

Processing Personal Data in Switzerland

Substantive requirements

Good faith

Personal data must be processed in good faith. Personal data must not be collected by misrepresentation or deception.

Proportionality

The processing of personal data must be proportionate. This means the data processing must be necessary for the intended purpose and reasonable in relation to the infringement of privacy. Subject to regulations on the safekeeping of records, personal data should not be retained longer than necessary.

Accuracy of the data

The data processor must ensure that the personal data are accurate.

Purpose of the processing

Personal data may only be used for the purpose intended at the time of collection. It is therefore very important to disclose all anticipated purposes for which the data will be used when they are collected. Because of this restriction, the legality of data mining is doubtful because it inherently involves the use of data for a range of purposes, some of which may not have been disclosed when the data were collected.

Transparency

The collection of personal data, and in particular the purposes for which the personal data is processed, must be evident to the person or entity from whom personal data are collected. This requirement does not always lead to a specific disclosure obligation, but it will be necessary to give notice of any use of personal data which is not apparent to the data subject from the circumstances. For example, if personal data are collected in the course of concluding or performing a contract, but the recipient of the personal data intends to use the data for purposes outside the scope of the contract or for the benefit of third parties, then such uses of the personal data must be disclosed to the data subject.

Lawful justification

Anyone who processes personal data must not breach the privacy of the data subjects unlawfully.

As a rule, no justification for processing personal data is required if the data subjects have made the data generally available and have not expressly restricted the data processing. Generally available data may include data published in phone books without a restriction on their use or data distributed on business cards.

A lawful justification for data processing exists if the data subject has consented to it, the law provides for it, or the data processor has an overriding interest in the data processing. The Swiss Federal Data Protection Act (DPA) provides that the interest of the data processor in processing personal data shall, in particular, be taken into account when:

- a) the data processing occurs directly in connection with the conclusion of a contract or its performance;
- b) the data processor competes for business with, or wants to compete for business with, another person and processes personal data for this purpose without disclosing the data to third parties;
- c) the data processor, for the purpose of evaluating the creditworthiness of another person, processes neither sensitive personal data nor personality profiles and discloses only data to third parties which are necessary for the conclusion of a contract with the data subject or the performance of such contract;
- d) the data processor processes data professionally for publication in the editorial part of a medium which is published periodically;
- e) the data processing is for purposes that are not related to a specific person, in particular research, planning or statistics, and the results are published in a manner that does not permit the identification of the data subjects;
- f) the data processor collects data about a person who is a public figure to the extent that the data relate to the role of the person as a public figure.

The fact that a data processor has one of the above-listed interests in processing personal data does not mean that the data processor has an overriding interest in processing the data. The interest of the data processor in processing the data must nevertheless be weighed against the interest of the data subject in being protected against an infringement of his or her privacy.

If the data processor does have an overriding interest in processing the data, the processing of personal data can be performed despite the objection of the data subject.

Data security

The data processing must comply with technical and organizational security requirements, especially when processed electronically. Personal data must be protected against intentional or accidental deletion, accidental loss, technical errors, falsification, theft and unlawful use, unauthorized access, changes, copying, or other unauthorized processing.

Detailed technical requirements for data processing are set out in the Swiss Data Protection Ordinance (DPO).

Processing by a third party (outsourcing)

Data processing may be delegated to a third party under an agreement, provided that the third party data processor processes data only to the same extent as the person employing the third party data processor was authorised to do and that no legal or contractual confidentiality obligation prohibits the outsourcing.

The employer of the third party data processor must ensure that the data processor can ensure the security of the data.

Consent

Under certain circumstances consent of the data subjects may be required for the processing of personal data. The DPA now requires such consent to be given expressly for the processing of sensitive personal data or personality profiles. Implied consent is no longer sufficient.

Formal requirements

Information

Unless certain exceptions apply, the DPA requires the controller of the data file (i.e., the person deciding on the purpose and the content of a data file) to inform data subjects of the collection of sensitive personal data or personality profiles. In principle, this notice needs to be given when the data are collected. Data subjects must be informed, at a minimum, of the identity of the controller of the data file, the purpose of the data processing and the categories of recipients of the data if the disclosure of the personal data to third parties is anticipated.

Intentionally refraining from either informing the data subjects of the collection of data or providing the minimum information required by law is an offence punishable by a fine of up to CHF 10'000.--. If the fine is not paid, it can be replaced by imprisonment for up to 3 months.

Registration of data files

As a general rule, if a private person or legal entity regularly processes sensitive personal data or personality profiles or regularly discloses personal data to a third party, then the data files must be registered, before they are created, with the Federal Data Protection and Information Commissioner. The DPA and the Swiss Federal Data Protection Ordinance (DPO) provide exceptions to the registration obligation, including if

- 1) a private person processes personal data under a legal obligation to do so;
- 2) the controller of the data file has appointed a person responsible for data protection who complies with the requirements set out in the Swiss Federal Ordinance on Data Protection Certification (DPCO) and who independently monitors internal compliance with data protection regulations and maintains an index of the data files. Such appointment has to be notified to the Federal Data Protection and Information Commissioner;
- 3) the controller of the data file has obtained a quality certification as specified in the DPA and the DPCO and has notified the result of the certification process to the Federal Data Protection and Information Commissioner;
- 4) the data file contains exclusively supplier or customer data and does not contain sensitive personal data or personality profiles;
- 5) it is an auxiliary data file for employee administration which does not contain sensitive personal data or personality profiles.

Under prior law, no registration of data files was required if the data subjects had knowledge of the processing of their sensitive personal data, personality profiles or the disclosure to third parties. This exception is no longer available and therefore many data files may now require registration.

Failure to register a data file when required to do so by law is an offence punishable by a fine of up to CHF 10'000.--. If the fine is not paid, it can be replaced by imprisonment for up to 3 months. The same applies if, when registering the data file, willfully false information is provided.

Right to access

Each person has the right to submit a written request to the controller of a data file, with evidence of the person's identity, for disclosure of whether data about such person is being processed.

The controller of the data file must inform the data subject about all data stored with respect to the data subject (including the available information on the source of the data) and also the purpose and, if applicable, the legal basis for the data processing, the categories of processed data, the participants in the data processing and the recipients of the data.

The reply must be complete and provided in writing within 30 days and without charge.

The controller of a data file may refuse, restrict or defer the provision of information only if:

- permitted by law;
- the overriding interests of a third party require it; or
- the controller's own overriding interests require it and the controller does not disclose personal data to third parties.

Special rules are applicable to the media (newspapers, radio and television broadcasters, etc.).

Intentionally providing inaccurate or incomplete information is an offence punishable by a fine of up to CHF 10'000.--. If the fine is not paid, it can be replaced by imprisonment for up to 3 months.

Right to rectification

Data subjects can request that their data be corrected or deleted. If it cannot be established whether the data are accurate, then the data subject can ask to have such dispute noted in the data record.

Remedies

As mentioned above, criminal sanctions may apply to some infringements of data protection laws.

In addition, a data subject can sue for interim injunctions against data processing which unlawfully infringes his or her privacy. It also is possible to sue for the correction or deletion of data or a prohibition on the disclosure of data to third parties. An action for damages also is permitted.