Ordinance on Data Protection (Data Protection Ordinance, DPO)

Unofficial English translation done in autumn 2022

The officials versions, in German, French and Italian, will be published on https://www.fedlex.admin.ch/de/, and will be the only legally binding versions.

walderwyss attorneys

Ordinance on Data Protection
(Data Protection Ordinance, DPO)

of 31 August 2022

The Swiss Federal Council,

based on Articles 8(3), 10(4), 12(5), 16(3), 25(6), 28(3), 33, 59(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 ensure adequate data security, the controller and the processor must determine the need for protection of personal data and specify the technical and organisational measures that are appropriate in view of the risk.

[2] The need for protection of personal data is assessed according to the following criteria:
a. the type of data processed;
b. the purpose, nature, extent and circumstances of the processing.

[3] The risk to the personality or fundamental rights of the data subject is assessed according to the following criteria:
a. causes of the risk;
b. main dangers;
c. measures taken or envisaged to reduce the risk;
d. the likelihood and severity of a data security breach despite the measures taken or envisaged.

[4] The following criteria shall also be taken into account when determining the technical and organisational measures:
a. the state of the art;
b. costs of implementation.

[5] The need for protection of personal data, the risk and the technical and organisational measures shall be reviewed over the entire processing period. The measures shall be adapted if necessary.

Art. 2 Objectives

The controller and the processor must take technical and organisational measures to ensure that in accordance with its need for protection the data processed is:
a. only accessible to authorised persons (confidentiality);
b. available when it is needed (availability);
c. not changed by unauthorised persons or not changed unintentionally (integrity);
d. processed in a traceable manner (traceability).

Art. 3 Technical and organisational measures

[1] In order to ensure confidentiality, the controller and the processor must take appropriate measures to guarantee that:
a. access by authorised persons is limited to the personal data that they require to fulfil their tasks (access control);
b. unauthorised persons are denied access to the premises and installations in which personal data is being processed (entrance control);
c. unauthorised persons may not use automated data processing systems by means of devices for data transmission (usage control).

1 SR **235.1**

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

a. unauthorised persons may not read, copy, alter, move, delete or destroy data carriers (data carrier control);

b. unauthorised persons may not store, read, change, delete or destroy personal data in storage (storage control);

c. when disclosing personal data and during the transport of data carriers, unauthorised persons may not read, copy, alter, delete or destroy personal data (transport control);

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

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

f. operating systems and application software are always kept up to date and known critical gaps are closed (system security).

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

a. it can be checked what personal data is entered or altered in the automated data processing system, at what time and by which person (input control);

b. it can be checked to whom personal data has been disclosed by means of devices for data transmission (disclosure control);

c. data security breaches can be quickly detected (detection), and measures can be taken to mitigate or eliminate their impact (elimination).

Art. 4 Records

[1] If sensitive personal data is processed automatically on a broad scale or if high-risk profiling is carried out and the preventive measures cannot guarantee data protection, the private controller and its private processor must at least record the storage, alteration, reading, disclosure, deletion and destruction of the data. The records must be kept in particular if it is otherwise not possible to establish retroactively whether the data was processed for the purposes for which it was collected or disclosed.
[2] During the automated processing of personal data, the federal body responsible and its processor shall at least record the storage, alteration, reading, disclosure, deletion or destruction of the data.
[3] In the case of personal data that is generally accessible to the public, the storage, alteration, deletion and destruction of the data must at least be recorded.
[4] The records must provide information on the identity of the person who carried out the processing, the nature, date and time of the processing and, if applicable, the identity of the recipient of the data.
[5] The records must be kept for at least one year separately from the system in which the personal data is being processed. They must be accessible only to the bodies and persons responsible for monitoring the application of data protection regulations or for maintaining or restoring the confidentiality, integrity, availability and traceability of the data, and may only be used for this purpose.

Art. 5 Processing policy for private persons

[1] The private controller and its private processor must draw up a processing policy for automated processing if they:

a. process sensitive personal data on a broad scale; or

b. carry out high-risk profiling.

[2] The processing policy must in particular contain information on the internal organisation, the data processing and control procedure and the measures taken to ensure data security.

[3] The private controller and its private processor must update the processing policy regularly. If a data protection advisor has been appointed, the processing policy must be made available to such advisor.

Art. 6 Processing policy for federal bodies

[1] The federal body responsible and its processor shall draw up a processing policy for automated processing if they:

a. process sensitive personal data;

b. carry out a profiling;

c. process personal data in accordance with Article 34(2)(c) FADP;

d. make personal data accessible to cantons, foreign authorities, international organisations or private persons;

e. interlink data files; or
f. operate an information system in conjunction with other federal bodies or manage data files.

[2] The processing policy must in particular contain information on the internal organisation, the data processing and control procedure and the measures taken to ensure data security.

[3] The federal body responsible and its processor must update the processing policy regularly and make it available to the data protection advisor.

Section 2 Data Processing by Processors

Art. 7

[1] The prior authorisation of the controller allowing the processor to transfer the data processing to a third party may be of a specific or general nature.

[2] In the case of a general authorisation, the processor shall inform the controller of any intended changes with regard to the involvement or replacement of other third parties. The controller may object to such changes.

Section 3 Cross-Border Disclosure of Personal Data

Art. 8 Assessment of the adequacy of the level of data protection of a State, a territory, a specific sector in a State or an international body

[1] The States, territories, specific sectors in a State and international bodies with an adequate level of data protection are listed in Annex 1.

[2] The assessment of whether a State, territory, specific sector within a State or international body ensures an adequate level of data protection must in particular be based on the following criteria:

a. the international obligations of the State or international body in particular with respect to data protection;
b. the rule of law and respect for human rights;
c. the applicable legislation in particular on data protection and its implementation, and the relevant case law;
d. the effective guarantee of the rights of data subjects and of judicial protection;
e. the effective functioning of one or more independent authorities competent for data protection matters in the State concerned or to which an international body is answerable, and which have sufficient powers and competences.

[3] The Federal Data Protection and Information Commissioner (FDPIC) shall be consulted on each assessment. The assessments of international bodies or foreign authorities responsible for data protection may be taken into account.

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

[5] The assessments shall be published.

[6] If an assessment under paragraph 4 or other information indicates that an adequate level of data protection is no longer ensured, Annex 1 shall be amended. This amendment has no effect on data disclosures made prior thereto.

Art. 9 Data protection provisions and specific safeguards

[1] The data protection provisions of a contract in accordance with Article 16(2)(b) FADP and the specific safeguards in accordance with Article 16(2)(c) FADP must at least contain the following aspects:

a. the application of the principles of lawfulness, good faith, proportionality, transparency, purpose limitation and accuracy;
b. the categories of personal data disclosed as well as the data subjects;
c. the nature and purpose of the disclosure of personal data;
d. where applicable, the names of the States or international bodies to which personal data is disclosed and the requirements for disclosure;
e. the requirements for the retention, deletion and destruction of personal data;
f. the recipients or the categories of recipients;
g. the measures to ensure data security;
h. the duty to report data security breaches;
i. if recipients are controllers: the duty to inform the data subjects of the processing;
j. the rights of the data subjects, in particular:

1. access right and right of data portability,
2. right to object to the disclosure of data,
3. right to correction, deletion or destruction of personal data,
4. right to seek judicial protection from an independent authority.

[2] The controller and, in the case of data protection provisions of a contract, the processor must take appropriate measures to ensure that the recipient complies with these provisions or the specific safeguards.

[3] If the FDPIC has been informed of the data protection provisions of a contract or the specific safeguards, the duty of information shall be deemed to be fulfilled for all further disclosures that:

a. are made subject to the same data protection provisions or safeguards, provided the categories of recipients, the purpose of the processing and the data categories remain essentially unchanged; or
b. take place within the same legal person or company or between legal persons or companies belonging to the same group.

Art. 10 Standard data protection clauses

[1] If the controller or the processor discloses personal data abroad by means of standard data protection clauses in accordance with Article 16(2)(d) FADP, the controller or the processor shall take appropriate measures to ensure that the recipient complies therewith.

[2] The FDPIC has published a list of standard data protection clauses that he has approved, established or recognised. He shall communicate the result of his examination of the standard data protection clauses submitted to him within 90 days.

Art. 11 Binding corporate rules on data protection

[1] Binding corporate rules on data protection in accordance with Article 16(2)(e) FADP apply to all companies belonging to the same group.

[2] They shall at least contain the aspects mentioned in Article 9(1) as well as the following information:

a. the organisation and contact details of the group and its companies;
b. the measures taken within the group to ensure compliance with the binding corporate rules on data protection.

[3] The FDPIC shall communicate the result of his examination of the binding corporate rules on data protection submitted to him within 90 days.

Art. 12 Codes of conduct and certifications

[1] Personal data may be disclosed abroad if an adequate level of data protection is ensured by a code of conduct or certification.

[2] The code of conduct must be submitted to the FDPIC for prior approval.

[3] The code of conduct or certification must be linked to a binding and enforceable obligation on the part of the controller or the processor in the third country to apply the measures contained therein.

Chapter 2 Duties of the Controller

Art. 13 Modalities of the duty of information

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

Art. 14 Retention of data protection impact assessment

The controller must retain the data protection impact assessment for at least two years after termination of the data processing activity.

Art. 15 Notification of data security breaches

[1] The notification of a data security breach to the FDPIC must contain the following information:

a. the nature of the data security breach;

b. as far as possible, the time and duration of the data security breach;
c. as far as possible, the categories and the approximate number of personal data concerned;
d. as far as possible, the categories and the approximate number of data subjects;
e. the impact, including any risks, for the data subjects;
f. what measures have been taken or are envisaged to remedy the defect and mitigate the impact, including any risks;
g. the name and contact details of a contact person.

[2] If the controller is unable to provide all the information at the same time, it shall provide the missing information as soon as possible.

[3] If the controller is obliged to inform the data subjects, the controller shall inform the data subjects in simple and comprehensible language of at least the information referred to in paragraph 1 letters a and e–g.

[4] The controller must document data security breaches. The documentation must contain all facts relating to the incidents, their effects and the measures taken. The documentation must be retained for at least two years from the date of notification according to paragraph 1.

Chapter 3 Rights of the Data Subject

Section 1 Access Right

Art. 16 Modalities

[1] Anyone who requests information from the controller as to whether personal data about him or her is 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. With the agreement of the controller, the data subject may also inspect his or her data in situ. The information may be provided verbally if the data subject agrees.

[3] The information request and the provision of information may be made electronically.

[4] The information must be provided to the data subject in a comprehensible form.

[5] The controller must take reasonable measures to identify the data subject. Data subjects are obliged to cooperate.

Art. 17 Responsibilities

[1] If several controllers jointly process personal data, the data subject may assert his or her access right against each controller.

[2] If the information request relates to data that is being processed by a processor, the processor shall assist the controller in providing the information, unless the processor is responding to the request on behalf of the controller.

Art. 18 Time limits

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

[2] If the information cannot be provided within 30 days, the controller must notify the data subject thereof and of the period within which the information will be provided.

[3] If the controller refuses, restricts or defers the provision of the information, it must notify the data subject thereof within the same period.

Art. 19 Exceptions to the exemption from costs

[1] The controller may request from the data subject the payment of an appropriate share of the costs if the provision of information involves a disproportionate effort.

[2] The share of the costs amounts to a maximum of 300 Swiss Francs.

[3] The controller must inform the data subject of the amount of the share before the information is provided. If the data subject does not confirm the information request within ten days, it shall be deemed to have been withdrawn without incurring any costs. The time limit in accordance with Article 18(1) shall begin to run after the expiry of the ten-day reflection period.

Section 2 Right of Data Portability

Art. 20 Scope of claim

[1] Personal data which the data subject has disclosed to the controller is deemed to be:
a. data that the data subject knowingly and willingly makes available to the controller;
b. data collected by the controller about the data subject and his or her behaviour in the context of the use of a service or device.

[2] Personal data generated by the controller through its own evaluation of the personal data provided or observed shall not be deemed to be personal data which the data subject has disclosed to the controller.

Art. 21 Technical requirements for implementation

[1] Common electronic formats are those that allow the personal data to be transferred with a reasonable effort and to be further used by the data subject or another controller.

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

[3] A disproportionate effort for the transfer of personal data to another controller exists if the transfer is technically not possible.

Art. 22 Time limits, modalities and responsibilities

Articles 16(1) and (5), and 17–19 apply mutatis mutandis to the right of data portability.

Chapter 4 Special Provisions for Data Processing by Private Persons

Art. 23 Data protection advisor

The controller must provide the data protection advisor with:
a. the necessary resources;
b. access to all information, documents, inventories of processing activities and personal data that the data protection advisor requires in order to fulfil his or her duties.
c. the right to inform the highest management or administrative body in important cases.

Art. 24 Exemptions from the duty to keep an inventory of processing activities

Companies and other organisations under private law which employ fewer than 250 members of staff on 1 January of a year, as well as natural persons, are exempt from the duty to keep an inventory of processing activities, unless one of the following conditions is met:
a. Sensitive personal data is being processed on a broad scale.
b. High-risk profiling is carried out.

Chapter 5 Special Provisions for Data Processing by Federal Bodies

Section 1 Data Protection Advisor

Art. 25 Appointment

Each federal body appoints a data protection advisor. Several federal bodies may jointly appoint a data protection advisor.

Art. 26 Requirements and duties

[1] The data protection advisor must meet the following requirements:
a. The data protection advisor has the necessary professional knowledge.
b. The data protection advisor performs his or her function towards the federal body in a professionally independent manner and without being bound by instructions.

[2] The data protection advisor must perform the following duties:

a. The data protection advisor assists in the application of the data protection regulations, in particular by:
   1. auditing the processing of personal data and recommending corrective measures if an infringement of the data protection regulations is detected;
   2. advising the controller on the preparation of the data protection impact assessment and reviewing its implementation.
b. The data protection advisor serves as a contact point for data subjects.
c. The data protection advisor trains and advises the members of staff of the federal body on data protection matters.

Art. 27 Duties of the federal body

[1] The federal body has the following duties towards the data protection advisor:
a. The federal body shall grant the data protection advisor access to all information, documents, inventories of processing activities and personal data that the data protection advisor requires in order to fulfil his or her duties.
b. The federal body shall ensure that the data protection advisor is informed of any data security breaches.

[2] The federal body publishes the contact details of the data protection advisor on the internet and communicates them to the FDPIC.

Art. 28 Contact point of the FDPIC

The data protection advisor serves as a contact point for the FDPIC for questions relating to the processing of personal data by the federal body concerned.

Section 2 Duties of Information

Art. 29 Duty of information when disclosing personal data

The federal body responsible shall notify the recipient of the up-to-dateness, reliability and completeness of the personal data that it discloses, provided this information is not evident from the data itself or from the circumstances.

Art. 30 Duty of information in the case of systematic collection of personal data

Where a federal body collects personal data systematically, the federal body responsible must inform accordingly the data subjects who are not obliged to provide information.

Section 3 Notification to the FDPIC of Projects Involving Automated Processing of Personal Data

Art. 31

[1] The federal body responsible shall notify the FDPIC of the planned automated processing activities at the time of the decision on the development of the project or the project approval.

[2] The notification must include the information specified in Article 12(2)(a-d) FADP and the expected date of commencement of the processing activities.

[3] The FDPIC shall include this notification in its register on processing activities.

[4] The federal body responsible shall update the notification at the time of the transition into productive operation or when the project is discontinued.

Section 4 Pilot Projects

Art. 32 Indispensability of pilot project

A pilot project is indispensable if one of the following conditions is met:
a. The fulfilment of a task requires technical innovations, the effects of which must first be evaluated.
b. The fulfilment of a task requires significant organisational or technical measures, the

effectiveness of which must first be evaluated, in particular in the case of cooperation between federal and cantonal bodies.
c. The fulfilment of a task requires that personal data be accessible in a retrieval procedure.

Art. 33 Procedure for authorisation of pilot project

[1] Before consulting the interested administrative units, the federal body responsible for the pilot project shall communicate as to how it is intended to meet compliance with the requirements of Article 35 FADP, and invite the FDPIC to comment thereon.

[2] The FDPIC shall comment on the issue of whether the authorisation requirements in terms of Article 35 FADP are fulfilled. The federal body shall provide him with all the documents required, and in particular with:

a. a general description of the pilot project;
b. a report that proves that the fulfilment of tasks provided for by law requires a processing in accordance with Article 34(2) FADP and that a test phase before a formal law enters into force is indispensable;
c. a description of the internal organisation as well as the data processing and control procedures;
d. a description of the security and data protection measures;
e. the draft of or the concept for an ordinance that regulates the details of the processing;
f. the planning of the various phases of the pilot project.

[3] The FDPIC may request further documents and carry out additional investigations.

[4] The federal body shall inform the FDPIC of any important modification relating to compliance with the requirements of Article 35 FADP. If required, the FDPIC shall again state his views thereon.

[5] The opinion of the FDPIC must be included in the application to the Federal Council.

[6] Automated data processing is 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 comment.

[2] The competent federal body shall submit the evaluation report with the opinion of the FDPIC to the Federal Council.

Section 5 Data Processing for Research, Planning and Statistics

Art. 35

If personal data is processed for purposes not related to specific persons, in particular research, planning and statistics, and at the same time for another purpose, the exceptions under Article 39(2) FADP are only applicable to processing for the purposes not related to specific persons.

Chapter 6 Federal Data Protection and Information Commissioner

Art. 36 Headquarters and permanent secretariat

[1] The FDPIC's headquarters are located in Bern.

[2] The employment of the members of the FDPIC's permanent secretariat is governed by the Federal Personnel Act. The employees are insured with the Federal Pension Fund within the framework of the Federal Pension Plan.

Art. 37 Communication channel

[1] The FDPIC communicates with the Federal Council via the Federal Chancellor. The Federal Chancellor shall pass on any proposals, opinions and reports from the FDPIC unchanged to the Federal Council.

[2] The FDPIC submits reports to the Federal Assembly via the Parliamentary Services.

Art. 38 Notification of decisions, guidelines and projects

[1] The departments and the Federal Chancellery notify the FDPIC of their data protection decisions as well as their data protection guidelines in anonymised form.

[2] The federal bodies shall submit to the FDPIC all draft legislation that relates to the processing of personal data, data protection or access to official documents.

Art. 39 Processing of personal data

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

a. to carry out his supervisory activities;
b. to carry out his advisory activities;
c. to cooperate with federal, cantonal and foreign authorities;
d. to perform tasks within the framework of the penal provisions under the FADP;
e. to conduct mediation proceedings and to issue recommendations in accordance with the Freedom of Information Act of 17 December 2004[2] (FoIA);
f. to carry out evaluations in accordance with the FoIA;
g. to carry out procedures for access to official documents in accordance with the FoIA;
h. to inform parliamentary oversight;
i. to inform the public;
j. to carry out his training activities.

Art. 40 Self-regulation

The FDPIC draws up a processing policy for all automated processing activities. Article 6(1) shall not apply.

Art. 41 Cooperation with the NCSC

[1] The FDPIC may pass on the notification of a data security breach to the National Cyber Security Centre (NCSC) for analysis of the incident with the consent of the controller that is subject to the notification duty. The notification may contain personal data.

[2] The FDPIC shall invite the NCSC to submit its comments before ordering the federal body to take the measures in accordance with Article 8 FADP.

Art. 42 Register on processing activities of federal bodies

[1] The register on the processing activities of federal bodies contains the information provided by the federal bodies according to Article 12(2) FADP and Article 31(2) of this Ordinance.

[2] The register is published on the internet. The register entries on planned automated processing activities in accordance with Article 31 shall not be published.

Art. 43 Codes of conduct

If a code of conduct is submitted to the FDPIC, he shall state in his opinion whether the code of conduct meets the requirements of Article 22(5)(a) and (b) FADP.

Art. 44 Fees

[1] The fees charged by the FDPIC are based on the time spent.

[2] An hourly rate of 150 to 250 Swiss Francs applies, depending on the function of the staff performing the task.

[3] In the case of services of exceptional scope, particular difficulty or urgency, surcharges of up to 50 percent of the fees pursuant to paragraph 2 may be levied.

[4] If the service provided by the FDPIC can be further used for commercial purposes by the person who is obliged to pay the fees, surcharges of up to 100 percent of the fees pursuant to paragraph 2 may be levied.

[5] In all other respects, the General Fees Ordinance of 8 September 2004[3] applies.

2 SR **152.3**

3 SR **172.041.1**

Chapter 7 Final Provisions

Art. 45 Repeal and amendments of other legislation

The repeal and the amendments of other legislation are set forth in Annex 2.

Art. 46 Transitional provisions

[1] For data processing activities that do not fall within the scope of Directive (EU) 2016/680[4], Article 4(2) shall apply at the latest three years after the entry into force of this Ordinance or at the latest at the end of the life cycle of the system. In the meantime, such processing activities shall be subject to Article 4(1).

[2] Article 8(5) shall not apply to assessments carried out before the entry into force of this Ordinance.

[3] Article 31 shall not apply to planned automated processing activities for which, at the time of entry into force of this Ordinance, the project has already been approved or the decision on the development of the project has already been made.

Art. 47 Entry into force

This Ordinance comes into force on 1 September 2023.

On behalf of the Swiss Federal Council

The President of the Confederation: Ignazio Cassis
The Federal Chancellor: Walter Thurnherr

[4] 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, version as amended in OJ L 119/89 of 4.5.2016, p. 89.

Annex 1

(Article 8(1))

States, territories, specific sectors in a State and international bodies with 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 ensured when the Canadian federal law "Loi sur la protection des renseignements personnels et les documents électroniques" of 13 April 2005[5] (Personal Information Protection and Electronic Documents Act) in the private sphere or a Canadian provincial law applies that is broadly equivalent to the federal law. The federal law applies to personal data that is collected, processed or disclosed in the context of commercial activities, irrespective of whether this is done by organisations such as associations, partnerships, individuals and trade unions or federally regulated entities such as facilities, plants, undertakings or business activities that fall within the legislative jurisdiction of the Canadian Parliament. The provinces of Québec, British Columbia and Alberta have enacted legislation that is broadly equivalent to the federal law. The provinces of Ontario, New Brunswick, Newfoundland and Labrador and Nova Scotia have enacted legislation that is broadly equivalent to the federal law with respect to health data. In all Canadian provinces the federal law applies to all personal data collected, processed or disclosed by federally regulated entities, including employee data of those entities. The federal law also applies to personal data transferred to another province or country in the course of commercial activities.
8.	Cyprus***	
9.	Croatia***	
10.	Denmark*	
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.	Iceland*	
23.	Israel***	
24.	Italy*	
25.	Jersey***	
26.	Latvia*	
27.	Liechtenstein*	
28.	Lithuania*	
29.	Luxembourg*	
30.	Malta*	
31.	Monaco***	
32.	Norway*	

5 The text of the Canadian federal law is available at https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html.

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***

* The data protection adequacy assessment includes the disclosure of personal data in accordance with Directive (EU) 2016/680[6].

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

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

6 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, version as amended in OJ L 119/89 of 4 May 2016, p. 89.

walderwyss

Contacts

Jürg Schneider
Dr. iur., Attorney at Law
Partner
Direct phone: +41 58 658 55 71
juerg.schneider@walderwyss.com

David Vasella
Dr. iur., Attorney at Law
Partner
Direct phone: +41 58 658 52 87
david.vasella@walderwyss.com

Hugh Reeves
MLaw, LL.M., Attorney at Law
Direct phone: +41 58 658 52 73
hugh.reeves@walderwyss.com