

Transferring Personal Data Abroad

Concept of transfer abroad

The transfer of personal data out of Switzerland must comply with the Swiss Federal Data Protection Act (DPA).

A transfer of data abroad occurs as soon as the personal data are outside of Switzerland. Thus, personal data are transferred abroad if the transfer is made through another country even if the destination is in Switzerland.

If personal data can be accessed from abroad, such access also is classified as a transfer of personal data, even if the personal data are never accessed from abroad. Therefore, it is somewhat misleading to speak only of "transfers" of personal data because a "disclosure" of data abroad or the ability to access it from abroad also qualifies as a "transfer" for the purposes of the DPA.

Requirement for transfer abroad

The DPA prohibits a transfer of personal data abroad if it could seriously endanger the personality rights of the data subjects. Such a danger can exist if the personal data are transferred to a country whose legislation does not provide for an adequate protection of personal data.

The countries which have implemented the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU Directive) are considered to provide the required adequate level of data protection for personal data of individuals, but the EU Directive, unlike the DPA, does not provide such protection for legal entities. Although some EU countries have implemented protection for legal entities in their national data protection laws, not all have done so and therefore the EU countries in general cannot be considered to provide an adequate level of data protection for the personal data of legal entities.

For non-EU countries, it is necessary to check on a case-by-case basis whether they provide an adequate level of data protection. For example, neither U.S. federal law nor the laws of any U.S. state are considered to provide an adequate level of data protection, unless each of the following requirements is met: (i) the recipient has certified its adherence to the Safe Harbor rules of the US Department of Commerce under the U.S.-Swiss Safe Harbor Framework; (ii) the disclosure concerns personal data relating to natural persons only, (iii) the type of data which is disclosed is covered by the certification and (iv) the method of processing the data is covered by the certification. The fact that a potential recipient of data has certified its adherence to the privacy principles of the EU-U.S.- Safe Harbor Framework does not constitute a certification of adherence to the U.S.-Swiss Safe Harbor Framework. The certification of adherence to the U.S.-Swiss Safe Harbor Framework must be explicit, but it can be made along with the certification of adherence to the EU-U.S.-Safe Harbor Privacy Principles.

Unless the laws of a country to which the personal data is transferred provide for an adequate level of protection for the personal data to be transferred, the disclosure may only be made if one of the exceptions provided for in the DPA applies. These exceptions are:

- i) there are sufficient safeguards (for example contractual clauses in a transborder data transfer agreement) to ensure an adequate level of protection for data transferred outside Switzerland;
- ii) the data subject has, in the specific case, consented to the transfer of the relevant data outside Switzerland;
- iii) the data processing is directly connected with the conclusion or performance of a contract and the personal data relates to a contractual party;
- iv) the transfer of data is necessary in the specific case, either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before courts;
- v) disclosure is required in a specific case in order to protect the life or the physical integrity of the data subject;
- vi) the data subject has made the relevant data generally accessible and has not expressly prohibited processing of the data; or
- vii) disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection.

With necessary amendments required in order to comply with Swiss law, the model agreement of the Council of Europe or the model contracts for the transfer of personal data to third countries of the European Commission may be used in order to provide sufficient safeguards as mentioned in paragraph i) above.

In addition, in the case of the exceptions mentioned in paragraphs i) and vii) above, the Federal Data Protection and Information Commissioner must be informed of the safeguards or rules used. The Federal Data Protection and Information Commissioner must be informed before the first transfer of data is made or, if that is not possible, immediately after the disclosure has occurred.

The intentional failure to inform the Federal Data and Information Commissioner of the safeguards or rules, in the case of the exceptions mentioned under i) and vii), above, is punished 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 the information provided is intentionally inaccurate or incomplete.

A transfer of personal data back to Switzerland is not an issue under Swiss data protection law, but the processing of the personal data in Switzerland must comply with the rules detailed above.