transitional period of three years to replace images that contravene this requirement.

Google was also required to provide information in regional and local media about when the cameras will be passing through, and when the data is about to be uploaded. Merely providing information on the Google website is not sufficient. The announcement must be made in each case at least one week before the photography or upload takes place.

[C] Transparency

Article 6(3) of FADP 2020 requires that personal data be collected only for a specific purpose that was either indicated when the data were collected or was evident to the data subjects from the circumstances or is provided for by law. [39]

The transparency is reinforced by a broad and general duty to inform data subjects as soon as personal data is collected. [40] The FADP 1992 only had a duty of information for private data controllers limited to the collection of sensitive personal data and personality profile.

[D] Purpose Limitation

[1] Purpose Limitation Principle

Article 6(3) of FADP 2020 also states that personal data must be processed in a way that is compatible with the initial purposes. Use of personal data for purposes other than those for which they were collected is, in principle, not permissible.

For example, credit card data must not be used to analyze consumer behavior. If, however, legally recognized justification exists, for example, if processing is necessary to fulfill a statutory obligation, data may also be processed for purposes other than those originally stated or evident.

[2] Examples of Application of the Purpose Limitation Principle

In the *Logistep* case decided by the Swiss Federal Supreme Court and already mentioned above, the Court found that Logistep infringed the personal rights of the Internet users concerned by collecting their IP addresses and other data. This is because data collection was not evident to users and they did not anticipate it. As a result, the principle that data may only be processed for the purpose specified or evident during collection was automatically infringed. The Court regarded this impairment of the personal rights of Internet users as not justified by the protection of predominantly private and public interests, namely the protection of copyright on protected works. The Court was aware that this made the protection of copyright significantly more difficult. In contrast, it pointed out that predominantly private interests may only be recognized with reluctance as justification for infringements of the privacy of other persons.

[E] Accuracy

According to Article 6(5), those who process personal data must make certain that the data are accurate. They must take all appropriate measures to ensure that data that are inaccurate or incomplete in view of the purpose of the collection or processing are corrected or destroyed. The appropriateness of the measures depends in

particular on the nature and extent of the data processing and on the risks that the processing entails for the privacy and personal rights of the data subjects. [41]

[F] Security

Data controllers and processors are required to ensure by means of appropriate organizational and technical measures that the security of personal data is adequate in relation to the risk involved. These measures must prevent any breach of security. [42] The OFADP specifies this general obligation more extensively for both private persons and for federal bodies.

Footnotes

31 FADP 2020, Articles 6(1) to 6(7) and 8.

32 FADP 2020, Article 6(1).

33 This principle was confirmed by the Federal Administrative Court TAF, 19.03.2019, A-3548/2018.

34 FADP 2020, Article 34.

35 FADP 2020, Article 6(2).

36 Unlike numerous modern data protection laws, there was no express statutory obligation to inform the concerned parties in case of data loss, theft, or leak. An obligation to report data security breaches is now included in Article 24 of FADP 2020.

37 FADP 2020, Article 6(2).

38 *See* the decision at http://relevancy.bger.ch/php/clir/http/index.php?lang=de&zoom=&type=show_document&highlight_docid=atf%3A%2F%2F138-II-346%3Afr (German only).

39 FADP 2020, Article 6(3).

40 FADP 2020, Article 19.

41 FADP 2020, Article 6(5).

42 FADP 2020, Article 8.

Global Privacy and Security Law - Gilbert, § SWI.07, Switzerland,DATA PROTECTION LAW—DATA SUBJECT'S RIGHTS

Francoise Gilbert, Global Privacy and Security Law § SWI.07 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

The Federal Act on Data Protection 2020, grants data subjects a wide range of rights, which include, for example, the right of access, right of data portability, right of correction, and right of blocking or deletion. In addition, the data subjects must receive notice of the data collection and in many cases must consent to the collection of their information and be informed of the purposes for which the information is collected.

[A] Right to Information

Under the FADP 1992, the duty of information existed for private data controllers only for the collection of sensitive personal data and profiling. [43] As will be discussed in more detail below in terms of the data controller's obligations, the FADP 2020 in its Articles 19 and 20 generalizes this duty to inform for both private persons and federal bodies. Article 19 defines the controller’s duty to inform data subjects when collecting

personal data and Article 20 sets forth exceptions to the duty to inform. Further, Article 21(1) requires the data controller to inform the data subject of a decision that is taken exclusively on the basis of an automated processing, and that has legal effects on the data subject.

[B] Right of Access

[1] Scope

Under Article 25(1) of the FADP 2020, any person is entitled to request information from the data controller on whether data related to him/her are being processed.

Article 25(2) states that the data subject shall be provided with the information necessary to enable him/her to assert his/her rights under the FADP and to ensure the transparency of the processing. The information provided to the data subject must include the following:

- The identity and contact details of the controller;
- The personal data being processed;
- The purpose of the processing;
- The period of time for which the personal data will be kept or, if this is not possible, the criteria for determining this period of time;
- The available information on the origin of the personal data, insofar as such data have not been collected from the data subject;
- Where applicable, the existence of an automated individual decision and the logic on which the decision is based;
- Where applicable, the recipients or categories of recipients to whom personal data is disclosed, as well as the State or international body to which the data is disclosed.

The information is, in principle, to be provided in writing, free of charge, and within 30 days.

The FADP 2020 allows the data controller to handle information on health data through a doctor specified by the person entitled to information. It also specifies that a data controller who has personal data processed by a data processor is still required to provide the requested information. [44]

The right to information cannot be waived in advance. [45]

Article 25(6) requires that the information be provided at no charge to the requesting party. However, there may be exceptions for cases where the efforts involved in gathering the data might be disproportionate.

[2] Restrictions

Pursuant Article 26 of the FADP 2020, the information may be refused, restricted, or its delivery may be delayed if:

- A formal enactment provides for it, in particular to protect a professional secret;
- It is required by an overriding interest of a third party; [46]
- The request is manifestly unfounded, in particular if it pursues an aim contrary to data protection or is manifestly of a frivolous nature.

Article 26(2) also allows private data controllers to refuse, restrict, or delay the delivery of the information to protect their own prevailing interests if they do not disclose the personal data to third parties. Federal bodies have a similar right of refusal with regard to the protection of prevailing public interests, in particular internal and external security, and in order to prevent any risk to the success of criminal investigations and other investigative procedures.

Other possibilities for refusing to supply information exist for those working in the media, in order to protect their sources of information, to prevent access to drafts for publications, or in cases in which the freedom of the

public to form an opinion would be put at risk by the information. The same restriction applies for files that serve exclusively as a personal working tool for a person working in the media. [47]

In any case, the data controller shall state the reason for refusing, restricting, or delaying the provision of information. [48]

[C] Right of Rectification

Under the Principle of Data Accuracy, [49] a data subject is entitled to have inaccurate data rectified whether against private persons [50] or federal bodies. [51] If data cannot be proved either accurate or inaccurate, the data subject is entitled to have an entry added to the data to indicate that their accuracy is disputed. [52]

[D] Right of Opposition

The data subject also has a right to object to the processing of personal data. That right derives from the right to self-determination contained in Article 13 of the Federal Constitution and is expressed in the FADP 2020 in particular as a right of action. [53] It is linked with the right of blocking and deletion grants the data subject the ability to prevent the further use of information.

As will be discussed further below in the section on private right of action, in order to prevent the unauthorized processing of data, the data subject may demand that data processing be prohibited, in particular that unauthorized disclosure to third parties be blocked, and, if the data processing is inadmissible overall, that the data be deleted. [54]

[E] Right to Data Portability

The FADP 2020 contains a new right of data portability. [55]

Under Article 28(1) of the FADP any data subject may request from that data controller, free of charge, the disclosure of the personal data that the data subject disclosed to the controller in a standard electronic format. Article 28(2) grants the data subject the right to request the data controller to disclose that personal data directly to another controller if the disclosure does not involve a disproportionate effort, and if the other grounds for data portability listed below are met.

The right of data portability is free of charge but limited to the data disclosed by the data subject to the data controller (in a broad sense) and only when: [56]

- The data controller processes the personal data in an automated manner; and
- The data is 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.

A data subject may request the controller to transfer his personal data to another data controller if the requirements immediately above are met. The direct sharing with another controller must not involve a disproportionate effort, or an exception may allow the data controller to charge a fee.

Pursuant to Article 29, the right to data portability may be refused by the data controller on the same grounds as mentioned above. The data controller shall in any case indicate the reason for refusing, restricting, or postponing the delivery or transmission of the personal data.

Footnotes

43 Federal bodies, however, had to inform the data subjects of the collection of any kind of personal data.

44 FADP 2020, Article 25(4).

45 FADP 2020, Article 25(5).

46 Article 25(3) specifies that companies belonging to the same group are not considered as third parties.

47 FADP 2020, Article 27.

48 FADP 2020, Article 26(4).

49 FADP 2020, Article 6(3).

50 FADP 2020, Article 32(1).

51 FADP 2020, Article 41(2)(a).

52 FADP 2020, Article 32(3) and Article 41(4).

53 FADP 2020, Article 32(2) and Article 41(1).

54 FADP 2020, Articles 32, 37, and 41.

55 FADP 2020, Article 28.

56 FADP 2020, Article 28(1).

Global Privacy and Security Law - Gilbert, § SWI.08, Switzerland,DATA PROTECTION LAW—CONTROLLER'S OBLIGATIONS

Francoise Gilbert, Global Privacy and Security Law § SWI.08 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

[A] Lawfulness of Processing

[1] Processing by Private Persons

In Switzerland, and as opposed to the GDPR, the processing of personal data is based on a presumption of lawfulness and does not systematically require a justification (Article 30 FADP 2020). On the other hand, there is a presumption of unlawful infringement of the privacy of the data subjects when:

- Personal data is processed in violation of the principles of Articles 6 and 8 of the FADP 2020;
- Personal data is processed against that person's declaration of intent;
- Sensitive personal data is disclosed to third parties (independent controllers).

Article 31 of the FADP 2020 (Justifications) sets forth the grounds for justifying an infringement of the data subjects' privacy. Thus, such an infringement can be justified : (i) by the consent of the victim, (ii) by an overriding private or public interest, or (iii) by law.

Article 31(2) provides a non-exhaustive list of overriding interests to allow the controller to justify such an infringement. For example:

- The processing is directly related to the conclusion or performance of a contract and the data processed concerns the contracting party;
- The processing is part of a current or future competitive economic relationship with another person, provided that no personal data processed is communicated to third parties;
- Personal data are processed for the purpose of assessing the creditworthiness of the data subject, provided certain conditions are met; [57]

- Personal data are processed in a professional manner exclusively for publication in the editorial section of a periodical medium or, if publication does not take place, serves exclusively as a personal working tool;
- Personal data are processed for purposes that do not relate to individuals, in particular for research, planning or statistics, if certain conditions are met; [58]
- The personal data collected concern a public figure and relate to his or her public activity.

[2] Processing by Federal Bodies

According to Article 34(1) of the FADP 2020, [59] Federal bodies may process personal data only if there is a legal basis for doing so. They are required to respect the principles and the legal basis and cannot rely on the justification set forth in Article 31.

In a more restrictive way, the FADP 2020 provides that federal bodies may process sensitive data or profiling data only if a formal enactment [60] expressly provides so. The same formality is required if the purpose or manner of the processing of personal data is likely to cause serious harm to the fundamental rights data subjects. [61] As an exception, a legal basis in a law in the substantive sense is sufficient if the processing is indispensable for the performance of a task defined in a formal enactment or if the purpose of the processing does not present any particular risk for the fundamental rights. [62]

Article 34(3) of the FADP 2020 nevertheless authorizes the processing of personal data by federal bodies in the absence of a legal basis when:

- The Federal Council has authorized the processing, considering that the rights of the data subjects were not endangered;
- The data subject has consented to the processing in question or has made his personal data general accessible and has not expressly prohibited its processing;
- The processing is necessary 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 period of time.

[B] Duty to Provide Information

[1] Duty to Inform the Data Subjects

The FADP 2020 provides that the collection of personal data and in particular its purpose must be transparent to the data subjects. Moreover, while the FADP 1992 only imposed a duty to inform on federal bodies and, in a limited way, on private persons, the FADP 2020 now extends to an actual and broad duty to inform data subjects for both private persons and federal bodies.

Pursuant Article 19(1) of the FADP 2020, the data controller must adequately inform the data subject of the collection of personal data, whether the data are collected from the data subject or not. The data controller must provide all information necessary to enable data subjects to assert their rights and to guarantee the transparency of the processing. In this respect, at least the following must be communicated: [63]

- The identity and contact details of the data controller;
- The purpose of the processing;
- Where applicable, the recipients or categories of recipients to whom personal data are transmitted;
- If the personal data is not collected from the data subject, the categories of data processed;
- If the personal data is communicated abroad, the name of the State or international organization to which it is communicated and, if applicable, the guarantees provided.

If the personal data is not collected from the data subject, the data controller must provide the data subject with the above-mentioned information no later than one month after it has obtained the personal data. If it discloses

the personal data before the expiry of this period, it must inform the person concerned at the latest at the time of disclosure. [64]

[2] Restrictions

The controller is released from the duty to provide information pursuant to Article 19 if one of the following conditions is met: [65]

- The data subject already has the relevant information;
- The processing of personal data is provided for by law;
- The controller is a private person and is bound by a legal obligation to maintain secrecy;
- The conditions of restrictions on the right of access applicable to medias are fulfilled.

Further, the controller may restrict, defer, or waive the provision of information if any of the following conditions is met:

- The overriding interests of a third party so require;
- The information prevents the processing from achieving its purpose;
- The controller is a private person and his overriding interests require it, and he does not disclose the data to a third party; [66]
- The controller is a federal body and an overriding public interest such as the internal or external security of Switzerland so requires, or if the disclosure of the information is likely to jeopardize an investigation, an inquiry, or a judicial or administrative procedure.

The FADP also specifies that the duty to inform does not apply when personal data is not collected from the data subject if the information is impossible to give, or if it requires disproportionate efforts. [67]

[C] Automated Individual Decisions

The FADP 2020 incorporates in its Article 21 an obligation similar to that which is found in the EU General Data Protection Regulation [68] regarding automated individual decisions. According to this provision, the data controller is required to inform the data subject of any decision that is taken exclusively on the basis of an automated processing of processing and that has legal effects on him/her or significantly affects him/her.

Most importantly, if the data subject so requests, the controller is required to give him/her the opportunity to state his/her opinion. The data subject also has the right to request that the automated individual decision be reviewed by a natural person. [69]

The above-mentioned rules do not apply if the automated individual decision is directly related to the conclusion or performance of a contract between the controller and the data subject and the request of the data subject is fulfilled, or if the data subject expressly consented to the decision being made by automated means. [70]

[D] Data Protection by Design and by Default

In its Article 7, the FADP 2020 introduces the obligations of Data Protection by Design and Data Protection Default. These obligations are similar to those found in the EU General Data Protection Regulation, Articles 25(1) and 25(2). [71] Data protection by design and by default are complementary obligations that mutually reinforce each other.

[1] Data Protection by Design

Article 7(1) the FADP 2020 introduces the obligation of “privacy by design,” an obligation for the data controller to set up technical and organizational measures in order for the data processing to meet the data protection regulations and in particular the principles set out in Article 6. The data controller must consider this

obligation from the planning of the processing and through all phases of the processing, including updates and modifications. This is not a principle per se and its violation does not constitute a violation of personality within the meaning of FADP 2020 Article 30(2).

Under Article 7(2) of the FADP 2020, the technical and organizational measures must be appropriate in particular regarding the state of the art, the type and extent of processing, as well as the risks that the processing at hand poses to the personality and the fundamental rights of the data subjects.

[2] Data Protection by Default

The obligation to ensure data protection by default is also an obligation deriving from the proportionality principle. According to FADP 2020 Article 7(3), the data controller must ensure through appropriate predefined settings that the processing of the personal data is limited to the minimum required by the purpose, unless the data subject directs otherwise.

[E] Data Protection Impact Assessment

According to Article 22 of the FADP 2020, a data protection impact assessment must be carried out whenever a planned processing operation is likely to result in a high risk to the personality or fundamental rights of the data subject.

Article 22(2) specifies that the existence of a high risk, when using new technologies, depends on the nature, extent, circumstances, and purpose of the processing. Such a risk exists, for example, in the case of large-scale processing of sensitive data or the systematic monitoring of large parts of the public domain.

The impact assessment must contain a description of the proposed processing, an assessment of the risks to the personality or fundamental rights of the data subject, and the measures planned to protect the personality and fundamental rights of the data subject. [72]

The private data controller has the right not to conduct the impact assessment: [73]

- If the processing is required by virtue of a legal obligation;
- If it uses a system, product, or service that (i) is certified in accordance with Article 13 of the FADP 2020 for the intended use, or (ii) complies with a code of conduct in accordance with Article 11. [74]

[F] Prior Consultation with the Federal Data Protection and Information Commissioner (FDPIC)

Pursuant to Article 23 of the FADP 2020, the data controller must consult the Federal Data Protection and Information Commissioner (FDPIC) prior to the processing when the data protection impact assessment reveals that, despite the measures planned by the data controller, the planned processing presents a high risk to the personality or fundamental rights of the data subject.

The FDPIC must notify the controller of its objections to the intended processing within two months. This period may be extended by one month in case of complex data processing. If the FDPIC has objections to the proposed processing, it shall propose appropriate measures to the controller.

It is interesting to note that the private controller may abstain from consulting with the FDPIC if it has first consulted its data protection officer. [75] This is one of the few advantages of having a data protection officer expressly stipulated by Swiss law.

[G] Representatives of Controllers Not Established in Switzerland

Article 3(1) of the FADP 2020 provides that the Act applies to fact patterns that have an effect in Switzerland even if they occurred abroad. In addition, Articles 14 and 15 of the FADP 2020 anticipates that private controllers might only have a registered office or a residence abroad.

[1] When Appointment of a Swiss Representative Is Required

According to Article 14 of the FADP 2020, a private data controller with a domicile or residence abroad must appoint a representative in Switzerland and publish his/her name and address when it processes personal data relating to persons located in Switzerland and the processing meets the following conditions:

- The processing is connected to the supply of goods or services or the monitoring of the behavior of persons in Switzerland. However, there is no requirement that the entity specifically target the Swiss market or Swiss residents;
- The processing is conducted on a large scale;
- The processing is a regular processing;
- The processing poses a high risk to the personality of the persons concerned.

This representative will be the contact point for the data subjects and the FDPIC, the Swiss Data Protection Authority.

[2] Duties of the Swiss Representative

Article 15 defines the duties of the representative:

- The representative must keep a register of the processing activities of the controller that contains specified information;
- The representative must provide the information contained in the register to the FDPIC upon request;
- The Representative must provide a data subject, upon request, with information on how the data subject can exercise his rights.

The information to be contained in the register of processing activities to be held by the representative is the same as that which is required to be included in the Inventory of Processing Activities that the controller must keep under Article 12 of the FADP 2020.

Footnotes

57 FADP 2020, Article 31(2)(c).

58 FADP 2020, Article 31(2)(e).

59 Formerly Article 17(1) of the FADP 1992.

60 A formal enactment an act that is adopted by the Federal Assembly as part of the legislative process and is entitled “law.”

61 FADP 2020, Article 34(2)(c).

62 FADP 2020, Article 34(3).

63 FADP 2020, Articles 19(2), 19(3), 19(4).

64 FADP 2020, Article 19(5).

65 FADP 2020, Article 20(1).

66 Companies belonging to the same group are not considered as third parties.

67 FADP 2020, Article 20(2).

68 GDPR, Article 22.

69 FADP 2020, Article 21(2).

70 FADP 2020, Article 21(3).

71 The European Data Protection Board (EDPB) had published guidelines and recommendations that explain how to implement the data protection by design and by default requirements. *See* https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

72 FADP 2020, Article 22(3).

73 FADP 2020, Article 22(4) and (5).

74 Pursuant to Article 22(5), the Code of conduct must meet the following conditions: (a) it is based on an impact analysis relating to the protection of personal data; (b) it provides for measures to protect the personality and fundamental rights of the data subject; and (c) it has been submitted to the FDPIC.

75 FADP 2020, Article 23(4).

Global Privacy and Security Law - Gilbert, § SWI.09, Switzerland,DATA PROTECTION LAW—ENGAGING A DATA PROCESSOR

Francoise Gilbert, Global Privacy and Security Law § SWI.09 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

The controller may engage processors to carry out certain operations on its behalf. Processing operations within the same legal person do not in principle constitute a case of outsourcing.

According to Article 9(1) of the FADP 2020, the processing of personal data may be assigned to third parties by agreement or by law under two conditions:

- The personal data processing is carried out only if the controller would be entitled to carry out that processing itself; and
- There is no legal or contractual obligation to maintain secrecy. [76]

While Article 9 requires that there be a contract, unlike Article 28 of GDPR, there are no specific requirements on the content of the contract, nor on its form, which can continue to be oral. A written contract is preferable for reasons of proof and required for federal bodies (signed agreement).

In all cases, the controller must ensure that the processor is able to guarantee the security of the data and the data processor may only outsource processing to a third party with the prior consent of the controller. [77] The processor may assert the same justifications as the controller. [78]

Footnotes

76 The outsourcing of personal data protected by secrecy restrictions is not excluded, but the specific conditions applicable to the secrecy concerned must be respected.

77 FADP 2020, Article 9(2) and (3).

78 FADP 2020, Article 9(4).

Global Privacy and Security Law - Gilbert, § SWI.10, Switzerland,DATA PROTECTION LAW—REGISTER OF PROCESSING ACTIVITIES

Francoise Gilbert, Global Privacy and Security Law § SWI.10 (First Edition, Supp. #40 2009)

First Edition, Supp. #40

Last Update: 1/2023

[A] Register of Processing Replaces Notification of FDPIC

The reform of the Swiss data protection law has made it possible to move from an obligation for certain data controllers to declare some of their files to the FDPIC [79] to an obligation for controllers (and processors) to keep a record of their processing activities.

Article 12 of the FADP 2020 requires controllers and processors to keep a record or inventory of their processing activities. It should be noted that both controllers and processors have this obligation; however, there are differences between their respective obligations.

[B] Content of Register of Processing by Data Controller

Pursuant to Article 12(2), the controller's register must contain at least the following information:

- The identity of the controller;
- The purpose of the processing;
- A description of the categories of data subjects and the categories of personal data processed;
- The categories of recipients;
- If possible, the period of storage of the personal data or the criteria for determining the storage period;
- A general description of the measures taken to ensure data security; and
- In the case of disclosure of personal data abroad, the name of the State concerned, and the guarantees provided to meet the requirements concerning cross-border disclosures of personal data under Article 16 of the FADP.

[C] Content of Register of Processing Held by a Data Processor

Processors are also required to establish and maintain a register of processing. For a processor, the register of processing activities must contain:

- Information concerning the identity of the processor and the controller;
- The categories of processing operations carried out on behalf of the controller;
- A general description of the measures taken to ensure data security; and
- In case of case of disclosure of personal data abroad, the name of the State concerned, and the guarantees provided to meet the requirements of Article 16. [80]

[D] Exceptions to the Obligation to Keep a Register of Processing

The obligation to keep a register of the processing activities is limited in scope. Article 12(5) states that the Federal Council shall provide for exceptions for companies that have fewer than 250 employees and whose data processing presents a limited risk of harm to the personality of the persons concerned. [81]

[E] Obligations for Federal Agencies

While private entities no longer have to notify the FDPIC, federal bodies must both keep a record of their processing activities, and file that record with the FDPIC. [82]

Footnotes

79 Pursuant to the FADP 1992, federal bodies as well as private data controllers regularly processing sensitive data, profiling, or disclosing personal data to third parties, were required to declare their files to the FDPIC for registration.

80 FADP 2020, Article 12(3).

81 FADP 2020, Article 12(5).

82 FADP 2020, Article 12(4).

Global Privacy and Security Law - Gilbert, § SWI.11, Switzerland,DATA PROTECTION LAW—DATA PROTECTION OFFICER

Francoise Gilbert, Global Privacy and Security Law § SWI.11 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

[A] Ability to Appoint a Data Protection Officer

Article 10 of the FADP 2020 allows private data controllers to appoint a data protection officer. [83] The French and German versions of the law might cause confusion. The French version of FADP 2020 uses the term "conseiller" which means "advisor," while the German version uses the term "Datenschutzverantwortlichen" which means "person responsible for data protection." [84]

This provision varies from the equivalent provision in the GDPR, which mandates (as opposed to "allow") the appointment of a data protection officer in certain cases. Article 37 of the GDPR requires controllers and processors to designate a data protection officer (DPO) when their core processing activities consist of:

- Activities whose scope or purposes require regular and systematic monitoring of data subjects on a large scale, or
- Processing on a large-scale of data that are part of the "special categories of data" (e.g., data pertaining to health or race) or data relating to criminal convictions and offenses.

In addition, public authority or bodies (except for courts acting in judicial capacities) that process personal data are also required to appoint a DPO.

[B] Tasks of the Data Protection Officer

According to Article 10(2) of the FADP 2020, the data protection officer is the contact point for the data subjects and the data protection authorities in Switzerland. Further, his/her duties include:

- Training and advising the private data controller in matters of data protection; and
- Participating in the implementation of the data protection regulations.

The data protection officer may be a company employee or an external third party. [85] The DPO must possess the necessary expertise and may not perform any activities that are not compatible with his/her responsibility as data protection officer. His/her duties include inspection of data processing in the company, recommendation of corrective measures in the event of infringement of the data protection provisions, and maintenance of the register of processing activities. [86]

In organizational terms, the data protection officer has a position within the company that allows him/her to carry out his/her duties independently, without being bound by instructions from the company management. In addition, the necessary resources must be made available to the DPO and the DPO has the right of access to all

personal data files and all other information within the company to which the DPO needs access in order to fulfill his/her tasks.

The law does not provide for any specific sanction for the data protection officer if he/she fails to fulfill his/her responsibilities or to fulfill them adequately. In such a case, the DPO is primarily responsible to the company under civil or labor law, because he has not performed the task assigned to him. At most, he may become liable to prosecution pursuant to the penal provisions cited in the “Enforcement” section below.

[C] Consequences of the Appointment of a Data Protection Officer; Exemption from Prior-Consultation Obligation

One of the few advantages conferred by the law on private data controllers who have appointed a data protection officer is that the private controller may invoke the exemption to the obligation to conduct a pre-consultation with the FDPIC when such prior-consultation would be required by Article 23 of the FADP 2020.

As explained elsewhere in this chapter, there are circumstances where a data protection impact assessment is required under Article 22 of the FADP 2020. When the data protection impact assessment reveals that, despite the measures planned by the data controller, the envisaged processing still poses a high risk to the personality or fundamental rights of the data subject, Article 23 of FADP 2020 requires that the data controller meet with the FDPIC to further evaluate the planned processing. Article 23(4) allows the controller to abstain from consulting with the FDPIC if the controller has appointed a data protection officer.

However, this exemption is available only under the conditions that the data protection officer: [87]

- Performs his or her function independently of the controller, and without being bound by instructions;
- Does not perform activities that are incompatible with his/her duties as data protection officer;
- Has the necessary professional knowledge; and
- The data controller publishes the contact details of the data protection officer, and communicates them to the FDPIC.

Footnotes

83 FADP 2020, Article 10(1).

84 *See also* https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/entreprises/les-conseillers-a-la-protection-des-donnees-en-entreprise/les-conseillers-a-la-protection-des-donnees-en-entreprise.html, (in French) regarding the issue under FADP 1992.

85 *See, e.g* ., https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/entreprises/les-conseillers-a-la-protection-des-donnees-en-entreprise/les-conseillers-a-la-protection-des-donnees-en-entreprise.html.

86 *See generally* https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/entreprises/les-conseillers-a-la-protection-des-donnees-en-entreprise/les-conseillers-a-la-protection-des-donnees-en-entreprise.html. Available in German, French and Italian.

87 FADP 2020, Article 10(3).

Global Privacy and Security Law - Gilbert, § SWI.12, Switzerland,DATA PROTECTION LAW—SECURITY OF PERSONAL DATA; DATA SECURITY BREACHES

Francoise Gilbert, Global Privacy and Security Law § SWI.12 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

[A] Security

Article 8(1) of the FADP 2020 requires controllers and processors to ensure the security of personal data through adequate technical and organizational measures. These measures must appropriately address the risk to such data.

Article 8(2) specifically requires that the technical and organizational measures enable the avoidance of security breaches.

Article 8(3) assigns to the Federal Council the responsibility to issue provisions on the minimum requirements for data security.

[B] Notification of Data Security Breaches

Article 5(h) of the FADP 2020 defines a “data security breach” as a breach of security that leads to an unintentional or unlawful loss, deletion, destruction, or modification of personal data or to personal data being disclosed or made accessible to unauthorized third parties.”

[1] Notification by the Data Controller

When a data security breach occurs, Article 24(1) of the FADP 2020 requires that the data controller notify the Data Protection Commissioner (FDPIC) as soon as possible if the data security breach is likely to result in a high risk to the data subject's personality or fundamental rights.

Compared to the EU GDPR Article 33, Swiss law requires a higher degree of risk to trigger a notification obligation. GDPR Article 33 requires that the notification be provided within 72 hours of becoming aware of the data breach, and the notification must be made in all cases, except if the breach is “unlikely to result in a risk to the rights and freedoms of natural persons.”

Under Article 24(2) of the FADP 2020, the notification must indicate at least:

- The nature of the data security breach;
- The consequences of the breach; and
- The measures taken or foreseen.

[2] Notification by the Data Processor

Article 24(3) requires the data processor to notify the controller of any data security breach as soon as possible. [88]

[3] Notification of the Data Subjects

Article 24(4) requires the controller to inform the data subject only when:

- Notification is necessary to protect the data subject; or
- The FDPIC requires that the concerned data subjects be notified. [89]

The necessity to protect the data subject is to be broadly understood (e.g., renew passwords, organize a press conference). It is not directly linked to a higher degree of risk, but to the possibility to mitigate the risk. [90]

There are nuances to the obligation to inform data subjects. Article 24(5) allows the data controller to restrict, postpone, or refrain from providing the information to the data subject (but not the notification to the FDPIC) in the following cases:

- There is an overriding private or public interest, or a legal duty to maintain secrecy that prohibits it;

- The information is impossible to provide or providing it would require disproportionate efforts;
- The information of the data subject can be ensured in an equivalent manner by a public announcement.

Footnotes

88 FADP 2020, Article 24(3).

89 FADP 2020, Article 24(4).

90 FF 2017 6681-6682.

Global Privacy and Security Law - Gilbert, § SWI.13, Switzerland,DATA PROTECTION LAW—CROSS-BORDER DISCLOSURE OR TRANSFER OF PERSONAL DATA

Francoise Gilbert, Global Privacy and Security Law § SWI.13 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

[A] Principles

While under the FADP 1992 the Swiss FDPIC was responsible for publishing a list of states that had legislation providing an adequate level of protection, this role is now expressly devolved to the Federal Council by application of Article 16(1) of the FADP 2020. The list of countries with legislation providing an adequate level of data protection is now in the Annex 1 of the FADP 2020.

Therefore, under FADP 2020, personal data may be communicated abroad if the Federal Council has established that the State or the international organization concerned has legislation ensuring an adequate level of protection. [91]

In the absence of a decision by the Federal Council, personal data may be disclosed abroad only if an appropriate level of protection is guaranteed by: [92]

- An international treaty;
- Contractual data protection clauses in a contract between the controller or the processor and his co-contractor, communicated in advance to the FDPIC;
- Specific guarantees drawn up by the competent federal body and communicated in advance to the FDPIC;
- Standard data protection clauses previously approved, established, or recognized by the FDPIC;
- Binding corporate rules previously approved by the FDPIC or by a data protection authority of a State that ensures an adequate level of protection.

[B] Standard Contractual Clauses

In a statement of August 27, 2021, the FDPIC recognized the Standard Contractual Clauses (SCCs) for the transfer of personal data out of the EU/EEA to third countries that were adopted in the EU/EEA to meet the requirements of the GDPR. [93] These SCCs were adopted formally in the EU/EEA through Implementing Decision 2021/914/EU). [94]

In its statement, the FDPIC recognized that those SCCs could serve as the basis for personal data transfers to a country without an adequate level of data protection, provided that the necessary adaptations and amendments are made for use under Swiss data protection law. The mandatory adaptations concern the supervisory

authority, the applicable law for contractual claims, the place of jurisdiction, and other adjustments regarding references to the GDPR.

The SCCs currently in effect in the EU/EEA are comprised of:

- Four templates that meet the requirements set forth in GDPR Art. 46 (to be used for crossborder transfers of personal data when a party is located outside the EU/EEA); [95] and
- One template that meets the requirements set forth in GDPR Art. 28 (to be used when the processing of personal data is conducted by a processor). [96]

[C] Swiss-U.S. Privacy Shield

For several years, the Swiss-U.S. Privacy Shield offered business friendly means of transferring personal data to U.S.-certified companies [97] in the same way as the EU-U.S. Privacy Shield eased that transfer of personal from the EU/EEA to the United States. The Swiss-U.S. Privacy Shield suffered the same fate as the EU-US Privacy Shield, which was declared invalid on July 16, 2020, by the European Court of Justice (CJEU). [98] The FDPIC issued a similar statement indicating that it no longer considers the U.S.-Swiss Privacy Shield a sufficient legal basis for transfers of personal data from Switzerland to the United States and supplementary measures are recommended. [99]

[D] Derogations to the Cross-Border Disclosure Rules

As a derogation from Articles 16(1) and 16(2) of FADP 2020, personal data may be disclosed abroad in the following cases:

- The data subject has expressly given his consent to the disclosure;
- The disclosure is directly related to the conclusion or performance of a contract between the controller and the data subject, or between the controller and his co-contractor, in the interest of the data subject;
- The communication is necessary to safeguard an overriding public interest or to establish, exercise, or defend a right before a court or other competent foreign authority;
- The disclosure is necessary to protect the life or physical safety of the data subject or a third party and it is not possible to obtain the consent of the data subject within a reasonable time;
- The data subject has made the personal data available to anyone and has not expressly objected to the processing;

The personal data originate from a register provided for by law, which is accessible to the public or to any person having a legitimate interest, provided that the legal requirements for consultation in the case in question are met.

Footnotes

91 Pursuant Article 18 of the FADP 2020, the publication of personal data by means of automated information and communication services for the purpose of informing the public is not considered to be communication abroad, even if the data can be accessed from abroad.

92 FADP 2020, Article 16(2).

93 Statement available at: https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#-1259254222.

94 SCC Implementing Decision available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

95 The EU Standard Contractual Clauses for International Transfers are available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

96 Note that the FADP 2020 does not have a provision equivalent to GDPR Art. 28, requiring that, when a private controller hires a processor to perform certain services, there be a written contract between these parties, and

that the contract contain specific clauses that must meet specific objectives. The EU Standard Contractual Clauses for controller to processor contracts are available at https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors.

97 https://www.privacyshield.gov/.

98 Press release of the CJEU, *available at* https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf ; full text of the decision, *available at* https://curia.europa.eu/juris/document/document.jsf;jsessionid=359783FFD29340BD65ED02016F1F2684?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1337979.

99 *See* Policy Paper of the FDPIC, *available at* https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2020/Positionspapier_PS_%20ED%C3%96B_EN.pdf.download.pdf/Positionspapier_PS_%20ED%C3%96B_EN.pdf ; and the Guide to checking the admissibility of direct or indirect data transfers to foreign countries, *available at* https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20EN.pdf.download.pdf/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20EN.pdf.

Global Privacy and Security Law - Gilbert, § SWI.14, Switzerland,DATA PROTECTION LAW—CODES OF CONDUCT AND CERTIFICATION MECHANISMS

Francoise Gilbert, Global Privacy and Security Law § SWI.14 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

Like the EU General Data Protection Regulation (GDPR), the FADP 2020 contains provisions for the creation of codes of conduct and certification bodies intended to help entities subject to the law to demonstrate their compliance with the law.

[A] Codes of Conduct

Article 11 of the FADP 2020 introduces the notion of codes of conduct. Professional associations, industry associations, and business associations whose statutes entitle them to defend the economic interests of their members, as well as federal bodies, may submit codes of conduct to the FDPIC, which would then have to review the document, and publish his opinion on the codes of conduct. It is not clear yet whether codes of conducts will be widely used or if Article 11 will just be an empty provision like it used to be with the certifications. At least, the legal advantages are very limited.

In the European Union, since the adoption of the GDPR, several trade organizations have developed Codes of Conduct intended to simplify certain processes or create uniform policies to facilitate the exchange of data. Some of these Codes of Conduct have been developed at the state level, and other at the EU/EEA level. Once the Code of Conduct is complete, it must be reviewed and adopted by the relevant data protection authority. For example, in May 2021, the European Data Protection Board (EDPB) approved a Code of Conduct for Cloud Services Providers submitted to Scope Europe, [100] and a Code of Conduct for Cloud Infrastructure Service Providers submitted by CISPE. [101]

[B] Certification Mechanisms

Article 13 of the FADP 2020 sets forth the general rules for a certification scheme. It allows providers of data processing systems or software as well as data controllers and data processors to submit their systems, products, and services for evaluation by recognized independent certification organizations.

The concept of certification is not new; it existed under the FADP 1992. Under FADP 1992, attempts were made to provide guidance on criteria for acceptable certification mechanisms. So far it has not received much interest because the process was complicated with almost no legal benefit.

In the European Union, the GDPR, in its Article 43, also encourages the establishment of data protection certification mechanisms and data protection seals and marks through which controller and processors can demonstrate their compliance with the Regulation. [102] There has been significant progress, as businesses view the certification as a means to reassure their customers that their processes meets the requirements of the applicable laws. [103] In February 2022, the EDPB issued its first opinion on certification criteria presented for approval by the GDPR-CARPA certification scheme submitted by the Luxembourg Supervisory Authority. [104]

Footnotes

100 Opinion 16/2021 of the EDPB, *available at* https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-162021-draft-decision-belgian-supervisory_en.

101 Opinion 17/2021 of the EDPB, *available at* https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-162021-draft-decision-belgian-supervisory_en.

102 In the EU, the certifications will be issued by certification bodies that have been accredited by the competent supervisory authority or a national accreditation body named in accordance with Regulation (EC) No.765/2008 of the European Parliament and of the Council (20) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the competent supervisory authority. Member States may also develop requirements for accreditation. For example, in Greece, the Hellenic Data Protection Authority has submitted draft supplementary criteria for accreditation to the EDPB and the EDPB has published Opinion 22/2020 on the draft decision of the competent supervisory authority of Greece regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43(3). https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinion_202022_on_the_el_sa_accreditation_requirements_for_certification_body_en.pdf.

103 *See, e.g* ., Statement of Andrea Jelinek, Chair of EDPB:

> This opinion is an important step towards greater GDPR compliance. The main aim of certification mechanisms is to help controllers and processors demonstrate compliance with the GDPR. Controllers and processors adhering to a certification mechanism also gain greater visibility and credibility, as it allows individuals to quickly assess the level of protection of the processing operations.

(https://edpb.europa.eu/news/news/2022/edpb-adopts-first-opinion-certification-criteria_en).

104 https://edpb.europa.eu/news/news/2022/edpb-adopts-first-opinion-certification-criteria_en. While the EDPB opinion requires that a number of changes need to be made to the draft certification criteria, it is nevertheless encouraging to see that the concept of certification is getting traction.

Global Privacy and Security Law - Gilbert, § SWI.15, Switzerland,DATA PROTECTION LAW—FEDERAL DATA PROTECTION AND INFORMATION COMMISSIONER (FDPIC)

Francoise Gilbert, Global Privacy and Security Law § SWI.15 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

[A] Role of the Federal Data Protection and Information Commissioner (FDPIC)

Article 4(1) of the FADP 2020 identifies the Federal Data Protection and Information Commissioner (FDPIC) as the Federal government agency responsible for supervising the proper application of the federal data protection law. [105] The scope of the supervision is limited. Several federal entities of the Swiss government, judiciary, and law enforcement are outside the scope of FDPIC supervision. [106]

The FDPIC is the competent authority for data processing by federal bodies and private persons. Data processing activities by cantonal or communal authorities are under the supervision of the cantonal and communal data protection commissioners.

The roles, tasks and powers of the Federal Data Protection Commissioner are detailed in Chapter 7 of the FADP 2020.

[B] Organization

Enforcement of the FADP is primarily the responsibility of the Federal Data Protection and Information Commissioner (FDPIC). Pursuant to Article 44(1) of the FADP 2020, the head of the FDPIC (the Commissioner) is elected by the Federal Assembly for four years. The appointment may be renewed twice. [107]

The Commissioner fulfills his responsibilities autonomously and independently without receiving or soliciting instructions from any authority or third party. The Commissioner has its own permanent secretariat and own budget. [108] He/she hires its own staff. He/she cannot be a member of the Federal Assembly, Federal Council, or hold any other office in the service of the Swiss Confederation. He/she cannot also engage in any secondary activity. [109]

According to Article 44(3) of the FADP 2020, the Federal Assembly may only dismiss the Commissioner before the end of his or her term of office:

- If he or she has seriously violated his or her duties intentionally or through gross negligence; or
- If he or she has permanently lost his or her capacity to perform his or her duties.

[C] General Responsibilities

The responsibilities and missions of the FDPIC have been considerably increased by the FADP 2020. The responsibilities of the FDPIC now include: the monitoring of compliance with the FADP and other data protection provisions by either federal bodies and private persons; the conduct of investigations into violations of data protection regulations; the administrative assistance to cantonal, federal, and foreign authorities in Switzerland; the maintenance of a register of processing activities of federal bodies; the submission of its annual report; and the information, training, and general awareness in the field of data protection. [110]

[D] Conduct of Investigations

Article 49 of the FADP 2020 allows the FDPIC to initiate an investigation against a federal agency or a private person, either ex officio or on the basis of a complaint, if there are sufficient indications that certain data processing may be in breach of data protection provisions.

Pursuant Article 50(1) of the FADP 2020, if the federal body or private person fails to comply with its obligation to cooperate, the FDPIC can order during the investigation and with the assistance of other federal bodies as well as with the help of cantonal or communal police: [111]

- Access to all information, documents, records of processing activities and personal data necessary for the investigation;
- Access to premises and facilities;
- The hearing of witnesses;
- Expert testimony.

[E] Administrative Measures

Under Article 51(1) of the FADP 2020, if data protection provisions are violated, the FDPIC may order the modification, suspension or cessation of all or part of the processing as well as the deletion or destruction of all or part of the personal data. Article 51(2) allows the FDPIC to suspend or prohibit the unlawful disclosure of personal data abroad. However, the FDPIC cannot impose any fine.

In addition, under Article 51(3)-(4), the FDPIC may order the federal body or the private data controller to:

- Provide information to the FDPIC or the data subjects under Articles 16 and 17 (Cross Border Data Disclosures);
- Take measures to ensure the security of its personal data processing, as required by Article 7 (Data Protection by Design and by Default) and 8 (Security);
- Inform the data subjects under Articles 19 (Duty of Information when Collecting Personal Data) and 21 (duty of Information in the Case of Automated Individual Decisions)
- Carry out a data protection impact assessment in accordance with Article 22;
- Consult with the FDPIC in accordance with Article 23 in connection with the performance of a data protection impact assessment;
- Inform the FDPIC or the data subjects in accordance with Article 24 (Security Breach Notification);
- Provide the data subjects with the information required by Article 25 (Right of Access);
- Appoint a representative in accordance with Article 14 (Data Representative for Controllers with an Office or Residence Abroad).

If the federal body or the private person has taken the necessary measures during the investigation to restore compliance with the data protection requirements, the FDPIC may only issue a warning, as provided in Article 51(4) of the FADP 2020.

[F] Other Tasks of the FDPIC

In addition to tasks described above, the FDPIC has numerous other responsibilities. For example, the FDPIC:

- Maintains a register of the processing activities of the federal bodies (Article 56);
- Prepares informative reports for the Federal Assembly and the public (Article 57);
- Informs, trains, and advises the federal bodies and private persons on matters of data protection (Article 58 (1)(a));
- Informs persons on how they can exercise their rights (Article 58(1)(d); or
- Draws up working tools as a recommendation of good practices for controllers, processors, and data subjects (Article 58(1)(g).

[G] Administrative Assistance to Other Authorities

Article 54 of the FADP 2020 sets forth the rules for cooperation between the federal and cantonal data protection authorities, while Article 55 sets forth the conditions and rules for cooperation of the FDPIC with foreign data protection authorities.

Footnotes

105 FDPIC website available in English at https://www.edoeb.admin.ch/edoeb/en/home.html. It is also available in German, French and Italian.

106 FADP 2020, Article 4(2).

107 FADP 2020, Article 44(1).

108 FADP 2020, Articles 43 and 45.

109 FADP 2020, Article 46 and 47. Nevertheless, the Federal Assembly may authorize the Commissioner to engage in an accessory activity, provided that the performance of the function and the independence and reputation of the FDPIC are not affected. The decision is published (FADP 2020, Article 47(2)).

110 FADP 2020, Articles 49, 51, 56, 57 and 58.

111 Professional secrecy remains reserved pursuant to Article 50(2) of the FADP 2020.

Global Privacy and Security Law - Gilbert, § SWI.16, Switzerland,DATA PROTECTION LAW—PRIVATE RIGHT OF ACTION; LEGAL CLAIMS BY DATA SUBJECTS

Francoise Gilbert, Global Privacy and Security Law § SWI.16 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

[A] Correction of Incorrect Data

Article 32(1) of FADP 2020 grants data subjects the right to request that personal data be corrected, with exceptions. Correction is not required if there is a statutory regulation prohibiting the correction or is the personal is being processed for archiving purposes in the public interest.

[B] Actions Relating to the Protection of Personality Rights

Article 32 of the FADP 2020, which refers to Articles 28, 28a and 28g–28j of the Swiss Civil Code, allows data subjects to institute civil actions against private data processors on the grounds of illicit processing in a limited number of circumstances. In this context, Article 32(2) provides that claimants may assert the following claims:

- The prohibition of a specific processing of personal data;
- The prohibition of a specific communication of personal data to third parties;
- The deletion or destruction of personal data.

If the accuracy or inaccuracy of personal data cannot be established, the applicant may also request that the data be marked as disputed.

The plaintiff may also demand that the blocking, deletion, correction, or dispute notation ordered in the judgment, or the entire judgment, be notified to third parties or published.

[C] Actions Relating to the Right of Access

A judicial claim may also be asserted to enforce the right of access pursuant to Article 25 of the FADP 2020.

[D] Actions Relating to Unauthorized Data Processing

If the data subject has suffered harm as a result of the unauthorized data processing, he may claim compensation and therefore, in the event that his personal rights have been substantially infringed, may claim payment of a sum in redress.

[E] Actions Related to Data Processing by Federal Bodies

In connection with data processing by federal bodies, data subjects have comparable rights and ability to make claims based on the administrative procedure. If a federal body does not want to meet the claim of a data subject, it will issue a decision on this matter, which can then be contested according to the rules of the administrative proceeding, ultimately before the Federal Administrative Court and the Swiss Federal Supreme Court.

Global Privacy and Security Law - Gilbert, § SWI.17, Switzerland,DATA PROTECTION LAW—CRIMINAL PROVISIONS

Francoise Gilbert, Global Privacy and Security Law § SWI.17 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

[A] Breach of Obligations to Provide Access and Information or to Cooperate; Violation of Duty of Diligence

In addition to the FDPIC enforcement measures, the FADP 2020 has strengthened the criminal provisions for the protection of personal data. The following violations are now punishable by fines of up to CHF 250,000:

- Intentional failure to comply with the obligation to provide access or information; [112]
- Provision of false information or intentional refusal to cooperate with the FDPIC or to provide information during an investigation; [113]
- Failure to exercise due diligence by: (i) transferring personal data abroad; or (ii) entrusting the processing of personal data to a processor; (iii) or not complying with the minimum data security requirements, in violation of the applicable provisions of the FADP 2020. [114]

[B] Breach of Professional Confidentiality

Further, any person who, in exercising his/her occupation, acquires knowledge of secret sensitive data or personality profiles and discloses such data without authorization is also punishable by fines up to CHF 250,000.

[C] Disregard of Decisions

Pursuant Article 63 of the FADP 2020, the same penalty could be applied on private persons who intentionally fail to comply with a decision of the FDPIC or an appeals authority, served on them under threat of this penalty.

[D] Violations Committed with Corporate Entities

In principle, only natural persons are concerned by the above-mentioned criminal provisions, but Article 64 allows a legal person to be convicted when the fine does not exceed CHF 50,000 and the investigation would require disproportionate measures to identify the perpetrator.

Footnotes

112 FADP 2020, Article 60(1).

113 FADP 2020, Article 60(2).

114 FADP 2020, Article 61.

Global Privacy and Security Law - Gilbert, § SWI.18, Switzerland,DATA PROTECTION LAW—PROCESSING BY FEDERAL BODIES

Francoise Gilbert, Global Privacy and Security Law § SWI.18 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

Processing by federal bodies is subject, in part, to different rules, which are primarily set forth in Articles 33 to 42 of the FADP 2020.

The main differences are:

- A violation cannot generally be justified by the consent of the data subject or an overriding interest. Articles 30 to 32 of the FADP 2020 only apply to private data controllers or processors.
- Federal bodies may process personal data only if there is a statutory basis for doing so, as detailed in Article 34 of the FADP 2020.
- Personal data must be offered to the Federal Archives before being deleted, as set forth in Article 38 of the FADP 2020;
- Federal bodies enjoy less stringent obligations with regard to the disclosure of personal data (Article 37 of the FADP 2020) and processing for research, planning, and statistics (Article 39 of the FADP 2020).

Global Privacy and Security Law - Gilbert, § SWI.19, Switzerland,COMMERCIAL COMMUNICATIONS

Francoise Gilbert, Global Privacy and Security Law § SWI.19 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

[A] Federal Act on Unfair Competition

The transmission of electronic advertising messages without the prior consent of the recipient, without an indication of the correct sender and/or without an indication of a straightforward and free means of rejecting further advertising messages, constitutes an infringement of the Federal Act on Unfair Competition (UCA). [115] The prohibition covers all telecommunications resources, such as e-mail, SMS, telephone, fax, etc. Infringement of the prohibition on spam may have consequences under civil law (application for an injunction, compensation) and criminal law (imprisonment for up to three years or a fine of up to CHF 540,000).

The transmission of advertising messages without the customer's prior consent is permissible only if the customer's data were collected in connection with the sale of goods or other services, if it mentions the possibility of rejecting future advertising communications, and if the advertising relates to similar goods or services.

[B] Telecommunications Act

Telecommunications providers are obligated, pursuant to Article 45a of the Telecommunications Act (TCA), to combat unfair mass advertising. Under the implementing provisions of the TCA, they must protect their customers against the receipt of unfair mass advertising to the extent that the current state of technological development permits. To this end, they are entitled to suppress spam messages and, if they establish that one of their customers is sending spam messages, they must immediately block the dissemination of further spam. They may remove the contravening customers concerned from the network for this purpose. Furthermore, every provider must set up a reporting center to receive communications about spam messages that originate in or are forwarded via the provider's network.

Telecommunications providers are also obligated to provide their customers who show probable cause that they are receiving spam with the information necessary to identify the sender insofar as it is available.

Footnotes

115 Federal Act on Unfair Competition, Article 3(1)(o).

Global Privacy and Security Law - Gilbert, § SWI.20, Switzerland,ELECTRONIC COMMUNICATIONS

Francoise Gilbert, Global Privacy and Security Law § SWI.20 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

[A] Confidentiality of Telecommunications under the Telecommunications Act

Under Article 43 of the TCA, all telecommunications providers and their employees are prohibited from giving details of the telecommunications traffic of subscribers or from giving third parties an opportunity to pass on such details. Infringement of this provision is punishable by a term of imprisonment of up to three years or a fine of up to CHF 540,000. Anyone who receives non-public information not intended for the recipient via a telecommunications system and makes unauthorized use of such non-public information, or discloses it to third parties, may be subject to prosecution and may be punished by a fine of up to CHF 540,000 and/or a term of imprisonment of up to one year. [116]

[B] Monitoring of Postal and Telecommunications Traffic

Monitoring of telecommunications traffic in connection with criminal investigations, international legal assistance in criminal matters, searching for missing persons and tracing persons who have been sentenced to imprisonment or against whom measures involving deprivation of liberty have been enforced, is governed by the Federal Act on the Surveillance of Post and Telecommunications (SPTA) and the associated Implementing Ordinance (SPTO). In the context of criminal investigations, monitoring is permissible only if there is a strong suspicion of a criminal act and if prosecution of one of the serious criminal acts listed in the Act is involved. An exception exists in relation to the obligation of Internet service providers to supply information identifying the perpetrator in the case of criminal acts carried out on the Internet. In this case, any criminal act suffices, and a particularly serious criminal act is not necessary.

Pursuant to its Articles 269 *et seq.,* the Swiss Criminal Procedure Code provides a legal framework for the surveillance of postal and telecommunications in the context of criminal investigations. Such a monitoring could be ordered by the public prosecutor for certain serious offences and only if there is a strong suspicion that such an offence has been committed and if investigative activities carried out so far have been unsuccessful or the enquiries would otherwise have no prospect of success or be made unreasonably complicated. An authorization

of the court of compulsory measures is necessary. The Code not only allows the public prosecutor in certain cases to order the use of special technical devices for the surveillance of telecommunications (e.g., IMSI catcher), but also the use of special software to do so.

Article 269ter of the Swiss Criminal Procedure Code allows under certain conditions the public prosecutor to order the introduction of special software into a data processing system in order to intercept and recover the content of communications and telecommunications metadata in unencrypted form. According to Article 269quater, the only special software that may be used in the context of such monitoring is that which records the surveillance unalterably and without interruption. The record will form part of the case files.

Article 273 sets out the legal framework and conditions for the seizure of secondary telecommunications data by the public prosecutor.

[C] Interception or Recording of Telephone Conversations

The interception or recording of telephone conversations between third parties, or the recording thereof by one of the parties to the conversation, is punishable by a term of imprisonment of up to one year (recording by one of the parties) or up to three years (interception or recording by a third party), or a fine of a maximum of CHF 540,000, except in cases where all those participating in the conversation in question had given their consent to such interception or recording. Exemption from prosecution is provided if calls are recorded by emergency, rescue, or security services and if enterprises record calls from customers relating to orders, contracts, bookings, and similar commercial transactions.

Footnotes

116 Telecommunications Act, Article 50.

Global Privacy and Security Law - Gilbert, § SWI.21, Switzerland,USE OF TRACKING TECHNOLOGIES

Francoise Gilbert, Global Privacy and Security Law § SWI.21 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

Article 45c of the TCA requires that users be informed whether data is processed on users' devices by means of transmission by telecommunications techniques, unless the processing of data is necessary for providing and billing telecommunications services. "Processing" means storing, accessing, or any other operation with data. Although not expressly mentioned in Article 45c of the TCA, its scope is not limited to personal data within the meaning of the FADP. Techniques falling under this provision are cookies, web-bugs (web beacons, tracking bugs, etc.), and other "hidden identifiers," but only if the data processed by using these techniques relate to identified or identifiable persons, which is not necessarily the case.

There is no specific requirement concerning the form of the user information. It may therefore be contained in disclaimers, data protection policies, terms of use, general terms or conditions, or other texts published on a website using cookies, provided these texts may be accessed in a reasonable manner by the users, by using a link placed on the website.

The information must contain a general description of the purposes and the functioning of the technique used and of how the user may refuse cookies (a generic description of the possibility to refuse cookies by appropriate settings in the user's browser).

If it is not possible to use a website or certain of its functionalities without accepting cookies, the user must also be informed so that the user knows that he or she may not, or not properly, use the website as a consequence of his or her refusal of cookies.

Global Privacy and Security Law - Gilbert, § SWI.22, Switzerland,OTHER LAWS PROTECTING PERSONAL DATA

Francoise Gilbert, Global Privacy and Security Law § SWI.22 (First Edition, Supp. #40 2009)
First Edition, Supp. #40

Last Update: 1/2023

In addition to the laws of the Federal State and those of the Cantons, provisions on data protection are also found in numerous other statutes. In federal law, for example, the Social Security Law regulates the transfer of personal data by the authorities mandated to fulfill social security responsibilities. In cantonal law, for example, numerous cantons stipulate specific provisions with respect to data protection in the health system.
