English is not an official language of the Swiss Confederation. This translation is provided for information purposes only and has no legal force.

Ordinance on Data Protection

(Data Protection Ordinance, DPO)

of 31 August 2022 (Status as of 1 December 2025)

The Swiss Federal Council,

on the basis of Articles 8 paragraph 3, 10 paragraph 4, 12 paragraph 5, 16 paragraph 3, 25 paragraph 6, 28 paragraph 3, 33, 59 paragraphs 2 and 3 of the Data Protection Act of 25 September 2020[1] (FADP),

ordains:

Chapter 1 General Provisions

Section 1 Data Security

Art. 1 Principles

[1] In order to guarantee an adequate level of data security, the controller and the processor must determine the extent to which personal data requires to be protected and adopt the technical and organisational measures that are appropriate to the risk.

[2] The extent to which personal data requires to be protected shall be assessed according to the following criteria:

a. the type of the data being processed;

b. the purpose, nature, extent and circumstances of the processing.

[3] The risk for the personality or fundamental rights of the data subject shall be assessed according to the following criteria:

a. the causes of the risk;

b. the main threats;

c. measures taken or planned to reduce the risk;

d. the probability and seriousness of a breach of data security despite the measures taken or planned.

[4] When determining the technical and organisational measures, the following criteria shall also be considered:

a. the state of the art;

AS **2022** 568

1 SR **235.1**

b. the implementation costs.

5 The extent to which personal data requires to be protected, the risk and the technical and organisational measures shall be reviewed throughout the period of processing. The measures shall be adjusted if necessary.

Art. 2 Goals

The controller and the processor must take technical and organisational measures in order to ensure, depending on the level of protection required, that the data being processed:

a. are only accessible to authorised persons (confidentiality);

b. are available when they are required (availability);

c. are not altered without authorisation or unintentionally (integrity);

d. are processed in a traceable manner (traceability).

Art. 3 Technical and organisational measures

1 In order to guarantee confidentiality, the controller and the processor must take appropriate measures to ensure that:

a. authorised persons only have access to those personal data that they require to fulfil their tasks (data access control);

b. only authorised persons have access to the premises and facilities in which personal data are processed (premises and facilities access control);

c. unauthorised persons are unable to use automated data processing systems by means of data transmission devices (user control).

2 In order to guarantee availability and integrity, the controller and the processor must take appropriate measures to ensure that:

a. unauthorised persons are unable to read, copy, alter, move, delete or destroy data carriers (data carrier control);

b. unauthorised persons are unable to save, read, alter, delete or destroy stored personal data (storage control);

c. unauthorised persons are unable to read, copy, alter, delete or destroy personal data in the event of the disclosure of personal data or when data carriers are being transported (transport control);

d. the availability of personal data and access to them can be rapidly restored in the event of a physical or technical incident (restoration);

e. all functions of the automated data processing system are available (availability), malfunctions are reported (reliability) and stored personal data cannot be damaged by system malfunctions (data integrity);

f. operating systems and application software always meet the latest security standards and known critical vulnerabilities are resolved (system security).

[3] In order to guarantee traceability, the controller and the processor must take appropriate measures to ensure that:

a. it can be verified what personal data were entered or altered in the automated data processing system at what time and by which person (entry control);

b. it can be verified to whom personal data are disclosed with the aid of data transmission devices (disclosure control);

c. breaches of data security are recognised rapidly (recognition) and measures are taken to mitigate or eliminate the consequences (elimination).

Art. 4 Logging

[1] If a large volume of sensitive personal data is processed by automated means or if high-risk profiling is carried out and if preventive measures are unable to guarantee data protection, the private controller and its private processor must as a minimum / log the storage, alteration, disclosure, deletion and destruction of the data and any access to the data. A log file must in particular be kept if otherwise it would not be possible to establish whether the data has been processed for the purposes for which it was collected or disclosed.[2]

[2] The responsible federal body and its processor shall when carrying out automated processing of sensitive personal data, profiling and automated processing that falls within the scope of Directive (EU) 2016/680[3], log as a minimum the storage, alteration, disclosure, deletion and destruction of the data, as well as any access to the data. For other forms of automated data processing, they shall assess in advance the risk to the fundamental rights of the data subjects. On this basis, and taking account of the state of the art and the costs of implementation, they shall determine whether and to what extent they log the aforementioned forms of processing. When assessing the risk, they shall take particular account of the nature of the data processed and the purpose, nature, scope and circumstances of the processing.[4]

[2bis] The assessment of the need for logging referred to in paragraph 2 shall be recorded in writing. The results and content of the assessment shall be communicated to the Federal Data Protection and Information Commissioner (FDPIC) on request.[5]

[3] In the case of personal data that are generally accessible, logs shall in the case of paragraphs 1 and 2 first sentence as a minimum be kept of the storage, alteration, deletion and destruction of the data.[6]

2 Amended by No I of the O of 29 Oct. 2025, in force since 1 Dec. 2025 (AS **2025** 694).
3 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, last amended by OJ. L 119 of 4.5.2016, p. 89.
4 Amended by No I of the O of 29 Oct. 2025, in force since 1 Dec. 2025 (AS **2025** 694).
5 Inserted by No I of the O of 29 Oct. 2025, in force since 1 Dec. 2025 (AS **2025** 694).
6 Amended by No I of the O of 29 Oct. 2025, in force since 1 Dec. 2025 (AS **2025** 694).

4 The log file must provide information about the identity of the person that carried out the processing, the form, date and time of processing, and, if applicable, the identity of the recipient of the data.

5 The log files must be retained for at least one year and kept separate from the system in which the personal data are processed. They may only be made accessible to the bodies and persons that are required to review the application of the data protection regulations or to safeguard or restore the confidentiality, integrity, availability and traceability of the data, and may only be used for this purpose.

Art. 5 Processing regulations for private persons

1 The private controller and its private processor must issue regulations on automated processing if they:

a. process a large volume of sensitive personal data; or

b. carry out high-risk profiling.

2 The regulations must in particular include details of the internal organisational structure, data processing and control procedures and the measures that guarantee data security.

3 The private controller and its private processor must update the regulations regularly. If a data protection officer has been appointed, the regulations must be made available to the officer.

Art. 6 Processing regulations for federal bodies

1 The responsible federal body and its processor must issue processing regulations for automated processing if they:

a. process sensitive personal data;

b. carry out profiling;

c. process personal data in accordance with Article 34 paragraph 2 letter c FADP;

d. allow cantons, foreign authorities, international organisations or private persons access to personal data;

e. link data collections with each other; or

f. operate an information system or manage data collections with other federal authorities.

2 The regulations must in particular include details of the internal organisational structure, data processing and control procedures, and the measures that guarantee data security.

3 The responsible federal body and its processor must update the regulations regularly and make them available to the data protection officer.

Section 2 Processing by Processors

Art. 7

1 The prior approval from the controller that allows the processor to assign the data processing to a third party may be specific or general in its scope.

2 In the case of general approval, the processor shall inform the controller of any plan to engage additional or replace existing third parties. The controller may object to such changes.

Section 3 Disclosure of Personal Data Abroad

Art. 8 Assessing the adequacy of the data protection offered by a State, territory, specified sector in a State, or international body

1 The States, territories, specified sectors in a State and international bodies that guarantee an adequate level of data protection are listed in Annex 1.

2 When assessing whether a State, a territory, a specified sector in a State or an international body guarantees an adequate level of data protection, the following criteria in particular shall be considered:

a. the international obligations of the State or international body, in particular in relation to data protection;

b. whether it respects the rule of law and human rights;

c. the legislation applicable, in particular to data protection, its implementation and the relevant case law;

d. that data subjects' rights and redress are effectively guaranteed;

e. the effective functioning of one or more independent authorities in the State concerned that are responsible for data protection or to which an international body is accountable and that have sufficient powers and responsibilities.

3 The FDPIC shall be consulted in the course of each assessment. The assessments of international bodies or foreign authorities responsible for data protection may be taken into account.[7]

4 The adequacy of the data protection shall be reassessed periodically.

5 The assessments shall be made public.

6 If the assessment under paragraph 4 or other information show that an adequate level of data protection is no longer guaranteed, Annex 1 shall be amended; this shall have no effect on disclosures of data already carried out.

7 Amended by No I of the O of 29 Oct. 2025, in force since 1 Dec. 2025 (AS **2025** 694).

Art. 9 Data protection clauses and specific guarantees

[1] The data protection clauses in an agreement under Article 16 paragraph 2 letter b FADP and the specific guarantees under Article 16 paragraph 2 letter c FADP must include at least the following points:

a. the requirement to apply the principles of legality, good faith, proportionality, transparency, purpose limitation and accuracy;

b. the categories of personal data disclosed and of data subjects;

c. the manner and purpose of the disclosure of personal data;

d. if applicable, the names of the countries or international organisations, in which personal data is to be disclosed and the requirements for disclosure;

e. the requirements for safeguarding, deleting and destroying personal data;

f. the recipients or the categories of recipients;

g. the measures to guarantee data security;

h. the requirement to report breaches of data security;

i. if the recipients are controllers: the requirement to inform the data subjects about the processing;

j. the rights of data subjects, and in particular:
   1. the right of access and the right to the data portability,
   2. the right to object to the disclosure of personal data,
   3. the right to the correction, deletion or destruction of their data,
   4. the right to request an independent authority for judicial protection.

[2] The controller and, in the case of data protection clauses in an agreement, the processor must take appropriate measures to ensure that the recipient complies with these clauses or the specific guarantees.

[3] If the FDPIC is informed about the data protection clauses in an agreement or the specific guarantees, the duty to provide information is deemed fulfilled for all further disclosures that:

a. are made in accordance with the same data protection clauses or guarantees, provided the categories of recipients, purpose of processing and data categories essentially remain unchanged; or

b. take place within the same legal entity or company or between company that belong to the same group of companies.

Art. 10 **S**tandard data protection clauses

[1] If the controller or the processor discloses personal data abroad based on standard data protection clauses in accordance with Article 16 paragraph 2 letter d FADP, it shall take appropriate measures to ensure that the recipient complies therewith.

2 The FDPIC shall publish a list of standard data protection clauses that it has approved, issued or recognised. It shall give notice of the result of its assessment of standard data protection clauses that it has been submitted within 90 days.

Art. 11 Binding corporate rules

1 Binding corporate rules in accordance with Article 16 paragraph 2 letter e FADP apply to all undertakings that belong to the same group of undertakings.

2 They shall include as a minimum the points mentioned in Article 9 paragraph 1 as well as the following information:

a. details of the organisational structure and the contact details for the group of undertakings and its members;

b. details of the measures taken within the group of undertakings to comply with the binding corporate rules.

3 The FDPIC shall give notice of the result of its assessment of the binding corporate rules that it has been submitted within 90 days.

Art. 12 Code of conduct and certification

1 Personal data may be disclosed abroad if a code of conduct or certification guarantees an appropriate level of data protection.

2 The code of conduct must be submitted beforehand to the FDPIC for approval.

3 The code of conduct or certification must be combined with a binding and enforceable obligation for the controller or the processor in the third State to apply the measures contained therein.

Chapter 2 Obligations of the Controller

Art. 13 Modalities of the duty to provide information

The controller must provide the data subject with information on the collection of personal data in a precise, transparent, comprehensible and easily accessible form.

Art. 14 Retention of the data protection impact assessment

The controller must retain the data protection impact assessment after concluding the data processing for a minimum of two years.

Art. 15 Report of breaches of data security

1 The report to the FDPIC of a breach of data security must include the following information:

a. the form of breach;

b. the time and duration, if possible;

c. the categories and approximate amount of personal data concerned, if possible;

d. the categories and the approximate number of data subjects, if possible;

e. the consequences, including any risks, for the data subjects;

f. the measures that have been taken or are planned in order to remedy the breach and mitigate the consequences, including any risks;

g. the name and the contact details of a contact person.

2 If the controller is unable to report all the details at one time, it shall supply the missing details as quickly as possible.

3 If the controller is required to inform the data subject, it shall provide the data subject with the details specified in paragraph 1 letters a and e–g in simple and comprehensible language.

4 The controller must document the breaches. The documentation must contain a summary of the circumstances of the incidents, their effects and the measures taken. It shall be retained from the time of the report under paragraph 1 for a minimum of two years.

Chapter 3 Rights of the Data Subject

Section 1 Right of Access

Art. 16 Modalities

1 Any person who requests information from the controller as to whether personal data relating to him or her are being processed must do so in writing. If the controller agrees, the request may also be made verbally.

2 The information shall be provided in writing or in the form in which the data is available. By agreement with the controller, the data subject may inspect his or her data on site. The information may be provided verbally if the data subject agrees.

3 Information may be requested and provided electronically.

4 The information must be given to the data subject in a comprehensible form.

5 The controller must take appropriate measures to identify the data subject. The data subject is obliged to cooperate in the identification process.

Art. 17 Responsibility

1 Where two or more controllers are processing personal data jointly, the data subject may exercise his or her right of access in relation to any one of them.

2 If the request relates to data that is being processed by one processor, the processor shall assist the controller in providing the information where it does not answer the request on behalf of the controller.

Art. 18 Deadline

[1] The information must be provided within 30 days of receipt of the request.

[2] If it is not possible to provide the information within 30 days, the controller must notify the data subject of this and of how long it will take to provide the information.

[3] If the controller decides to refuse, restrict or defer the right of access, it must notify the data subject of this within the same deadline.

Art. 19 Exception to the requirement not to charge fees

[1] If providing the information involves a disproportionate cost, the controller may require the data subject to contribute to the costs in an appropriate manner.

[2] The contribution may not exceed 300 francs.

[3] The controller must notify the data subject of the amount of the contribution before providing the information. If the data subject does not confirm the request within ten days, the request is deemed to have been withdrawn with no costs incurred. The period referred to in Article 18 paragraph 1 shall begin on expiry of the ten-day reflection period.

Section 2 Right to Data Portability

Art. 20 Scope of the right

[1] Personal data that the data subject has disclosed to the controller are:

a. data that the data subject has knowingly and voluntarily made available;

b. data that the controller has obtained relating to the data subject and his or her behaviour while the data subject was using a service or device.

[2] Personal data that the controller has itself generated from its own evaluation of the personal data provided or observed are not deemed to be personal data that the data subject has disclosed to the controller.

Art. 21 Technical requirements for implementation

[1] A conventional electronic format is any format that allows the personal data to be transmitted and reused by the data subject or another controller at a proportionate cost.

[2] The right to data portability does not create any requirement for the data controller to adopt or maintain technically compatible data processing systems.

[3] The cost of transferring personal data to another controller is disproportionate if the transfer is technically impossible.

Art. 22 Deadline, modalities and responsibility

Articles 16 paragraphs 1 and 5 and 17–19 apply mutatis mutandis to the right to data portability.

Chapter 4 Special Provisions on Data Processing by Private Persons

Art. 23 Data protection officer

The controller must grant the data protection officer:

a. access to the required resources;

b. access to all information, documents, records of processing activities and personal data that the officer requires to fulfil his or her tasks;

c. the right to notify the highest management or governing body in important cases.

Art. 24 Exemption from the obligation to keep a record of processing activities

Undertakings and other private organisations employing fewer than 250 employees on 1 January of any year and natural persons are exempt from the obligation to keep a record of processing activities unless any one of the following requirements is met:

a. a large volume of sensitive personal data is being processed;

b. high-risk profiling is being carried out.

Chapter 5 Special Provisions on Data Processing by Federal Bodies

Section 1 Data Protection Officer

Art. 25 Appointment

Every federal body shall appoint a data protection officer. Two or more federal authorities may appoint a joint data protection officer.

Art. 26 Requirements and tasks

[1] The data protection officer must meet the following requirements:

a. He or she has the required specialist knowledge.

b. He or she carries out his or her work in relation to the federal body in a professionally independent manner and is not bound by instructions.

[2] He or she must carry out the following tasks:

a. He or she participates in applying the data protection regulations, in particular in that he or she:

1. examines the processing of personal data and recommends corrective measures if a breach of the data protection regulations is established;

2. advises the controller on preparing the data protection impact assessment and reviews its implementation.

b. He or she serves as a contact point for data subjects.

c. He or she trains and advises employees of the federal body on data protection matters.

Art. 27 Obligations of the federal body

[1] The federal body has the following obligations in relation to the data protection officer:

a. It shall grant him or her access to all information, documents, records of processing activities and personal data that he or she requires to fulfil his or her tasks.

b. It shall ensure that he or she is notified of any breach of data security.

[2] It shall publish contact details for the data protection officer online and notify the FDPIC of these details.

Art. 28 Contact point for the FDPIC

The data protection officer serves as the FDPIC's contact point for any questions in connection with the processing of personal data by the federal body concerned.

Section 2 Duties to Provide Information

Art. 29 Duty to provide information in the event of the disclosure of personal data

The federal body shall inform the recipient about the up-to-dateness, reliability and completeness of the personal data that it has disclosed, unless this information is evident from the data themselves or from the circumstances.

Art. 30 Duty to provide information in the event of the systematic collection of personal data

If the data subject is not under any obligation to provide information, the responsible federal body shall inform him or her of this fact in relation to any systematic collection of personal data.

Section 3
Notifying the FDPIC of Projects for the Automated Processing of Personal Data

Art. 31

1 The responsible federal body shall notify the FDPIC of any planned automated processing activities at the time that the decision is taken to develop or approve the project.

2 Notification must include the details in Article 12 paragraph 2 letters a–d FADP and the anticipated date on which the processing activities will begin.

3 The FDPIC shall record the notification in the register of processing activities.

4 The responsible federal body shall update the notification on transition to productive operations or termination of the project.

Section 4 Pilot Projects

Art. 32 Mandatory nature of the pilot trial

A pilot trial is mandatory if any one of the following conditions is satisfied:

a. Fulfilling a task requires technical innovations, the effects of which must first be evaluated.

b. Fulfilling a task requires significant organisational or technical measures, the effectiveness of which must first be tested, in particular in the case of the cooperation between federal and cantonal authorities.

c. Fulfilling a task requires personal data to be made accessible in the online search process.

Art. 33 Procedure for authorising the pilot trial

1 Before consulting the administrative units with an interest, the federal body responsible for the pilot trial shall explain how it planned to comply with the requirements under Article 35 FADP, and invite the FDPIC to provide its opinion.

2 The FDPIC shall provide its opinion on whether the authorisation requirements under Article 35 FADP are met. The federal body shall provide it with all the documents required to do this, and in particular:

a. a general description of the pilot trial;

b. a report that demonstrates that fulfilling the statutory tasks requires processing under Article 34 paragraph 2 FADP and that a test phase before the act formally comes into force is essential;

c. a description of the internal organisational structure and the data processing and control procedures;

d. a description of the security and data protection measures;

e. the draft of an ordinance that regulates the details of the processing, or the plan for an ordinance;

f. the plans for the various phases of the pilot trial.

3 The FDPIC may request further documents and conduct additional enquiries.

4 The federal body shall inform the FDPIC of any significant change that affects compliance the requirements of Article 35 FADP. The FDPIC shall again provide its opinion if required.

5 The FDPIC's opinion shall be included with the application to the Federal Council.

6 Automated data processing shall be regulated in an ordinance.

Art. 34 Evaluation report

1 The competent federal body shall submit the draft of the evaluation report for the Federal Council to the FDPIC for the FDPIC to provide an opinion.

2 The competent federal body shall submit the evaluation report to the Federal Council with the FDPIC's opinion.

Section 5
Data Processing for Purposes not related to Specific Persons

Art. 35

If personal data are processed for purposes not related to specific persons, in particular research, planning and statistics, but at the same time are processed for a different purpose, the exceptions under Article 39 paragraph 2 FADP only apply to the processing for purposes not related to specific persons.

Chapter 6 Federal Data Protection and Information Commissioner

Art. 36 Seat and permanent secretariat

1 The seat of the FDPIC is in Bern.

2 The federal legislation on personnel governs the employment contracts of the employees of the FDPIC's permanent secretariat. The employees shall be insured with the Federal Pension Fund.

Art. 37 Method of communication

1 The FDPIC shall communicate with the Federal Council via the Federal Chancellor. The Federal Chancellor shall pass on the FCPIC's proposals, opinions and reports unedited the Federal Council.

2 The FDPIC shall submit reports to the Federal Assembly via the Parliamentary Services.

Art. 37*a*[8] Conclusion and amendment of declarations of intent

The FDPIC shall report annually to the Federal Council on the declarations of intent that it has concluded and amended regarding its cooperation with foreign data protection authorities.

Art. 38 Notice of decisions, guidelines and projects

1 The departments and the Federal Chancellery shall notify the FDPIC of their decisions in anonymised form and of their guidelines relating to data protection.

2 The federal authorities shall submit all legislative drafts to the FDPIC that relate to the processing of personal data, data protection and access to official documents.

Art. 39 Processing personal data

The FDPIC may process personal data, including sensitive personal data, for the following purposes in particular:

a. in order to carry out its supervisory activities;

b. in order to carry out its advisory activities;

c. in order to cooperate with federal, cantonal and foreign authorities;

d. in order to fulfil tasks in terms of the criminal provisions in the FADP;

e. in order to conduct mediation proceedings and to issue recommendations under the Freedom of Information Act of 17 December 2004[9] (FoIA);

f. in order to conduct evaluations under the FoIA;

g. in order to conduct proceedings for access to official documents under the FoIA;

h. in order to provide information to the parliamentary supervisory authorities;

i. in order to provide information to the public;

j. in order to carry out its training activities.

Art. 40 Self-regulation

The FDPIC shall issue processing regulations for all automated processing; Article 6 paragraph 1 does not apply.

8 Inserted by No I of the O of 29 Oct. 2025, in force since 1 Dec. 2025 (AS **2025** 694).
9 SR **152.3**

Art. 41[10] Cooperation with the National Cybersecurity Centre

1 …[11]

2 The FDPIC shall invite the NCSC to comment before it orders the federal body to take measures under Article 8 FADP.

Art. 42 Register of processing activities by federal authorities

1 The register of the processing activities by federal authorities shall contain the details provided by the federal authorities in accordance with Article 12 paragraph 2 FADP and Article 31 paragraph 2 this Ordinance.

2 It shall be published online. The register entries on planned automated processing activities under Article 31 shall not be published.

Art. 43 Code of conduct

If a code of conduct is submitted to the FDPIC, the FDPIC shall confirm in its opinion whether the code of conduct meets the requirements of Article 22 paragraph 5 letters a and b FADP.

Art. 44 Fees

1 The fees charged by the FDPIC shall be calculated on the basis of the time taken.

2 An hourly rate of 150 to 250 francs applies, depending on the seniority of the members of staff carrying out the work.

3 In the case of services that are exceptionally extensive, complex or urgent, a surcharge of up to 50 per cent of the fee under paragraph 2 may be added.

4 If the service provided by the FDPIC can be commercially exploited by the person liable to pay the fee, a surcharge of up to 100 per cent of the fee under paragraph 2 may be added.

5 The General Fees Ordinance of 8 September 2004[12] also applies.

Chapter 7 Final Provisions

Art. 45 Repeal and amendment of other legislation

The repeal and the amendment of other legislation are regulated in Annex 2.

10 Amended by No II 7 of the O of 22 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 746).
11 Repealed by Annex No 2 of the Cybersecurity Ordinance of 7 March 2025, with effect from 1 April 2025 (AS **2025** 169).
12 SR **172.041.1**

Art. 46 Transitional provisions

[1] In the case of automated processing of personal data that was planned or started before the amendment of 29 October 2025 came into force, the assessment of the need for logging under Article 4 paragraph 2 must be carried out by 31 December 2026. If logging proves to be necessary, it must be implemented by 31 December 2029. The foregoing does not apply to the automated processing of sensitive personal data, profiling and automated data processing that falls within the scope of Directive (EU) 2016/680[13].[14]

[2] Article 8 paragraph 5 does not apply to assessments carried out before this Ordinance comes into force.

[3] Article 31 does not apply to planned automated processing activities in respect of which the decision to develop or approve the project has already been taken when this Ordinance comes into force.

Art. 47 Commencement

This Ordinance comes into force on 1 September 2023.

13 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, last amended by OJ L 119 of 4.5.2016, p. 89.

14 Amended by No I of the O of 29 Oct. 2025, in force since 1 Dec. 2025 (AS **2025** 694).

Annex 1[15]
(Art. 8 para. 1)

States, territories, specified sectors in a State and international bodies that guarantee an adequate level of data protection

1	Germany*	
2	Andorra***	
3	Argentina***	
4	Austria*	
5	Belgium*	
6	Bulgaria***	
7	Canada***	An adequate level of data protection is guaranteed if the Canadian Federal Act on Personal Information Protection and Electronic Documents of 13 April 2000[16] or the act of a Canadian province that largely corresponds to this Federal Act applies to the private sphere. The Federal Act applies to personal data that is collected, processed or disclosed in the course of commercial activities, irrespective of whether it relates to organisations such as associations, partnerships, individuals or trade unions or undertakings regulated by federal law such as facilities, works, undertakings or business activities that fall within the legislative authority of the Canadian Parliament. The provinces of Quebec, British Columbia and Alberta have issued an act that largely corresponds to the Federal Act; the provinces of Ontario, New Brunswick, Newfoundland and Labrador and Nova Scotia have issued an act that largely corresponds to this act in relation to health data. In all Canadian provinces, the Federal Act applies to all personal data that are collected, processed or disclosed by undertakings regulated by federal law, including data on employees of these undertakings. The Federal Act also applies to personal data transferred to another province or another country in the course of commercial activities.
8	Cyprus***	
9	Croatia***	
10	Denmark*	

15 Amended by No I of the O of 14 Aug. 2024, in force since 15 Sep. 2024 (AS **2024** 435).
16 The text of the Canadian Federal Act is available at https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html.

11 Spain*
12 Estonia*
13 Finland*
14 France*
15 Gibraltar***
16 Greece*
17 Guernsey***
18 Hungary*
19 Isle of Man***
20 Faroe Islands***
21 Ireland***
22 Island*
23 Israel***
24 Italy*
25 Jersey***
26 Latvia*
27 Liechtenstein*
28 Lithuania*
29 Luxembourg*
30 Malta*
31 Monaco***
32 Norway*
33 New Zealand***
34 Netherlands*
35 Poland*
36 Portugal*
37 Czech Republic*
38 Romania***
39 United Kingdom **
40 Slovakia*
41 Slovenia*

42	Sweden*	
43	Uruguay***	
44	United States***	For personal data processed by organisations certified under the Principles of the Swiss-US Privacy Framework[17], an adequate level of protection is deemed to be guaranteed based on the safeguards provided by Executive Order 14086 of 7 October 2022[18], the Rule on the United States Attorney General's Data Protection Review Court of 7 October 2022[19] and Intelligence Community Directive 126 (Implementation Procedures for the Signals Intelligence Redress Mechanism under Executive Order 14086) issued by the Office of the Director of National Intelligence on 6 December 2022[20] and the Designation of Switzerland on 7 June 2024[21] as a country covered by the two-layer redress mechanism, including access to the Data Protection Review Court.

* The assessment of the adequacy of data protection includes the disclosure of personal data in accordance with Directive (EU) 2016/680[22].

** The assessment of the adequacy of data protection includes the disclosure of personal data in accordance with an implementing decision of the European Commission in which the adequacy of data protection is established in accordance with Directive (EU) 2016/680.

*** The assessment of the adequacy of data protection does not include the disclosure of personal data in terms of the cooperation provided for under Directive (EU) 2016/680.

17 The principles are available at: www.dataprivacyframework.gov/s/framework-text?tabset-c1491=3.

18 The Executive Order 14086 is available at: www.state.gov/executive-order-14086-policy-and-procedures/.

19 The Rule is available at: www.federalregister.gov/documents/2022/10/14/2022-22234/data-protection-review-court.

20 The Directive is available at: www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.

21 The list is available at: www.justice.gov/opcl/media/1355326/dl?inline.

22 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, last amended by OJ. L 119 of 4.5.2016, p. 89.

Annex 2[23]
(Art. 45)

Repeal and amendment of other legislation

I

The Ordinance to the Federal Data Protection Act of 14 June 1993[24] is repealed.

II

The enactments below are amended as follows:

…[25]

23 Revised by Annex 6 No II 1 of the O of 23 Sept. 2022 on Human Genetic Testing, in force since 1 Sept. 2023 (AS **2022** 585).
24 [AS **1993** 1962; **2000** 1227 Annex No II 7; **2006** 2331 Annex 2 No 3, 4705 No II 24; **2007** 4993; **2008** 189; **2010** 3399]
25 The amendments may be consulted under AS **2022** 568.