The Legal 500 & The In-House Lawyer
Comparative Legal Guide
Switzerland: Data Protection & Cyber Security

This country-specific Q&A provides an overview to data protection and cyber security laws and regulations that may occur in Switzerland.

This Q&A is part of the global guide to Data Protection & Cyber Security. For a full list of jurisdictional Q&As visit http://www.inhouselawyer.co.uk/practice-areas/data-protection-cyber-security/


**Country Author:**
**Meyerlustenberger Lachenal Ltd**

The Legal 500

**Lukas Bühlmann, LL.M., Partner**

**lukas.buehlmann@mll-legal.com**

**The Legal 500**

**Dr. Michael Reinle, LL.M., Partner**

**lmichael.reinle@mll-legal.com**

**The Legal 500**


1. **Please provide an overview of the legal framework governing privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the laws enforced)?**

   **Initial Remarks**

The following answers are based on the current statutes dealing with data privacy. It must, however, be emphasized that the Federal Act on Data Protection, which is the main legal source for data protection (see next section), will be revised. The parliamentary debate about the revised statute is still ongoing. The main purpose of the revision is to harmonize Swiss law with the EU General Data Protection Regulation (GDPR) so that Swiss data protection laws will still be accepted as adequate by the EU. As a consequence, many of the obligations as set out in the GDPR, such as the information obligation, data breach notification, data protection impact assessment, will be integrated into the new Swiss statute. However, the provisions of the GDPR will not simply be copied. There will remain some differences. The revised statute will most likely not enter into force prior to 2020. There will then be a time period of two years for the implementation of the new duties by the data controllers.

**Federal Act on Data Protection**

The main regulation governing privacy in Switzerland is the Federal Act on Data Protection (FADP; see a tentative English translation here). As set out in art. 1 FADP, the statute aims to protect the privacy and the fundamental rights of persons when their data is processed. FADP applies to the processing of data pertaining to natural persons and legal persons by

- private persons and
- federal bodies.

The FADP covers any data processing by any private persons, i.e. individuals and legal entities, in any sectors. Data processing is defined in a broad way and includes 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 (see art. 3 lit. e FADP).

**Cantonal Data Protection Acts**

FADP solely governs data processing by federal bodies. Data processing by cantonal bodies is governed by cantonal data protection statutes. Each canton has implemented its own data protection act. Each canton has also appointed its own Cantonal Data Protection and Information Officer.

Most cantonal data protection laws are quite similar than the section of the FADP regarding the data processing by federal bodies.

**Secrecy Obligations**

Different statues include secrecy obligations, which also aim to protect privacy in a broader sense. The following secrecy obligations are important:

- Banking secrecy (art. 47 of the Federal Banking Statute): The banking secrecy protects any information relating to the relationship between the bank customer and the banking institute, including the fact that there is a customer relationship. Subject to this secrecy obligation are banking institutes as defined in the respective statute and any auxiliary persons, such as service providers. The banking secrecy is, in particular, important regarding outsourcing of bank customer data to cloud solutions.
- Patient secrecy (art. 321 of the Swiss Criminal Code): The patient secrecy protects any information relating to the relationship between a patient and surgeon or any other healthcare practitioner mentioned in art. 321 of the Swiss Criminal Code.

**Labor Law**

Art. 328b of the Swiss Code of Obligations sets out the following regarding data processing by employers: “The employer may handle data concerning the employee only to the extent that such data concern the employee's suitability for his job or are necessary for the performance of the employment contract. In all other respects, the provisions of the Federal Act of 19 June 19922 on Data Protection apply.”

Illegal data processing by employers can either be enforced in the same way as

ordinary infringements of the employment relationship, i.e. by filing a claim to the civil courts, or by using the remedies set out in the FADP.

2. **Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?**

FADP sets out a duty to register data files for the controller of such data files (see art. 11a FADP). Pursuant to art. 11a para. 2 FADP federal bodies must notify and register all their data files with the FDPIC. Private persons must notify their data files only in two constellations (see art. 11a para. 3 FADP):

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

Art. 11a para. 5 FADP contains a list with exemptions from the notification duty. One of the most important exemptions is set out in art. 11a para. 5 lit. e FADP: Data files must not be registered in the case that the respective controller has appointed an internal data protection officer.

Data file as set out in art. 11a FADP means any set of personal data that is structured in such a way that the data is accessible by data subject (see art. 3 lit. g FADP).

Controller of the data file means private persons or federal bodies that decide on the purpose and content of a data file (art. 3 lit. i FADP).

Sensitive personal data means data on: 1. religious, ideological, political or trade union-related views or activities, 2. health, the intimate sphere or the racial origin, 3. social security measures, and 4. administrative or criminal proceedings and sanctions (see art. 3 lit. c FADP).

Personality profiles means a collection of data that permits an assessment of essential characteristics of the personality of a natural person (art. 3 lit. d FADP).

3. **How do these laws define personally identifiable information (PII) versus sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?**

Personal data are defined as all information relating to an identified or identifiable person (art. 3 lit. a FADP). It is important to mention that Swiss law currently still covers not only information relating to individual persons, but also to legal entities (see the definition of data subjects in art. 3 lit. b FADP where both categories of persons are mentioned).

In a landmark decision dealing with the question on whether an IP-address is a personal data, the Swiss Federal Court, the highest Swiss court, has defined personal data as follows (see BGE 136 II 508): "A person is identified when it is clear from the information itself that it is precisely that person. The person is identifiable if he or she can be inferred on the basis of additional information. However, not every theoretical possibility of identification is sufficient for the determinability. If the effort is so great that, according to general life experience, it is not to be expected that an interested party will take it upon himself, there is no identifiability. The question is to be answered depending on the concrete case, whereby in particular also the possibilities provided by technology are to be considered, so for example the search tools available in the Internet. Of importance, however, is not only what effort is objectively required to be able to assign a certain piece of information to a person, but also what interest the data processor or a third party has in identification."

Regarding the definition of sensitive personal data, see Question 2 above.

4. **Are there any restrictions on, or principles related to, the general processing of PII – for example, must a covered entity establish a legal basis for processing PII in your jurisdiction or must PII only be kept for a certain period? Please outline any such restrictions or "fair information practice principles" in detail?**

Based on the legality principle, FADP requires a legal basis for the data processing by federal bodies. Federal bodies are solely permitted to process personal data if explicitly justified by law.

Contrary to the GDPR, FADP does not require a legal basis for any data processing by private persons. FADP solely requires that any data processing complies with the "General Data Protection Principles" as set out in art. 4 et seq. FADP. The general data protection principles are the following:

- **Legality Principle**: Personal data may only be processed lawfully (art. 4 para. 1 FADP). Prohibited is, for example, the illegal data collection, such as illegal communication recording, etc. The prohibitions may either be set out in the FADP or in other Swiss statutes, such as the Swiss Criminal Code.
- **Good Faith and Proportionality Principle**: The processing must be carried out in good faith and must be proportionate (see art. 4 para. 2 FADP). The principle of proportionality is one of the most relevant principles. It means, for example, that data retention must be proportional, i.e. personal data must only be retained as long as necessary. From the principle of good faith the FDPIC has derived the duty to notify data breaches. Such a notification duty is otherwise not explicitly mentioned in the FADP.
- **Purpose Limitation**: Personal data may 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 (see art. 4 para. 3 FADP).
- **Transparency Principle**: The collection of personal data and, in particular, the purpose of its processing must be evident to the data subject (see art. 4 para. 4 FADP). The transparency principle is one of the most relevant principles in the FADP. The FADP contains no explicit active information duty that is similar than the one in art. 13 et seq.

GDPR – except for sensitive personal data and personality profiles (see art. 14 FADP). As long as the data processing is transparent, no active and comprehensive information is required. However, in practice it is quite common to have data privacy notices in place.

- **Consent Requirements**: If the consent of the data subject is required for the processing of personal data, such consent is valid only if given voluntarily on the provision of adequate information. Additionally, consent must be given expressly in the case of processing of sensitive personal data or personality profiles (art. 4 para. 5 FADP).
- **Accuracy Principle**: Anyone who processes personal data must make certain that it is correct. He must take all reasonable measures to ensure that data that is incorrect or incomplete in view of the purpose of its collection is either corrected or destroyed (art. 5 FADP).

5. **Are there any circumstances where consent is required or typically used in connection with the general processing of PII and, if so, are there are rules relating to the form, content and administration of such consent?**

The processing of "normal" personal data does generally not need to be justified by a consent. Only if provisions of the FADP, in particular the general data protection principles (and most prominently the transparency principle as well as the principle of purpose limitation), were infringed, consent would be required. However, consent is pursuant to art. 13 FADP only one justification option. The other justifications are statutory obligations or an overriding interest of the public or the controller.

Consents are most likely thought after in connection with data processing for marketing purposes, such as e-mail marketing and profiling. However, in connection with e-mail marketing, the consent duty rather stems from art. 3 para. 1 lit. o Unfair Competition Act (see later in question 25).

The requirements for obtaining consents are set out in art. 4 para. 5 FADP (see above Question 4). It is important to mention that consent may also be provided

implicitly. As the burden of proof for obtaining a sufficient consent is on the controller, it is, however, recommended that data subjects be asked for an explicit consent and that the consent is documented. Swiss law does not ask for an explicit manner of documentation. At the end, the controller must prove who consented when to what kind of data processing. It is therefore important not only to prove who consented to what kind of data processing, but it is also important to keep the information that was provided to the data subject at the time of the consent.

6. **What special requirements, if any, are required for processing sensitive PII? Are there any categories of PII that are prohibited from collection?**

Sensitive personal data and personality profiles are subject to stricter requirements than the processing of “normal” personal data. When collecting and processing sensitive personal data or personality profiles, the data controller is subject to an active information duty (see art. 14 FADP). Furthermore, the disclosure of such data to third parties must be justified by consent, law or an overriding interest (see art. 12 para. 2 lit. c in connection with art. 13 FADP).

There are no categories of personal data, which are generally prohibited from collection.

7. **How do the laws in your jurisdiction address children’s PII?**

There is no specific provision for children’s personal data in the FADP. As a consequence, children’s personal data are dealt with in the same way as other personal data.

However, Swiss entities usually mention that children under the age of 18 (or sometimes 16) are not permitted to submit any personal data without the consent of their parents.

Finally, in the case that consent is required for a specific data processing activity, the Swiss Civil Code governs whether and on how children may provide such a consent (see art. 11 et seq. Swiss Civil Code).

8. **Are owners or processors of PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.**

**Maintenance of Records**

There is no explicit requirement to maintain records of the data processing activities in the current FADP. Art. 11a para. 5 lit. e FADP sets out that the internal data protection officer, if one is appointed at all, must maintain a list of data files. This obligation is, however, not comparable with the requirement to record all data processing activities as set out in the GDPR.

Notwithstanding the above, art. 10 of the Ordinance to the FADP requires for the automated processing of sensitive personal data and personality profiles the maintenance of records. Art. 10 sets out as follows: "the controller of the data file shall maintain a record of the automated processing of sensitive personal data or personality profiles if preventive measures cannot ensure data protection. Records are necessary in particular if it would not otherwise be possible to determine subsequently whether data has been processed for the purposes for which it was collected or disclosed."

**Internal Processes and Written Documentation**

FADP does not explicitly require the implementation of internal processes and written documentation. However, such obligations arise implicitly from other obligations set out in the FADP. The access right as set out in art. 8 et seq. FADP requires certain internal processes in order to comply with access requests timely. Furthermore, it requires written documentation for compliance and evidence purposes. The same applies to deletion or correction requests. As the FDPIC requires in certain constellations the notification of data breaches, an internal process and a written documentation is also recommended in that regard.

Finally, art. 7 FADP sets out in an general way that personal data must be protected against unauthorised processing through adequate technical and organisational measures. The appropriate technical and organizational measures must be documented in writing and may include the establishment of internal processes and policies. This is explicitly mentioned in art. 11 of the Ordinance to the FADP, where data controllers are required to establish a processing policy in the case that they maintain data files that must be notified pursuant to art. 11a FADP.

As the FADP and the Ordinance related thereto follow a risk-based approach, every legal entity may implement the internal processes in a way that are most appropriate taken the organizational structure, size etc. of the respective company. The processes are typically as follows:

- There is a policy in which the employees are, for example, informed about the access right of data subjects.
- The employees are informed in the policy to whom (i.e. to which individual or function) such requests must be forwarded in case that they are submitted to an employee who is not responsible.
- The companies appoint an employee who is responsible for data protection questions and receives requests etc. The respective employee must not necessarily be an official data

protection officer as set out in art. 11a para. 5 lit. e FADP. The main task is to centralize data protection related requests and questions.

9. **Are consultations with regulators recommended or required in your jurisdiction and in what circumstances?**

   Consultations are not required pursuant to the current FADP. However, it is quite common to contact the FDPIC and discuss with him specific data processing activities or the interpretation of a provision by the FDPIC. The communication is conducted on a no-name-basis, i.e. the client is not mentioned. The FDPIC is quite easy to reach.

10. **Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?**

    It is not required under the current FADP. However, it is still recommended that a legal analysis be conducted prior to implementing new data processing activities that might not be compliant with the FADP.

11. **Do the laws in your jurisdiction require appointment of a data protection officer, or other person to be in charge of privacy or data protection at the organization? What are the data protection officer's legal responsibilities?**

    The appointment of an official data protection officer is optional. Often a data protection officer is appointed in order to avoid the notification of data files (see art. 11a para. 5 lit. e FADP).

If appointed, the responsibilities are set out in art. 12b of the Ordinance to the FADP. The data protection officer has the following duties:

- he audits the processing of personal data and recommends corrective measures if he ascertains that the data protection regulations have been infringed.
- he maintains a list of the data files in accordance with art. 11a para. 3 FADP, which are operated by the controller of the data files; this list must be made available to the FDPIC or on request to data subjects.

Art. 12b Ordinance to the FADP further requires that the data protection officer

- acts independently and without instructions from the controller of the data file;
- has the necessary resources; and
- has access to all data files and receives all necessary information.

12. **Do the laws in your jurisdiction require providing notice to individuals of the business' processing activities? If so, please describe these notice requirements (e.g. posting an online privacy notice).**

For "normal" personal data, FADP does not explicitly require a notice to the data subjects. It solely requires that the data collection and data processing must be transparent (see art. 4 para. 4 FADP). Transparency may also derive from the context or the constellation.

Only for the collection of sensitive personal data and personality, profiles an active and comprehensive information is required (see art. 14 FADP).

It is, however, quite common to have data privacy notices in place. This is particularly true if transparency cannot be achieved solely through the context or implicit information. Such data privacy notices are usually posted online. There is no case law regarding the question on whether the information about

offline data collection may be provided in the form of an online data privacy notice, i.e. by referring to the online notice. Depending on the circumstances, it is quite common to include some few data privacy information in offline documents and refer for more detailed information to the data privacy notice on the company website.

13. **Do the laws in your jurisdiction apply directly to service providers that process PII, or do they typically only apply through flow-down contractual requirements from the owners?**

Many obligations in the FADP explicitly address the controller of the data file (for example the right to access or the notification of data files to the FDPIC). Other provisions do not only address the controller of the data file, but any person who processes personal data. This is the case for the general data processing principles (art. 4 et seq. FADP) or the data security obligation (see art. 7 FADP).

Furthermore, art. 10a FADP sets out the following: The processing of personal data may be assigned to third parties by agreement or by law if:

- the data is processed only in the manner permitted for the instructing party itself; and
- it is not prohibited by a statutory or contractual duty of confidentiality.

The instructing party must in particular ensure that the third party guarantees data security.

14. **Do the laws in your jurisdiction require minimum contract terms with service providers or are there any other restrictions**

**relating to the appointment of service providers (e.g. due diligence or privacy and security assessments)?**

FADP does not require any minimum contract terms. There are also no other explicit restrictions relating to the appointment of service providers. However, the controller of the data file remains liable for data protection infringements by the service provider. It has therefore an interest in diligently selecting service providers and in monitoring the behavior of the service provider.

15. **Is the transfer of PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (for example, does cross-border transfer of PII require notification to or authorization form a regulator?)**

Data transfers abroad are governed by art. 6 FADP. The mechanism is identical to the one in the GDPR:

- Data transfers to countries with adequate data protection laws in place are permitted without further safeguards (art. 6 para. 1 FADP). FDPIC has published a country list (see here).
- For data transfers to countries without adequate data protection laws additional safeguards are required. Art. 6 para. 2 FADP contains a list with accepted safeguards. As obtaining consent from all data subjects is often not a viable option, the most common safeguards are either contractual safeguards accepted by the FDPIC – currently the FDPIC accepts its own template outsourcing agreement or the EU standard clauses –, or corporate binding rules.
- In case that companies use contractual safeguards or corporate binding rules, they must inform the FDPIC about that use. In the case of the use of the template outsourcing agreement of the FDPIC or the EU standard clauses, the companies must solely inform the FDPIC once that they use them for any data transfer abroad. However, the respective templates must be used without any modifications. In all other cases, copies of the contracts must be sent to the FDPIC for review.

16. **What security obligations are imposed on PII owners and on service providers, if any, in your jurisdiction?**

Art. 7 FADP sets out that personal data must be protected against unauthorised processing through adequate technical and organisational measures. Switzerland has chosen a risk-based approach, i.e. it did not specify the necessary security measures.

Art. 8 of the Ordinance to the FADP sets out that the technical and organisational measures must be adequate. In particular, they must take account of the following criteria:

- the purpose of the data processing;
- the nature and extent of the data processing;
- an assessment of the possible risks to the data subjects;
- the current state of the art.

It further requires that the measures must be periodically reviewed.

More specifically, art. 9 of the Ordinance to the FADP requires the following kind of measures:

- Entrance Control: Unauthorised persons must be denied access to facilities in which personal data is being processed;
- Personal Data Carrier Control: Unauthorised persons must be prevented from reading, copying, altering or removing data carriers;
- Transport Control: On the disclosure of personal data as well as during the transport of data carriers, the unauthorised reading, copying, alteration or deletion of data must be prevented;
- Disclosure Control: Data recipients to whom personal data is disclosed by means of devices for data transmission must be identifiable;
- Storage Control: Unauthorised storage in the memory as well as the unauthorised knowledge, alteration or deletion of stored personal data must be prevented;

- Usage Control: The use by unauthorised persons of automated data processing systems by means of devices for data transmission must be prevented;
- Access Control: The access by authorised persons must be limited to the personal data that they required to fulfilment their task ("need-to-know");
- Input Control: In automated systems, it must be possible to carry out a retrospective examination of what personal data was entered at what time and by which person.

17. **Does your jurisdiction impose requirements of data protection by design or default?**

    Data privacy by design and by default are not explicitly mentioned. However, implicitly FADP requires such policies to a certain degree. Data privacy by default is a consequence of the principle of proportionality and data minimization. Data privacy by design may help to comply with the general data processing principles.

18. **Do the laws in your jurisdiction address security breaches and, if so, how does the law define “security breach”?**

    Security breaches are solely mentioned in art. 7 FADP. Unauthorized access to personal data or involuntary loss or destruction of such data must be avoided.

19. **Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?**

    FADP does not explicitly address the duty to notify the FDPIC or the data

subjects in case of data breaches. Nonetheless, the FDPIC has established in its practice the duty to notify data breaches based on art. 4 para. 2 FADP (data must be processed with good faith). As there is no explicit obligation and as there are no specific criteria on when a notification is appropriate, the data controller has some discretion when considering a notification. It can be reasonable to consult the FDPIC on a no-name basis in tricky cases in order to get additional advise.

As there is no explicit duty to notify the data subjects about data breaches, companies are rather reluctant regarding such notifications. FDPIC recommends that data subjects be notified in cases in which such notification allows the data subjects to minimize damages, for example by blocking credit cards, by changing passwords.

20. **Do the laws in your jurisdiction provide individual rights, such as the right to access and the right to deletion? If so, please provide a general description on what are the rights, how are they communicated, what exceptions exist and any other relevant details.**

**Access / Information Right**

FADP explicitly mentions the right to access in art. 8 et seq. FADP. There is no explicit duty of the controller of the data file to inform the data subjects about this right (for example in the data privacy notice). However, it is quite common to mention the respective right in the data privacy notice. However, irrespective of this common practice, data subjects can find detailed information on the statutory right to access as well as how to exercise this right on the website of the FDPIC. The FDPIC offers on its website also template access requests for the data subjects.

When receiving an access / information request, the controller of the data file must provide the requested information generally within 30 days. The information request is generally free of charge. However, the controller of the data file may ask for reimbursement if the costs connected to the access request are extraordinary, for example because the data subject requests to receive copies of documents and the copying requires substantial time and material.

The controller of the data file must provide the following information:

- all available data concerning the subject in the data file, including the available information on the source of the data;
- the purpose of and if applicable the legal basis for the processing as well as the categories of the personal data processed, the other parties involved with the file and the data recipient.

There are exemptions from the access / information right. The controller of a data file may refuse, restrict or defer the provision of information where:

- a statute so provides;
- this is required to protect the overriding interests of third parties.

The private controller of a data file may further refuse, restrict or defer the provision of information where his own overriding interests so require and he does not disclose the personal data to third parties.

The controller of a data file must indicate the reason why he has refused, restricted or deferred access to information.

A federal body may further refuse, restrict or defer the provision of information where:

- this is required to protect overriding public interests, and in particular the internal or external security of the Confederation;

- the information would jeopardise the outcome of a criminal investigation or any other investigation proceedings.

**Other Individual Rights**

Other individual rights are mentioned in art. 15 FADP. The other individual rights are, in particular:

- Request to block data processing;
- Prohibition to disclose personal data to third parties;
- Request to have personal data corrected;
- Deletion request;
- Where it is impossible to demonstrate that personal data is accurate or inaccurate, the data subject may request that a note to this effect be added to the data.

These other individual rights are, contrary to the access / information right, not further specified.

21. **Are individual rights exercisable through the judicial system or enforced by a regulator or both? When exercisable through the judicial system, does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances? Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury of feelings sufficient?**

The individual rights mentioned in Question 20 are generally enforced by way of a civil litigation. Art. 15 FADP sets outs as follows:

1. Actions relating to protection of privacy are governed by Articles 28, 28a and 28l of the Civil Code. The plaintiff may in particular request that data processing be stopped, that no data be disclosed to third parties, or that the personal data be corrected or destroyed.

2. Where it is impossible to demonstrate that personal data is accurate or inaccurate, the plaintiff may request that a note to this effect be added to the data.
3. The plaintiff may request that notification of third parties or the publication of the correction, destruction, blocking, and in particular the prohibition of disclosure to third parties, the marking of the data as disputed or the court judgment.
4. Actions on the enforcement of a right to information shall be decided by the courts in a simplified procedure under the Civil Procedure Code of 19 December 20083

Data subjects may claim damages. However, Swiss law requires that the plaintiff substantiate the actual damage. This is generally quite difficult as data privacy breaches do often not result in a direct financial damage. As a consequence, it is not that common to ask for a damage.

22. **How are the laws governing privacy and data protection enforced? What is the range of fines and penalties for violation of these laws? Can PII owners appeal to the courts against orders of the regulators?**

Data subjects can only appeal to the courts in the case that they themselves initiate a civil litigation (see above Question 21). In the case of investigations by the FDPIC and subsequent decisions, the data subjects are not anymore party to the proceeding and cannot appeal.

Apart from civil law claims by the data subjects, FADP is generally enforced by the FDPIC. The FDPIC may investigate potential data privacy infringements by its own initiative or based on a complaint by data subjects or third parties. After the investigation the FDPIC renders a recommendation in case that the FADP has been infringed. Recommendation means that he informs the respective data controller about the non-compliance and provides recommendations for curing the respective breaches. In the case that a recommendation is not complied with or rejected, the FDPIC may forward the case to the Federal Administrative Court for a decision. Both, the FDPIC and the data controller may

appeal against the decision of the Federal Administrative Court.

There are some few constellations, in which non-compliance with the FADP is criminally sanctioned, i.e. enforced by the criminal authorities based on complaints by the data subjects or the FDPIC. Art. 34 FADP mentions criminal sanctions in case that the controller of the data file:

- breaches its obligations under art. 8-10 FADP (access / information right) and art. 14 FADP (information duty when collecting sensitive personal data and personality profiles), in that they wilfully provide false or incomplete information; or
- wilfully fails (1) to inform the data subject in accordance with art. 14 para. 1 FADP, or (2) to provide information required under art. 14 para. 2 FADP.

Private persons are further liable to a fine if they wilfully:

- fail to provide information in accordance with art. 6 para. 3 FADP (information of the FDPIC when using contractual safeguards or corporate binding rules for cross-border data transfers) or to declare files in accordance with art. 11a FADP or who in doing so wilfully provide false information; or
- provide the FDPIC with false information in the course of a case investigation or who refuse to cooperate.

Finally, art. 35 FADP sanctions the breach of the data secrecy. It sets out as follows: "Anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality profiles that have come to their knowledge in the course of their professional activities where such activities require the knowledge of such data is, on complaint, liable to a fine. The same penalties apply to anyone who without authorisation wilfully discloses confidential, sensitive personal data or personality profiles that have come to their knowledge in the course of their activities for a person bound by professional confidentiality or in the course of training with such a person.The unauthorised disclosure of confidential, sensitive personal data or personality profiles remains an offence after termination of such professional activities or training."

The fine mentioned above is up to Swiss francs 10’000.00.

23. **Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.**

Pursuant to art. 2 para. 2 FADP, the statute does not apply to:

- personal data that is processed by a natural person exclusively for personal use and which is not disclosed to outsiders;
- deliberations of the Federal Assembly and in parliamentary committees;
- pending civil proceedings, criminal proceedings, international mutual assistance proceedings and proceedings under constitutional or under administrative law, with the exception of administrative proceedings of first instance;
- public registers based on private law;
- personal data processed by the International Committee of the Red Cross.

24. **Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies – how are these terms defined and what restrictions are imposed, if any?**

Monitoring or profiling may, but most not necessarily, result in personality profiles (see art. 3 lit. d FADP). As already mentioned, the requirements for the collection and processing of personality profiles are stricter than the ones for “normal” personal data (see Question 6).

More important, art. 45c lit. b of the Federal Act on Telecommunication Services sets out that processing of data on external equipment by means of transmission using telecommunications techniques is permitted only if users are

informed about the processing and its purpose and are informed that they may refuse to allow processing. This provision applies to the use of cookies.

Regarding the use of cookies Swiss law requires therefore that users are informed about cookies (usually in the privacy notice on the website) and are also informed that they may refuse data collection and processing by cookies. A consent is not needed.

25. **Please describe any laws addressing email communication or direct marketing?**

The collection of e-mail addresses for marketing purposes is governed by the FADP. As the e-mail address is not a sensitive personal data, the FADP does generally not require the consent of the data subject. Furthermore, profiling for marketing purposes is also governed by the FADP (see above Question 24).

The FADP is, however, superseded by art. 3 para. 1 lit. o of the Federal Statute on Unfair Competition with respect to e-mail marketing. It sets out that an individual acts unfair "who sends or causes to be sent mass advertising without a direct link to a requested content by telecommunications, without first obtaining the consent of the customer, indicating the correct sender or indicating a possibility of refusal without any problems and free of charge; anyone who receives contact information from customers when selling goods, works or services and indicates the possibility of refusal does not act unfairly if he sends mass advertising for his own similar goods, works or services to these customers without their consent."

As a general rule, Swiss law requires therefore an informed opt-in for sending e-mail marketing and the recipients must be informed about their right to withdraw at any time. As an exemption, marketing e-mails may be sent to existing customers without an opt-in. However, the sender must have informed

the recipients prior to sending the first marketing e-mail about their withdrawal right. It is not sufficient if the withdrawal right is solely mentioned in the marketing e-mail.

Art. 3 para. 1 lit. o Unfair Competition Act does not specify the format of the consent. It is, however, clear that the consent must be documented as the burden of proof is with the sender. Due to that burden of proof, it is often recommended that a double opt-in be implemented, i.e. the user registers for the newsletter, receives an e-mail with an activation link, and must confirm the registration / consent by using the link.

In case of an infringement of art. 3 para. 1 lit. o Unfair Competition Act, the recipient has two options:

- Civil law proceeding, i.e. he / she can ask the civil court to prohibit the further sending of e-mails. He / she may also ask for damages. However, it might be rather difficult to prove an effective financial damage.
- More common is a criminal complaint with the competent criminal authorities. Intentional infringement of art. 3 para. 1 lit. o Unfair Competition Act is sanctioned with prison of up to three years or a monetary penalty. The sanction will always be a monetary penalty. The penalty amount is dependent on the specific circumstances, i.e. severity of the infringement, first-time infringement vs. repeated infringer, etc.