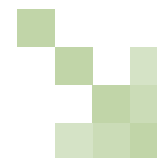


Switzerland

David Rosenthal, Homburger



www.practicallaw.com/9-261-8963

REGULATION

1. What national law(s) apply to the collection and use of personal data? If applicable, has Directive 95/46/EC on data protection (Data Protection Directive) been implemented?

The collection and use of personal data is mainly governed by the Federal Data Protection Act of 19 June 1992 (DPA), and its Ordinance (DPO). However, there are a number of provisions in other laws, mainly in the public sector (for example, mandatory health insurance, homeland security) and regulated markets (for example, banking), which further restrict or permit the processing of personal data. For example:

- The Telecommunication Act regulates the use of “cookies” by web-servers.
- The Code of Obligations further restricts the processing of personal data of employees.
- The Unfair Competition Act governs unsolicited e-mail adverts and other forms of electronic commercial communications.

In addition, a number of laws contain statutory secrecy obligations (for example, banking secrecy and telecommunications secrecy), which apply in parallel to the DPA.

As Switzerland is not in the EU or the European Economic Area (EEA), it has not implemented the Data Protection Directive. However, the European Commission has found that Swiss data protection legislation provides an adequate level of data protection, as is required under the Data Protection Directive (*Decision 2000/518/EC*).

The DPA came into force on 1 July 1993. On 24 March 2006, the Federal Parliament adopted a major revision to the DPA, currently expected to come into force towards the end of the summer of 2007. The following answers are primarily based on the revised DPA, and will point out where the current law provided for different rules. However, at the date of this publication, the related revision of the DPO has not yet been completed.

2. To whom do the rules apply (EU: data controller)?

The DPA applies to the processing of data by private bodies (that is, individuals, private sector businesses, non-profit organisations)

and federal bodies (that is, the Federal Administration) (cantonal bodies are subject to their own, cantonal data protection laws).

The rules for processing personal data do not only apply to data controllers, but also, in principle, to data processors, who can also be liable for violations of such rules. The DPA does not use the term “controller”; it refers to the “owner” of a data collection, which is the person who decides the purpose and the content of a data collection. A “data collection” is defined as any set of personal data that is structured in such a way as to enable a search of that data with regard to a particular data subject.

The following answers are limited to the processing of personal data by private bodies. Data processing by federal bodies is subject to additional restrictions (these also apply to private bodies if they are acting under public law, such as a company providing mandatory health insurance).

3. What data is regulated (EU: personal data)?

The DPA regulates personal data, which is any information that relates to an identified or identifiable natural person or legal entity.

There is no limit to certain categories of data. The following data types are examples only; they can all be personal data if it is possible to relate the information contained in them to one or more identified or identifiable individuals or legal entities:

- Customer data.
- Employee files.
- Business and private documents.
- Images.
- Videos.
- Sound recordings.
- E-mails.
- Log-files.
- The content of a fixed disc.

Whether a person is identifiable depends on whether the persons having access to the data could identify the data subject with reasonable efforts, for instance by using other data already available

to them. Anonymous or anonymised data is not subject to the DPA.

Similarly to the Data Protection Directive, the DPA provides for stricter rules with regard to sensitive personal data. Sensitive personal data includes information on an individual's:

- Religious, philosophical and ethical beliefs and activities.
- Political beliefs and activities.
- Trade union beliefs and activities.
- Health.
- Sexuality.
- Racial or ethnic origin.
- Measures in the field of social security.
- Administrative or criminal proceedings and sanctions.

Also under Swiss law, "personality profiles" are protected under the DPA in the same way as sensitive personal data. Personality profiles are collections of data that allow the appraisal of essential characteristics of the personality of an individual (for example, personnel files often fall into this category).

4. What acts are regulated (EU: processing)?

The DPA applies to any kind of processing of personal data, whether manual or automated. Processing is defined as any operation concerning personal data, irrespective of the means (paper, electronic, and so on) and procedures applied. In particular, processing of data includes its:

- Collection.
- Storage.
- Use.
- Amendment.
- Disclosure.
- Archiving.
- Destruction.

5. What is the jurisdictional scope of the rules?

In cases of privacy infringements, Swiss courts generally apply the DPA, if requested to do so by the data subject, if:

- The data subject is resident in Switzerland (provided this was foreseeable for the person infringing privacy).
- The person infringing privacy has its seat or residence or a branch in Switzerland.

- The violation of privacy occurs in Switzerland (again provided this was foreseeable for the person infringing privacy).

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

The DPA does not apply to:

- Anonymous data.
- Personal data that is processed by an individual exclusively for personal use and is not disclosed to third parties.
- Deliberations of the Federal Parliament and Parliamentary Committees.
- Pending civil actions (before a Swiss court), criminal proceedings in Switzerland, international judicial assistance proceedings in Switzerland, and constitutional and administrative proceedings in Switzerland (except for administrative proceedings at first instance).
- Public registers based on private law.
- Personal data processed by the International Committee of the Red Cross.

7. Is notification or registration required before processing data? If so, please provide brief details.

Owners of data collections that regularly process sensitive personal data or personality profiles, or regularly disclose personal data to third parties (including affiliates) must register their data collections with the regulatory authority (Federal Data Protection and Information Commissioner (FDPIC) (*see box, The regulatory authority*)) before they start processing. This will become possible to do over the internet. Non-compliance can be fined. If a company is required to register, it becomes subject to additional documentary obligations.

There are several exemptions, but only a few of them are relevant in practice. For example, registration is not required if the data is being processed because of an obligation imposed by law (such as by social security laws or anti-money laundering laws), or if the controller has its own independent data protection officer monitoring the controller's data protection compliance (the revised DPO (*see Question 1*) will provide further details in this regard; however, there is no obligation to appoint a data protection officer). It is expected that the revised DPO will contain further exemptions, for instance, for data archived solely for historical or scientific purposes, data collections exclusively based on publicly available information, and certain data used for non-personal purposes such as statistics or research.

Under the current DPA, registration is not necessary if the data subjects are aware of the processing, which is why many companies did not have to register in the past.

Obligations to notify the FDPIC also exist in connection with the export of personal data (*see Question 16*).

MAIN DATA PROTECTION RULES AND PRINCIPLES

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

The DPA sets out a number of “principles” for processing personal data. The principles apply equally to processors and controllers and a violation of them is considered an infringement of privacy.

The principles are:

- Personal data can only be processed lawfully and in accordance with the principle of good faith.
- Personal data must be collected in a manner that its collection and, in particular, the intended purpose of processing is recognisable by the data subject (this principle will be formally introduced with the revised DPA).
- Personal data can only be processed for the purpose:
 - indicated at the time of collection (or agreed);
 - that is evident from the circumstances at the time of collection; or
 - as provided for by law.
- Personal data cannot be processed excessively. That is, it can only be processed to the extent needed for the purpose of processing.
- Whoever processes personal data must ensure that it is accurate (to the extent this is necessary in view of the purpose for which such data is processed).
- Personal data cannot be transferred abroad if the privacy of the data subjects may seriously be endangered (*see Question 16*).
- Personal data must be protected by appropriate technical and organisational measures against unauthorised processing (*see Question 14*).

In addition:

- Sensitive personal data or personality files cannot be disclosed to a third party without a sufficient justification.
- Personal data cannot be processed against the explicit will of the data subject without a sufficient justification.

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

- What rules are there regarding the form and content of consent? Would online consent suffice?
- Are there any special rules regarding the giving of consent by minors?

If the principles for processing personal data (*see Question 8*) are complied with, no consent is required from the data subject to process its personal data. The data subject's consent is only required if compliance with the principles is not possible or not intended.

Form and content of consent

The revised DPA clarifies that any consent is only valid if given voluntarily and following appropriate information being given to the data subject (“informed consent”). The revised DPA further provides that any consent relating to sensitive personal data or personality profiles is only valid if given explicitly.

The DPA does not, however, require that consent must be given in writing. Therefore, oral or online consent is sufficient. Depending on the circumstances, it may still be advisable for evidentiary purposes to obtain consent in writing or by e-mail, and to obtain that consent in an explicit, rather than an implicit, manner.

It is generally accepted that a data subject can withdraw its consent at any time, and also that a data subject, in principle, has no obligation to react to requests from third parties for their consent. Therefore, it cannot necessarily be assumed that a data subject has given its consent from its non-reaction to a letter or e-mail stating that its consent will be deemed to have been granted for a particular processing if no objection is received within a certain deadline. However, in a pre-existing relationship, depending on the circumstances, this may be a practical approach for obtaining consent from a large group of data subjects.

Consent by minors

The DPA does not specially regulate consent of minors. However, according to a general principle of civil law, minors can validly consent as long as this does not involve financial obligations for them, and provided the minor is able to understand the implications of his consent and decide accordingly.

10. If there is no consent, on what other grounds (if any) can processing be justified?

Under the current DPA, it is possible to justify a violation of the data processing principles (*see Question 8*) by:

- Having the data subject's consent.
- An overriding private interest.
- An overriding public interest.
- Some other justification provided for by law.

The DPA lists a number of examples in which an overriding private interest of the person processing personal data is usually assumed. These include processing personal data:

- Related to a contractual partner in direct connection with the conclusion or performance of the relevant contract.
- About competitors (provided such information is not disclosed to third parties).
- For the purpose of credit rating (provided such information is disclosed only to third parties requiring such information in connection with the conclusion of a contract with the data subject, and further provided no sensitive personal data and no personality profiles are processed).
- By the media for the publication in the editorial part of a periodical publication.
- For non-personal purposes, such as research, planning, and statistics (provided the results are published in a way which leaves the data subjects anonymous).
- Of a person of public interest (provided the data relates to public activities of that person).

However, in the revised DPA the Federal Parliament tried to eliminate the possibility of justifying a violation of the principles on the basis of an overriding private or public interest. If this is how the new law will be interpreted in practice, it will no longer be allowed to process personal data in breach of the principles, except with the data subject's consent (or special rule of law overriding the DPA's principles). Consequently, several common data processing practices will become illegal. It is possible, though, that a legal doctrine will develop according to which overriding private and public interests may still justify a violation of the principles based on general principles of law.

The change does not affect the situation in which sensitive personal data or personality files are to be disclosed to a third party, and in which personal data are to be processed against the explicit will of the data subject. In both cases, an overriding private or public interest is still considered a sufficient justification.

There is no infringement of privacy if the data subject makes its data generally available and does not expressly prohibit its processing.

11. Do special rules apply in the case of certain types of personal data, for example sensitive data? If so, please provide brief details.

In general, the processing of sensitive personal data and personality profiles is considered more critical than the processing of other personal data. This must be taken into account when applying the principles of processing of personal data as well as when determining whether an overriding private or public interest justifies an infringement of privacy. For example, sensitive personal data requires more robust technical and organisational measures for preventing unauthorised data processing than "normal" personal data. Also, consent must be explicit to be valid (see *Question 9*).

A number of provisions of the DPA expressly refer to the processing of sensitive personal data and personality profiles, for example with regard to:

- The obligation to register data collections when sensitive personal data or personality profiles are processed on a regular basis (see *Question 7*).
- The obligation to obtain the data subject's explicit consent or other sufficient justification before disclosing sensitive personal data or personality profiles to third parties (see *Question 8*).
- The obligation of the owner of a data collection containing sensitive personal data or personality profiles to actively inform data subjects about the collection of their data. This obligation will be introduced under the revised DPA (see *Question 12*).
- A fine for persons who, without authorisation and intentionally, reveal sensitive personal data or personality profiles acquired in the course of their profession, provided that profession requires the knowledge of such data.

In addition, the Swiss Penal Code provides criminal sanctions for persons who without authorisation and intentionally collect sensitive personal data or personality profiles from a non-public data collection.

RIGHTS OF INDIVIDUALS

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

Unless provided otherwise by law, personal data must be collected in a manner that its collection and, in particular, the intended purpose of its processing, is recognisable by the data subject (that is, no covert data collection). This requirement will be introduced by the revised DPA. Currently, it only exists for federal bodies collecting sensitive personal data or personality profiles.

In addition, the revised DPA requires the owner of a data collection, containing sensitive personal data or personality profiles, to actively inform data subjects that the owner is collecting such data about them. The data subjects have to be informed of the:

- Purpose for which their data is processed.
- Categories of persons being supplied with such data (if any).
- Identity of the owner of the data collection.

Non-compliance with this information requirement can be fined.

Some exceptions exist, although an overriding private interest can only be relied on by owners who do not share the personal data with third parties (including affiliates).

The obligation to inform also applies when sensitive personal data or personality profiles are obtained from third parties, except if:

- The data subjects have already been informed.

- Storage or disclosure of their data is explicitly provided for by law.
- Informing them puts an undue burden on the owner of the data collection.

Owners of data collections have one year from the enactment of the revised DPA to implement the necessary measures to comply with these requirements. As a result, many companies will need to amend their online privacy policies and terms and conditions to contain the necessary information. However, in most cases, it is already necessary under the current DPA to fully advise data subjects about the purpose for which their personal data is collected, as otherwise it violates the principle of purpose limitation (see *Question 8*).

13. What other specific rights (such as a right of access to personal data or the right to object to processing) are granted to data subjects?

Data subjects have the following rights:

Right of access

A data subject can ask the owner of a data collection to inform him whether personal data about him is being processed. If it is, the data subject has a right to be informed about:

- All the personal data in the data collection related to him.
- The purpose and, if appropriate, the legal basis of the processing, as well as the categories of personal data processed, other parties involved with the file, and the data recipients.
- Any available information about the source of the data (under the revised DPA).

The information must be provided in writing and, usually, free of charge.

There are certain exceptions to the right of access, particularly if a law provides so or if overriding interests of a third party require this. An overriding private interest of the owner of the data collection can only be relied on if the personal data is not shared with third parties.

Non-compliance with the right of access can be fined.

The right of access cannot be waived. It can also be enforced against a person processing the data on behalf of the owner of the data collection, if the identity of the owner is not disclosed, or if the owner is not in Switzerland.

Right of rectification

A data subject can demand that (objectively) incorrect data about him is rectified. The data subject can also demand the entry of an appropriate remark if the accuracy of a particular piece of information is in dispute.

Right of objection

A data subject can object to the processing of his personal data, or the disclosure of such data to third parties. The data subject can also request the destruction of personal data about him. However, the data can still be processed if the processing can be justified (see *Question 10*).

SECURITY REQUIREMENTS

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

Personal data must be protected by appropriate technical and organisational measures against unauthorised processing. Systems and procedures for processing or transmitting personal data must ensure the confidentiality, accuracy and accessibility of such data. In particular, the DPO provides that personal data must be protected against:

- Unauthorised or accidental destruction.
- Accidental loss.
- Technical faults.
- Forgery.
- Theft.
- Unlawful use.
- Unauthorised alteration.
- Copying.
- Unauthorised access.
- Other unauthorised processing.

The DPO also provides that the technical measures must be examined periodically and must take into account the:

- Purpose of the data processing.
- Manner and extent of data processing.
- Risk for the data subjects.
- Currently available technology.

With regard to automated data processing, the DPO sets out a number of special measures to be implemented. These include:

- Data access control.
- Data transmission control.
- Control of the identity of recipients of personal data.
- Role based access.
- Processing permissions.

- Audit trails with regard to the entry of personal data (and other processing, if necessary to ensure data protection compliance in case of sensitive personal data or personality profiles).

PROCESSING BY THIRD PARTIES

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

The processing of personal data can be transferred to a third party if:

- The data controller ensures that the data will only be processed by the third party to the extent that the controller itself is entitled to do.
- No legal or contractual secrecy obligation prohibits the outsourcing of the data processing.

The revised DPA also emphasises that the controller must make sure that the third party ensures the security and safety of the personal data processed on behalf of the controller.

Although the DPA does not require it, a written contract for outsourcing data processing to a third party is recommended. The contract typically requires the third party to process the personal data solely on behalf of, and for the purposes of, the controller and according to the controller's instructions.

INTERNATIONAL TRANSFER OF DATA

16. What rules govern the transfer of data outside your jurisdiction?

Personal data can only be transferred outside Switzerland if an adequate level of data protection is ensured in the country of the data recipient (that is, the country to which the data is exported). Under the current DPA, there is no express rule on how to achieve such protection in the absence of an adequate data protection law in the destination country, although use of a data transfer agreement is the generally accepted method. Currently, it is even allowed to transfer data abroad without ensuring any protection (or providing only for a reduced level of protection) if this can be justified by an overriding private or public interest, or if the data subject has consented to it.

However, the revised DPA contains a conclusive list of acceptable methods for ensuring adequate data protection abroad (an overriding private interest will no longer be sufficient):

- The destination country has an adequate level of data protection. The FDPIC maintains and publishes a list of such countries. With regard to personal data related to individuals (but not personal data related to legal entities), it is expected that all EEA countries provide an adequate level of data protection. The US is generally considered not to provide an adequate level of data protection.
- There are "sufficient warranties" ensuring an adequate level of protection abroad, such as data transfer agreements (see

THE REGULATORY AUTHORITY

Federal Data Protection and Information Commissioner (FDPIC)

Head. Hanspeter Thür

Contact details. Office of the Federal Data Protection and Information Commissioner

Feldeggweg 1
CH - 3003 Berne
Switzerland
T +41 31 322 43 95
F +41 31 325 99 96
E info@doeb.admin.ch
W www.doeb.admin.ch

Main area of responsibility. Data Protection Act, Freedom of Information Act.

Contact for queries.

www.doeb.admin.ch/kontakt/index.html?lang=en

Obtaining information. See website above.

Question 17. Such agreements or other warranties must be notified to the FDPIC (model contracts or approved clauses are likely to be exempted).

- There are binding corporate rules (BCRs) that sufficiently ensure data protection in cross-border data flows within a single legal entity or a group of companies. Such BCRs have to be notified to the FDPIC (again, model or approved clauses are likely to be exempted).
- The data subject consents to the particular export. Under the revised law, consent must be given for one "individual case". While generic consent is not sufficient, it is not necessary to obtain the data subject's consent for every single transfer if the transfer forms part of an overall transfer scheme which has been approved by the data subject.
- The export of the personal data is required for the conclusion or performance of a contract with the data subject.
- The export of the personal data is necessary to maintain overriding public interests or to establish, execute or enforce legal rights in court proceedings (however, other provisions of Swiss law may still restrict such disclosures).
- The export of the personal data is necessary to protect the life or physical integrity of the data subject. A similar provision already exists under the Data Protection Directive.
- The data subject has made the personal data publicly available and has not expressly prohibited the processing of such data.

Under the current DPA, the transfer of a data collection outside Switzerland must be notified to the FDPIC (notifications are not publicly accessible, but the FDPIC may further investigate the matter), except when there is a legal duty for such a transfer (which is rare) or when the data subjects have knowledge of the transfer. In practice, many companies have amended their terms

and conditions and privacy policies to provide for the necessary information to avoid notification. This notification obligation will be abolished under the revised DPA (and replaced by the notification obligations stated above).

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

Data transfer agreements or clauses are frequently used in practice. The DPA does not require the use of a standard form. It is the responsibility of the exporter to conclude an agreement sufficiently protecting the rights of the data subject.

However, the FDPIC does provide a model data transfer agreement (controller to processor), which can be accessed on its website (*see box, The regulatory authority*) (using “transborder outsourcing” as the search term).

Although the contract is directly based on Swiss law and is rather short, it mirrors to a large extent the model clauses of the European Commission as well as the standard provisions used within the framework of Safe Harbour Agreements.

The European Commission’s model contracts can also be used provided that they are adapted to extend protection to the personal data of legal entities and personality profiles, if appropriate.

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

No consent is required if the data transfer agreement is appropriate and properly implemented, or if an adequate level of data protection abroad is ensured by other means (*see Question 16*). In addition, the other principles of processing must be complied with. For example, if the transfer abroad is unnecessary for the purpose of processing, this may be considered an excessive processing (*see Question 8*).

Secrecy obligations can also restrict data transfers abroad. Depending on their nature, they can result in the need to obtain prior consent.

19. Does the relevant national regulator need to approve the data transfer agreement? If so, please provide brief details.

Approval of the data transfer agreement by the FDPIC is not required.

ENFORCEMENT AND SANCTIONS

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

The FDPIC has no direct enforcement powers against private bodies processing personal data, and has only limited resources. It

typically concentrates on data processing by federal bodies and, in the private sector, on cases of a certain significance or publicity. However, the FDPIC can carry out investigations (including the right to demand the production of documents, make inquiries and ask for a demonstration of a particular processing of personal data) and issue and publish “recommendations”. The recommendations are not binding, but if they are not followed, or are rejected, the case can be submitted to the Federal Data Protection Commission (and, ultimately, to the Federal Supreme Court), and can become binding, if upheld.

21. What are the sanctions and remedies for non-compliance with the data protection laws? To what extent are the laws actively enforced?

The data subject can apply for injunctive relief and file claims based on infringement of its privacy, including claims for damages and satisfaction. The data subject can also seek the assistance of the civil court in exercising its rights of access, rectification and objection (*see Question 13*), and can request that the decision of the court is communicated to third parties or published.

Within Switzerland, claims can be filed at the place of residence (or seat) of the claimant (that is, the data subject) or of the defendant (the data controller or processor).

However, the infringement of privacy, particularly violations of the data protection principles (*see Question 8*), is not criminally sanctioned (no fines). This is also true in cases of non-compliance with a recommendation of the FDPIC, as it is non-binding (*see Question 20*).

There are fines up to CHF10,000 (about US\$7,990) for intentional non-compliance with the:

- Right of access (refusing to allow access or giving wrong or incomplete information) (*see Question 13*).
- Obligation to inform data subjects about the collection of sensitive personal data or personality profiles (*see Question 12*).
- Registration and notification obligations (*see Questions 7 and 16*).
- Obligation to co-operate with investigations of the FDPIC (*see Question 20*).
- Obligation of certain professionals to keep sensitive personal data and personality profiles confidential (*see Question 11*).

Compliance with the DPA by private bodies is rarely enforced in court. Likewise, criminal sanctions are very rare. Between April 2005 and March 2006, the FDPIC conducted 63 official investigations (50 cases concerned the right of access to homeland security files) and made five recommendations (*see Question 20*). Negative media reports about companies violating the privacy of consumers and employees are more frequent, and usually quite effective.



Homburger is a major Swiss business law firm. Since its establishment in 1957, Homburger has advised and represented Swiss and international corporate clients and individual entrepreneurs on key aspects of business law. We offer our clients expert legal advice, support them in business negotiations and transactions, represent them before arbitral tribunals and in court, and protect their interests in civil and administrative proceedings.

Homburger
Weinbergstrasse 56 | 58
CH - 8006 Zurich
P.O. Box 338 | CH - 8035 Zurich

Phone +41 43 222 10 00
Fax +41 43 222 15 00
lawyers@homburger.ch
www.homburger.ch

Homburger is organized in six practice groups integrating the skills and experience of some 100 lawyers focusing on specific areas. Our practice groups are Corporate and Transactions, Financial Services, Litigation and Arbitration, Tax, IP | IT, and Competition.

The Homburger IP | IT practice group consists of three partners and eight counsels | associates | trainees. The group offers a comprehensive range of legal services in the areas of IP and TMT.

In TMT, such services include in particular:

- litigation and arbitration on all matters involving IT, telecommunications, media and entertainment;
- IT transactions such as ITO, BPO, IT carve-outs, in-sourcing, etc.
- IT and media contracts such as software licensing and servicing, content acquisition and distribution, sports exploitation, etc.
- all aspects of telecommunications, including e-business
- data protection, e-discovery, document retention, etc.

Contacts in matters involving IT and Telecommunications

- Georg Rauber (georg.rauber@homburger.ch)
- Gregor Bühler (gregor.buehler@homburger.ch)
- David Rosenthal (david.rosenthal@homburger.ch)