DATA PROTECTION LAWS OF THE WORLD

Switzerland

SWITZERLAND

Last modified 22 August 2023

LAW

The processing of personal data is mainly regulated by the Federal Act on Data Protection of 25 September 2020 (FADP) and its ordinances, i.e., the Ordinance on Data Protection (ODP) and the Ordinance on Data Protection Certification. The FADP (including its ordinances) has entered into force on 1 September 2023 and become effective without any transition period.

The FADP has recently been revised with the aim to strengthen data protection in general and to align it with the requirements of the EU General Data Protection Regulation (GDPR) in order to facilitate compliance of Swiss companies with those aspects of the GDPR that are applicable to controllers or processors outside of the EU, and to ensure that the EU will continue to consider Switzerland as providing an adequate level of data protection. However, the FADP continues to provide for certain deviations from the GDPR, thus requiring certain “Swiss Add-Ons” in a number of areas.

The processing of personal data is further restricted by provisions in other laws, mainly with regard to the public sector and regulated markets.

Key differences between the former and the new FADP

- Scope of “personal data”: The former FADP was applicable to personal data pertaining to both natural persons and legal persons. In contrast, the new FADP only protects personal data of natural persons.
- Data processing principles: While the data processing principles have essentially remained the same, the new FADP, in addition, explicitly provides for the principles of “privacy by design” and “privacy by default”.
- Information obligation: With the new FADP, an extended duty to inform data subjects has been introduced.
- Additional obligations: The new FADP imposes a number of additional obligations. In particular, the controller and /or processor must, under certain circumstances, maintain records of processing activities, perform data protection impact assessments and notify data security breaches.
- Data subject rights: With the new FADP, certain data subject rights have been extended and a new right to data portability has been introduced.
- Supervisory authority: The new FADP grants the supervisory authority expanded powers, in particular to issue administrative measures in the event that data protection provisions have been violated.

Sanctions: While the new FADP continues to provide for criminal sanctions that are (primarily) directed against the responsible individual, the catalogue of punishable offences has been extended and the fines have been significantly increased.

Territorial scope

The FADP, like the GDPR, has an extraterritorial scope and is applicable to circumstances that have an effect in Switzerland, even if they were initiated abroad. This includes, for instance, international companies with group entities in Switzerland or, under certain circumstances, international companies even without such subsidiary in Switzerland based on their doing business in Switzerland. For civil claims, the Swiss conflict of law rules apply.

In addition, the FADP provides that private controllers domiciled abroad must designate a representative in Switzerland if they process personal data of data subjects in Switzerland and if the data processing fulfils all of the following requirements:

- The processing is connected to offering goods or services in Switzerland or to monitoring the behaviour of data subjects in Switzerland;
- the processing is extensive;
- the processing is carried out regularly;
- the processing involves a high risk for the personality of the data subjects.

DEFINITIONS

Definition of personal data

Personal data means any information relating to an identified or identifiable natural person. In contrast to its previous version, the FADP does no longer apply to personal data pertaining to legal persons.

Definition of sensitive personal data

Sensitive personal data is defined as:

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

Profiling and high-risk profiling

Profiling means any form of automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

High-risk profiling means profiling that poses a high risk to the data subject's personality or fundamental rights by matching data that allow an assessment to be made of essential aspects of the personality of a natural person.

High-risk profiling is subject to certain stricter requirements.

Breach of data security

Breach of data security means a breach of security that leads to the accidental or unlawful loss, deletion, destruction or modification or unauthorised disclosure of or access to personal data.

NATIONAL DATA PROTECTION AUTHORITY

Federal Data Protection and Information Commissioner (FDPIC)
Feldeggweg 1
CH - 3003 Berne Switzerland
T +41 (0)58 462 43 95
F +41 (0)58 465 99 96

Website and contact forms: https://www.edoeb.admin.ch/

The FDPIC supervises and advises federal and private bodies, comments on federal legislative projects and informs the public about his findings and rulings in cases of general interests.

REGISTRATION

The FADP does not require the registration of any data collections or processing activities for private data controllers. Instead, the FADP provides for a general duty for controllers and processors to maintain a record of processing activities (ROPA). The controller's ROPA shall at least contain the following information:

- The controller's identity;
- the purpose of the processing;
- a description of the categories of data subjects and the categories of processed personal data;
- the categories of the recipients;
- if possible, the period of storage of the personal data or the criteria to determine this period;
- if possible, a general description of the measures taken to guarantee data security;
- if the data is disclosed abroad, details of the country concerned and the implemented guarantees.

The processor's ROPA may be limited to information on the identity of the processor and of the controller, the categories of processing activities performed on behalf of the controller as well as, if possible, a general description of the data security measures and, in case of cross-border data transfer, the details of the country concerned and the implemented guarantees.

However, companies with less than 250 employees as well as natural persons do not have to maintain a ROPA unless:

- They process sensitive personal data on a large scale; or
- they carry out high-risk profiling.

DATA PROTECTION OFFICERS

There is no requirement to appoint a data protection officer (DPO).

However, controllers have the option to appoint a DPO as a contact point for the data subjects and the competent data protection authorities. A DPO's main tasks would be to train and advise private controllers in data protection matters and to participate in the implementation of data protection regulations.

The controller may also designate an “independent” DPO who meets certain additional qualifications. In such a case, the controller has to ensure that the DPO has all necessary resources (including access to the data processing activities and personal data) to fulfil its tasks and has the right to inform the management or governing body regarding important data protection matters. Additionally, the DPO must exercise its function in a professionally independent manner and without being bound by instructions from the controller and shall not perform any activities which are incompatible with its tasks as DPO. The DPO shall also possess the required expertise. Finally, the contact details of the DPO must be published and notified to the FDPIC.

In case an “independent” DPO is appointed, the controller has no obligation to consult with the FDPIC in the event that a data protection impact assessment indicates a high risk to the personality or the fundamental rights of the data subject despite the planned measures by the controller (see here). This is the only relief granted in case of appointing an “ independent” DPO.

COLLECTION & PROCESSING

Data Processing Principles and Duties

The following principles apply to the collection and processing of personal data:

- Personal data may only be processed lawfully, in good faith and in accordance with the principle of proportionality.

- The collection of personal data and, in particular, the purpose of its processing must be evident to the data subject. In addition, the FADP imposes the following duties on controllers:
    - a duty to inform the data subject about the collection of personal data similar as under the GDPR, with the list of minimum information being shorter, but drafted more openly and in a non-exhaustive manner (however, the FADP goes beyond the GDPR in that it requires the controller to specify all countries to which personal data is transferred, or from which it is accessed, and to provide some additional information in this context);
    - under certain circumstances a duty to inform the data subject about decisions based solely on automated processing that have legal consequences or significant impact on the data subject (automated individual decision).

Wilful violations of the information duty may be subject to sanctions (see here).

- Personal data should only be processed for a purpose that is indicated or agreed at the time of collection, evident from the circumstances at the time of collection, and/or provided for by law.
- The controller and any processor must ensure that the data processed is accurate.
- Personal data must not be transferred abroad if the privacy of the data subject may be seriously endangered (see here).
- The controller must design the processing in technical and organisational terms to comply with data protection law, in particular the (other) data processing principles (privacy by design). Furthermore, the controller is obliged to ensure by means of suitable default settings that the processing is limited to the minimum required for the respective purpose (privacy by default).
- Personal data must be protected from unlawful and unauthorized processing by appropriate technical and organisational measures.
- Personal data must not be processed against the explicit will of the data subject, unless this is justified by:
    - an overriding private or public interest; or
- Sensitive personal data must not be disclosed to a third party, unless this is justified by:
    - the consent of the data subject (which must be given expressly in addition to being voluntary and based on adequate information);
    - an overriding private or public interest; or
- Personal data shall be destroyed or anonymized as soon as it is no longer required for the respective processing purpose.

The FADP imposes on the controller a duty to conduct a data protection impact assessment if the processing may constitute a high risk for the personality or the fundamental rights of the data subject (particularly when new technologies are used) and also defines specific cases where a data protection impact assessment may be necessary, including in the event of processing sensitive personal data on a large scale and systematic surveillance of extensive public areas. The FDPIC generally needs to be consulted if the data protection impact assessment shows that the processing presents a high risk for the personality or fundamental rights of the data subject despite the measures envisaged by the controller.

Rights of the Data Subject

Data subjects enjoy certain rights to control the processing of their personal data:

Right of access

A data subject is generally entitled to request access to, and obtain a copy of, his or her personal data that is being processed (i.e. the personal data as such), together with prescribed information on the identity and contact details of the controller, the purpose of processing, as well as the period of storage of the personal data (or the criteria used to determine the period) and the available information about the source of the personal data, if it has not been collected from the data subject. If applicable, the data subject is also entitled to be informed about the existence of an automated individual decision and the logic on which this decision is based as well as the recipients (or categories of recipients) to which the personal data is disclosed. In case of cross-border data transfer, the destination country and the implemented guarantee (if applicable) shall also be provided to the data subject. There are certain exceptions, e.g. a data controller may invoke its own overriding interests, however, only if it does not disclose the personal data to third parties (whereby companies controlled by the same legal entity are not considered third parties).

Wilful violations of data subject access rights by giving incomplete or wrong information are subject to sanctions (see here).

Right to rectify / Right to erasure / Right to restriction of processing / Right to object

The data subject may request that inaccurate personal data concerning him or her be corrected. Taking into account the purpose of the processing, he or she may also request that incomplete personal data be completed. This right is, however, restricted to the extent that a legal provision prohibits the modification or the personal data is processed for archival purposes in the public interest.

If the personal data is processed unlawfully and there is no justification (i.e. consent, overriding private or public interest or legal basis), the personal data must be deleted or destroyed. Under such circumstances, the data subjects may also request that the data processing be prohibited or restricted or they may object to the processing in question.

Right to data portability

Data subjects may request the controller to deliver the personal data that they have disclosed to it in a conventional electronic format if the controller is carrying out automated processing of the data and if the personal data is being processed with the consent of the data subject or in direct connection with the conclusion or the performance of a contract between the controller and the data subject. In addition, the data subject may request the controller to transfer the personal data to another controller if the aforementioned requirements are met and no disproportionate effort is required. There are certain exceptions, e.g. a data controller may invoke its own overriding interests, however, only if it does not disclose the personal data to third parties.

TRANSFER

Personal data may be transferred outside Switzerland if the destination country offers an adequate level of data protection. The Federal Council maintains and publishes a list of such countries as Annex 1 to the ODP. It should be noted that, under Swiss data protection law, remote access to data residing in Switzerland from outside of Switzerland is also considered a transfer/disclosure abroad.

The Federal Council deems, *inter alia*, the data protection legislations of all EEA countries as well as of the United Kingdom to be adequate. However, the countries covered by an adequacy decision of the European Commission do not fully correspond to those considered as adequate by the Federal Council.

In the absence of legislation that guarantees adequate protection, personal data pertaining to individuals may be disclosed abroad only if at least one of the following conditions is fulfilled:

- Data protection clauses in an agreement between the controller or the processor and its contractual partner that ensure an adequate level of data protection. The use of such clauses must be notified to the FDPIC beforehand.
- Specific guarantees drawn up by the competent federal body that ensure an adequate level of data protection. The use of such guarantees must be notified to the FDPIC beforehand.
- Standard data protection clauses that the FDPIC has approved, issued or recognised beforehand. On 4 June 2021, the European Commission had issued new Standard Contractual Clauses (SCC). According to the FDPIC, these new SCC can also be used to safeguard cross-border data transfers from Switzerland to countries without an adequate level of data protection, provided they are (slightly) amended to comply with the FADP. “Old” safeguards based on the former SCC may no longer be used. Contrary to the former FADP, the FDPIC does not have to be notified about the implementation of SCC anymore. Other safeguards still have to be notified.
- Binding corporate rules that ensure an adequate level of data protection in cross-border data flows within a single legal entity or a group of affiliated companies. Such rules must have been approved by the FDPIC or by the authority responsible for data protection in a country that guarantees an adequate level of protection.
- The data subject explicitly consents to the particular data export.
- The disclosure is directly connected with the conclusion or performance of a contract between the controller and the data subject or between the controller and its contracting partner in the interest of the data subject.
- The disclosure is essential in order to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal rights before a court or another competent foreign authority.
- The disclosure is required in order to protect the life or the physical integrity of the data subject or of a third party and it is not possible to obtain the data subject's consent within a reasonable period of time.

- The data subject has made the personal data generally accessible and has not expressly prohibited its processing.
- The data originates from a register provided for by law which is accessible to the public or to persons with a legitimate interest, provided that the legal conditions for the consultation are met in the specific case.

Violations of certain obligations regarding cross-border transfers of personal data are subject to sanctions (see here).

Regarding cross-border data transfers to the US, the EU and the US have established a new “EU-US Data Privacy Framework” (as successor of the invalidated EU-US Privacy Shield). On 10 July 2023, the EU Commission issued an adequacy decision for the EU-US Data Privacy Framework as the US would ensure an adequate level of protection for personal data transferred from the EU to organisations in the US that are included in the “Data Privacy Framework List”. Therefore, a transfer of personal data from the EU to a US company certified under the EU-US Data Privacy Framework no longer requires additional safeguards pursuant to the GDPR. While neither the EU-US Data Privacy Framework nor the adequacy decision by the EU directly impact data transfers from Switzerland to the US, the FDPIC took, for the time being, note of these developments. It may be anticipated that the Swiss authorities will aim at establishing a similar framework in the foreseeable future.

SECURITY

The data controller and any processor shall guarantee a level of data security appropriate to the risk by taking suitable technical and organisational measures. The measures must make it possible to avoid data security breaches and ensure the confidentiality, availability, integrity and traceability of the personal data. In particular, personal data must be protected against the following risks:

- Unlawful or accidental loss, deletion and destruction;
- technical errors;
- forgery, theft or unlawful use;
- unauthorized altering, copying, accessing or other unauthorized processing.

The technical and organisational measures must be appropriate, in particular with regard to the type of processed data and the purpose, nature, extent and circumstances of the data processing, the risks for the personality or fundamental rights of the data subjects and the current technological standards and implementation costs. The ODP sets out these requirements in more detail.

Wilful violations of the minimum data security requirements (which, however, are only defined generally in the ODP) are subject to sanctions (see here).

BREACH NOTIFICATION

The FADP provides for three different notification obligations in the event a data security breach occurs:

1. The controller shall notify the FDPIC as soon as possible of any data security breach that is likely to lead to a high risk to the data subject's personality or fundamental rights. The FDPIC has made available a reporting portal (see here), which may be used to submit a notification.
2. The controller shall inform the affected data subjects of any data security breach if this is required for their protection or if the FDPIC so requests. Even though the FADP does not stipulate a specific time frame in this regard, it is evident that such information must be provided in a timely manner in order to achieve its purpose.
3. The processor shall notify the controller of any data security breach as soon as possible. The FADP does not provide for a threshold in this respect. Therefore, a notification is required regardless of the specific risk involved.

A data security breach is defined as a breach of security that leads to the accidental or unlawful loss, deletion, destruction or modification or unauthorised disclosure or access to personal data. The ODP details what information a breach notification must contain and imposes a documentation obligation on the controller.

ENFORCEMENT

Investigations by the FDPIC

The FDPIC may initiate an investigation against a federal body or a private person if there are sufficient indications that a data processing activity could violate data protection regulations. If the data protection regulations have been violated, the FDPIC may issue administrative measures, for instance, the FDPIC may order the modification/suspension/termination of the processing and deletion of personal data or delay or even prohibit the disclosure abroad.

Criminal Sanctions

The FADP provides for criminal liability and fines of up to CHF 250,000, which are primarily directed against the responsible natural person (and not the respective company as under the GDPR). In particular, the following duties are subject to criminal fines in the event of certain wilful violations:

- Duty to provide information when collecting personal data and in the case of an automated individual decision;
- duty to provide information upon a data subject access request;
- duty to cooperate with the FDPIC in the context of an investigation;
- duty to meet certain requirements in connection with cross-border data transfers;
- duty to meet certain requirements in connection with the assignment of processors;
- duty to meet certain minimum requirements for data security;
- professional duty of confidentiality;
- duty to comply with a ruling issued by the FDPIC or a decision of the appeal courts.

Criminal proceedings must be initiated by the competent cantonal prosecution authority.

Finally, under Swiss civil law the data subject may apply for injunctive relief and may file a claim for damages as well as satisfaction and/or surrender of profits based on the infringement of his/her privacy.

ELECTRONIC MARKETING

Electronic marketing practices must comply with the provisions of the Swiss Federal Act Against Unfair Competition (UCA).

With regard to the sending of unsolicited automated mass advertisement (which, in addition to emails, includes SMS, automated calls and fax messages), the UCA generally requires prior consent by the recipient, i.e., 'opt-in'. As an exception, mass advertisings may be sent without the consent of the recipient:

- If the sender received the contact information in the course of a sale of his/her products or services;
- if the recipient was given the opportunity to refuse the use of his/her contact information upon collection (opt-out); and
- if the mass advertising relates to similar products or services of the sender.

In addition, mass advertising emails must contain the sender’s correct name, address and email contact and must provide for an easy-access and free of charge ‘opt-out’ from receiving future advertisements.

The UCA generally applies to business-to-consumer as well as to business-to-business relationships, i.e., mass advertisements sent to individuals and to corporations are subject to the same rules.

Direct marketing by telephone is not *per se* impermissible in Switzerland as long as it is not done in an aggressive way (e.g., by repeatedly calling the same person). However, the UCA prohibits direct marketing by telephone:

- If the recipient is not listed in the Swiss telephone directory or if the recipient is listed in the Swiss telephone directory, but has indicated that he/she does not wish to receive advertising from persons with whom he/she has no business relationship; or
- if the caller is not calling from a telephone number that (i) is listed in the Swiss telephone directory, (ii) is shown when calling, and (iii) he/she is entitled to use.

In order to enforce the above criteria, the UCA not only sanctions the violation of these principles, but also the use of information that has been obtained in violation thereof (e.g. someone using the information obtained from non-compliant call centres). An intentional violation can be sanctioned with a custodial sentence of up to three years or a monetary penalty.

In addition to the rules of the UCA, the general data protection principles under the DPA also apply with regard to electronic marketing activities, e.g., the collection and maintenance of email addresses or processing of any other personal data.

ONLINE PRIVACY

The processing of personal data in the context of online services is subject to the general rules pertaining to the processing of personal data under the FADP. In addition, certain aspects of online privacy are covered by other regulations, such as the use of cookies which is also subject to the Swiss Telecommunications Act (TCA).

Under the TCA, the use of cookies is considered to be processing of data on external equipment, e.g., another person’s computer. Such processing is only permitted if users are informed about the processing and its purpose as well as about the means to refuse the processing, e.g., by configuring their web browser to reject cookies.

In addition, the general rules under the FADP apply where cookies collect data related to persons who are identified or identifiable, i.e., personal data. In particular, the controller must provide the data subjects with certain information when collecting personal data (for more details on the information obligation see here). In practice, this is often fulfilled by including a section on cookies in the website's privacy policy or implementing a specific cookie policy. In accordance with the principles of privacy by design and privacy by default, the controller shall furthermore only pre-select essential cookies. Non-essential cookies (e.g. analysing cookies) may, depending on the circumstances, only be used with the data subject's consent.

Where the personal data collected through a cookie is:

- Considered sensitive personal data, e.g., data regarding religious, ideological, political views or activities; or
- so comprehensive that it permits an assessment of essential characteristics of the personality of a person (i.e. high-risk profiling)

the stricter rules pertaining to the processing of sensitive personal data and high-risk profiling are applicable. These stricter rules provide, *inter alia,* that consent (if necessary) must be given expressly. Furthermore, sensitive personal data may not be disclosed to third parties without justification.

KEY CONTACTS

Schellenberg Wittmer Ltd
www.swlegal.ch/

Roland Mathys
Partner / Attorney at Law
T +41 (0)44 215 3662
roland.mathys@swlegal.ch

Kenzo Thomann
Associate / Attorney at Law
T +41 (0)44 215 3659
kenzo.thomann@swlegal.ch

Helen Reinhart
Associate / Attorney at Law
T +41 (0)44 215 9360
helen.reinhart@swlegal.ch

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.