Data protection in Switzerland: overview

- **Resource type: Country Q&A**
- **Status: Law stated as at 01-Aug-2014**
- **Jurisdiction: Switzerland**

A Q&A guide to data protection in Switzerland.

This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects; rights to access personal data or object to its collection; and security requirements. It also covers cookies and spam; data processing by third parties; and the international transfer of data. This article also details the national regulator; its enforcement powers; and sanctions and remedies.

To compare answers across multiple jurisdictions, visit the Data Protection *Country Q&A tool*.

This article is part of the multi-jurisdictional guide to data protection. For a full list of contents, please visit *www.practicallaw.com/dataprotection-mjg*.

Roland Mathys, Schellenberg Wittmer Ltd

Contents

Regulation

Legislation

1. What national laws regulate the collection and use of personal data?

General laws

Data protection is mainly regulated in the Swiss Federal Data Protection Act (DPA) and the related Data Protection Ordinance (DPO). The DPA and DPO apply to private persons and legal entities, and also to federal governmental bodies as data controllers.

This guide will focus on the provisions of the DPA in the private sector.

Sectoral laws

Each canton in Switzerland has a cantonal data protection act in place. These cantonal acts are directed to cantonal governmental bodies as data controllers.

Additional provisions that only apply to specific sectors or circumstances can be identified in a number of statutes, for example, employment law, criminal law, banking law, telecom law, life sciences law, social security law or unfair competition law.

Scope of legislation

2. To whom do the laws apply?

The Swiss Federal Data Protection Act (DPA) and the Data Protection Ordinance (DPO) apply to all private persons, legal entities and federal bodies controlling or processing personal data.

The cantonal data protection acts apply to the processing of data by governmental bodies of the respective canton in Switzerland.

3. What data is regulated?

The Swiss Federal Data Protection Act (DPA) and the Data Protection Ordinance (DPO) apply to personal data, that is data relating to an identified or identifiable individual. Individuals can be natural persons or legal entities (*Article 3(b), DPA).*

4. What acts are regulated?

The Swiss Federal Data Protection Act (DPA) and the Data Protection Ordinance (DPO) regulate the act of processing. Processing is interpreted very broadly, and means any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data (*Article 3(e), DPA*).

5. What is the jurisdictional scope of the rules?

In private international law, the Swiss Federal Data Protection Act (DPA) and the Data Protection Ordinance (DPO) apply (*Article 139, paragraph 1 and 3, Swiss Federal Act on Private International Law (PILA)*):

- If the data subject (as the potentially infringed party) is a Swiss resident.
- If the data controller or processor (as the potentially infringing party) is a Swiss resident; or
- If a data protection breach has an effect in Switzerland.

In the non-private sector, the DPA and the DPO (or respective cantonal legislations) apply to the processing of data by Swiss federal or cantonal governmental bodies.

6. What are the main exemptions (if any)?

The Swiss Federal Data Protection Act (DPA) does not apply to (*Article 2, paragraph 2, DPA*):

- The processing of data by a natural person exclusively for his private use (if the data is not disclosed to third parties).
- Pending civil or criminal proceedings.
- Public registers based on private law, for example, the commercial register.

Notification

7. Is notification or registration required before processing data?

Data files or collections must be registered in advance by federal bodies. Private persons only need to register (*Article 11a, paragraph 2 and 3, Swiss Federal Data Protection Act (DPA)*):

- If they regularly process sensitive personal data or personality profiles; or
- If they regularly disclose personal data to third parties.

There are some exceptions from the duty to register, for example, if the data controller has designated an internal data protection officer (*Article 11a, paragraph 5 DPA*).

In addition, there is a duty under the DPA to provide specific information on the collection of sensitive personal data and personality profiles. This includes information on the data controller, the purpose of collection and the categories of potential data recipients (*Article 14, DPA*).

In the case of a cross border data transfer, specific safeguards taken by the data controller to ensure an adequate level of data protection abroad must also be notified (*see Question 23).*

Main data protection rules and principles

Main obligations and processing requirements

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

The Swiss Federal Data Protection Act (DPA) provides several principles that must be observed when processing personal data. The principles are as follows (*Article 4, DPA*):

- Personal data may only be processed lawfully (principle of lawfulness).
- Processing must be carried out in good faith and must be proportionate (principle of proportionality).
- Personal data can only be processed for the purpose indicated at the time of collection, that is evident from the circumstances or that is provided for by law (principle of appropriation).
- The collection of personal data and in particular the purpose of its processing must be evident to the data subject (principle of transparency).

In addition, proper processing requires:

- The processed personal data to be accurate and correct (*Article 5, DPA*).
- The personal data to be protected against unauthorised processing by appropriate organisational and technical means (*Article 7, DPA*).

9. Is the consent of data subjects required before processing personal data?

Consent is not necessarily required for the lawful processing of personal data. The processing of personal data is generally considered as lawful if certain principles are followed (*see Question 8*). However, consent may justify an act of data processing that would otherwise be considered unlawful (*Article 13, paragraph 1, Swiss Federal Data Protection Act (DPA)*).

Consent can be implied or inferred, provided it is given voluntarily on the provision of adequate information (informed consent). Express consent is required for the processing of sensitive personal data or personality profiles (*Article 4, paragraph 5, DPA)* (*see Question 11*).

It is generally recommended to ask for express consent, as this is the most clear and evidential way to prove that consent has been given.

There are no specific rules that apply to consent by minors. The general rules on minors' capacity to act (minor's capability of judgement and consent of the minor's legal representative) are applicable.

10. If consent is not given, on what other grounds (if any) can processing be justified?

If consent is not given, processing can be justified on the basis of an overriding private or public interest or by law (*Article 13, paragraph 1, Swiss Federal Data Protection Act (DPA)*). The DPA contains a non-exhaustive list of potentially overriding private interests, including the processing of data in connection with the conclusion or performance of a contract and processing for research purposes (*Article 13, paragraph 2, DPA*).

Special rules

11. Do special rules apply for certain types of personal data, such as sensitive data?

Special rules apply for sensitive data and personality profiles.

Sensitive data

Sensitive personal data is defined as data on (*Article 3(c) Swiss Federal Data Protection Act (DPA)*):

- Religious, ideological and political views and activities.
- Health, the intimate sphere or racial origin.
- Social security measures.
- Administrative or criminal proceedings and sanctions.

Data on financial standing, wealth and income is not considered to be sensitive data.

Personality profiles

A personality profile is a collection of data that permits an evaluation of essential characteristics of the personality of a natural person (*Article 3 (d), DPA*).

For sensitive data and personality profiles, the following special rules exist:

- The requirement for express consent (*Article 4, paragraph 5, DPA*).
- The duty to provide information to data subjects (*Article 7, DPA*) (*see Question 12*).
- The duty to register the respective data files (*Article 11a, paragraph 3, DPA*) (*see Question 7*).
- The duty to provide information on the collection of the data (*Article 14, DPA*) (*see Question 7*).

Disclosure of sensitive data and personality profiles to third parties, without justification, always constitutes a data protection breach (*Article 12, paragraph 2 (c), DPA*).

Rights of individuals

12. What information should be provided to data subjects at the point of collection of the personal data?

In general, the data subject needs to be informed or be aware of the purposes of data collection and processing.

For sensitive personal data and personality profiles, the data subject must be notified of the data collection and given some basic information with the notification (*Article 14, Swiss Federal Data Protection Act (DPA)*) (*see Question 7*).

13. What other specific rights are granted to data subjects?

The data subject is entitled to request:

- Information from the data controller if his data is being processed (*Article 8, Swiss Federal Data Protection Act (DPA)*).
- The correction of incorrect or inaccurate data (*Article 5, DPA*).

14. Do data subjects have a right to request the deletion of their data?

The Swiss Federal Data Protection Act (DPA) provides data subjects with the right to request deletion of their data. However, this is only if the collection or processing of the data has been unlawful (*Article 15, paragraph 1, DPA*).

There is no general right to deletion of personal data.

Security requirements

15. What security requirements are imposed in relation to personal data?

The security requirements concerning personal data are set out in Article 7 of the Swiss Federal Data Protection Act (DPA) and, in further detail, in the Data Protection Ordinance (DPO). In general, the data controller is required to provide adequate technical and organisational protection measures.

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

There is no notification requirement under the Swiss Federal Data Protection Act (DPA). However, the general principle of transparency in data processing recommends notification (*see Question 8*).

Processing by third parties

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

Data processing may be assigned to third parties by agreement or by law if (*Article 10a, paragraph 1, Swiss Federal Data Protection Act (DPA)*):

- The third party data processor processes the data in the same way that has been authorised for the data controller; and
- The assignment is not prohibited by a statutory or contractual duty of confidentiality.

Electronic communications

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

Swiss data protection legislation does not provide specific terms relating to the use or storage of cookies. Cookies regularly constitute or contain personal data and are subject to the general principles (*see Question 8*). As a result, cookies should only be stored if the data subject is informed and is given the choice to de-activate cookies (opt-out mechanism).

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

The sending of unsolicited electronic communications (spam) is not specifically addressed in the Swiss Federal Data Protection Act (DPA) but in the Unfair Competition Act (UCA). The mass sending of spam is considered an act of unfair competition unless (*Article 3 (o), UCA*):

- The receiver has given consent.
- The sender is disclosed and identifiable; and
- The receiver is given a convenient and free of charge opportunity to unsubscribe from the communication.

International transfer of data

Transfer of data outside the jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

The cross border transfer of personal data requires that the privacy of the data subjects will not be seriously endangered. The risk is obvious if the legislation in the receiving state does not provide for adequate data protection (*Article 6, Swiss Federal Data Protection Act (DPA)*).

The Swiss Federal Data Protection and Information Commissioner (FDPIC) regularly publishes and updates a (non-binding) country list that states whether the level of data protection in a foreign jurisdiction is adequate or not. As a general rule, most jurisdictions in the EU provide for adequate protection, but some EU countries do not award protection to the personal data of legal entities. Outside of the EU, many jurisdictions do not provide a sufficient level of protection. In the case of inadequate protection, alternative measures must be taken. Such measures include the data subject's consent or contractual solutions (*see Question 21*).

The transfer of personal data within a group of companies in different jurisdictions is still considered a cross border data transfer and the rules set out above apply. Binding corporate rules may be invoked to provide adequate protection (*Article 6, paragraph 2(g), DPA*).

Data transfer agreements

21. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

Data transfer agreements are in use in Switzerland. They have been derived from the EU model clauses for transferring personal data. Templates in English and French can be downloaded from the website of the Federal Data Protection and Information Commissioner (FDPIC) (*see box, Regulator details*).

22. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

In general, data transfer agreements are considered sufficient to legitimise the transfer of data. However, depending on the type of personal data and the intended method of data processing, additional requirements may apply.

23. Does the relevant national regulator need to approve the data transfer agreement?

There is no requirement for the Federal Data Protection and Information Commissioner (FDPIC) to approve data transfer agreements. However, the FDPIC must be informed of data transfer agreements (*Article 6, paragraph 3, DPA*).

Enforcement and sanctions

24. What are the enforcement powers of the national regulator?

The Federal Data Protection and Information Commissioner (FDPIC) has the power to initiate investigations and issue recommendations to change or stop a method of data processing. If the data controller does not comply with the recommendations, the FDPIC may refer the matter to the Federal Administrative Court, with a right to appeal to the Federal Supreme Court (*Article 29 DPA*). The FDPIC has used this approach in a number of cases (for example, the landmark Google Street View Case).

25. What are the sanctions and remedies for non-compliance with data protection laws?

Civil, administrative and criminal sanctions and remedies are available for non-compliance with data protection laws.

Civil remedies

In civil proceedings, potentially infringed data subjects may file actions and request interim measures. Actions and interim measures include the (*Article 15, DPA*):

- Prohibition of data processing or disclosure.
- Correction of inaccurate personal data.
- Destruction of personal data that has been collected or processed unlawfully.

Administrative remedies

Administrative proceedings may be initiated by the Federal Data Protection and Information Commissioner (FDPIC) (*see Question 24*).

Criminal penalties

Some specific data protection breaches are sanctioned with criminal charges (fines up to CHF10,000). These include breaches of:

- The obligation to provide information, to register and to cooperate (*Article 34, DPA*).
- Professional confidentiality (*Article 35, DPA*).

Regulator details

Federal Data Protection and Information Commissioner (FDPIC) Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

W www.edoeb.admin.ch

Main areas of responsibility.

The FDPIC advises private persons on data protection matters, conducts investigations, issues recommendations and files complaints, reports to the Federal Council and informs the public on data protection matters of general interest, renders opinions on data protection matters and new legislation (*Article 28-31, DPA*).

Online resources

W www.admin.ch/opc/de/classified-compilation/19920153/index.html

Description. Official website of the Swiss Federal Government with full text of the DPA in German.

W www.admin.ch/opc/en/classified-compilation/19920153/index.html

Description. Official website of the Swiss Federal Government with non-binding English translation of the DPA.

Contributor profiles

Roland Mathys, Partner/Attorney at law

Schellenberg Wittmer Ltd

T +41 44 215 5252
F +41 44 215 5200
E roland.mathys@swlegal.ch
W www.swlegal.ch

Professional qualifications. MLaw, Basel, 1998; Attorney at law, Switzerland, 2000

Areas of practice. Data protection, general ICT, ICT outsourcing, ICT compliance.

Non-professional qualifications. MA in Economics and Computer Science, Zurich, 1994; Information Technology LL.M, London School of Economics, 2003

Recent transactions

- Acting for a major Swiss retail chain in various data protection issues.

- Advising a global pharmaceutical company in data protection issues related to the pooling of data centres.
- Rendering a legal opinion for an association faced with employee data disclosure to foreign jurisdictions and authorities.
- Reviewing privacy policies for a number of companies in the health care sector.

Languages. English, German, French

Professional associations/memberships. International Technology Law Association (ITechLaw, Director), International Bar Association (IBA), Swiss Bar Association (SBA), Swiss Arbitration Association (ASA), German Association for Law and Information Technology (DGRI), panellist to the WIPO Arbitration and Mediation Centre

Publications. *Legal and Data Protection Challenges of Wearable Computing (2014), E-Discovery and Data Protection (2012), Cross Border Data Transfer (2009), How to Protect my Virtual Identity (2007).*

Resource information

Resource ID: 9-502-5369

Law stated date: 01-Aug-2014

Products: Data Protection multi-jurisdictional guide, PLC Cross-border, PLC UK Commercial, PLC UK Corporate, PLC UK Employment, PLC UK Financial Services, PLC UK Law Department, PLC UK Public Sector, PLC US Intellectual Property & Technology, PLC US Law Department

Series: Country Q&A

Related content

Topics

Cross-border: IP&IT (http://uk.practicallaw.com/topic3-200-1614)

Article

Data Protection: Philippines (http://uk.practicallaw.comtopic0-503-0761)