Data Protection & Privacy

Contributing editor
Wim Nauwelaerts

2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2018

Contributing editor
Wim Nauwelaerts
Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2012
Sixth edition
ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Switzerland

Lukas Morscher and Leo Rusterholz
Lenz & Staehelin

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

Switzerland has dedicated data protection laws. On the federal level the Federal Data Protection Act (DPA) of 19 June 1992, together with its Ordinance (DPO) of 14 June 1993, governs processing of what in Switzerland is called 'personal data' by private parties or federal bodies. Processing of PII by cantonal authorities (cantons are the Swiss states) is subject to state legislation, which will not be discussed here. Additionally, several other federal laws contain provisions on data protection, especially laws that apply in regulated industries (such as financial markets and telecommunications), which further address the collection and processing of PII:

- the Swiss Federal Code of Obligations (Code of Obligations) sets forth restrictions on the processing of employee data, and Ordinance 3 to the Swiss Federal Employment Act (Employment Act) limits the use of surveillance and control systems by the employer;
- the Swiss Federal Telecommunication Act (Telecommunication Act) regulates the use of cookies;
- the Swiss Federal Unfair Competition Act regulates unsolicited mass advertising by means of electronic communications such as email and text messages;
- statutory secrecy obligations, such as banking secrecy (set forth in the Swiss Federal Banking Act (Banking Act)), securities dealer secrecy (set forth in the Swiss Federal Stock Exchange and Securities Dealer Act (Stock Exchange Act), financial market infrastructure secrecy (set forth in the Swiss Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (the Financial Market Infrastructure Act)) and telecommunications secrecy (set forth in the Telecommunication Act) apply in addition to the DPA;
- the Banking Act, the Stock Exchange Act and the Swiss Federal Act on Combating Money Laundering and Terrorist Financing in the Financial Sector stipulate specific duties to disclose information; and
- the Swiss Federal Act regarding Research on Humans, the Swiss Federal Act on Human Genetic Testing and the Swiss Federal Ordinance on Health Insurance set out specific requirements for the processing of health-related data.

Switzerland is a member state to certain international treaties regarding data protection, such as:

- the European Convention on Human Rights and Fundamental Freedoms; and
- the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (Convention ETS 108) and its additional protocol of 8 November 2001.

Although Switzerland is not a member of the EU and, hence, has not implemented the EU Data Protection Directive 95/46/EC, it has been officially recognised by the European Commission as providing an adequate level of protection for data transfers from the EU.

A revision of the DPA (see Update and trends) shall align the DPA with international rules on data protection in order to comply with the upcoming revision of Convention ETS 108 and the EU General Data Protection Regulation 2016/679 (GDPR). This will allow Switzerland to uphold its status as a country adequately protecting personal data from an EU perspective, which allows for easier transfer of personal data from the EU and to ratify Convention ETS 108 of the Council of Europe.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The Federal Data Protection and Information Commissioner (FDPIC) is the federal data protection authority in Switzerland. In addition, cantons are competent to establish their own data protection authorities for the supervision of data processing by cantonal and communal bodies. The FDPIC's contact details are as follows:

Federal Data Protection and Information Commissioner
Feldeggweg 1
3003 Berne
Switzerland
Tel: +41 58 462 43 95
Fax: +41 58 465 99 96
www.edoeb.admin.ch

The FDPIC has no direct enforcement or sanctioning powers against private bodies processing PII. Nevertheless, the FDPIC can carry out investigations on its own initiative or at the request of a third party if methods of processing are capable of violating the privacy of a large number of persons (system errors), if data collections must be registered (see question 23) or if there is a duty to provide information in connection with a cross-border data transfer (see question 32). To this effect, the FDPIC may request documents, make inquiries and attend data processing demonstrations. On the basis of these investigations, the FDPIC may recommend that a certain method of data processing be changed or abandoned. However, these recommendations are not binding. If a recommendation made by the FDPIC is not complied with or is rejected, he or she may refer the matter to the Federal Administrative Court for a decision. The FDPIC has the right to appeal against such decision to the Federal Supreme Court.

The preliminary draft of the revised DPA (see 'Update and trends') foresees that the FDPIC may upon investigation issue binding administrative decisions (instead of recommendations under the current DPA), for example, to modify or terminate unlawful processing.

3 Breaches of data protection

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Violations of the data protection principles (see question 10) are generally not criminally sanctioned. However, private persons are liable to a fine of up to 10,000 Swiss francs if they wilfully:

- fail to provide information with regard to safeguards in the case of cross-border data transfers or to notify data collections or in so doing wilfully provide false information; or
- provide the FDPIC with false information in the course of an investigation or refuse to cooperate.

In addition, the wilful non-compliance with the following duties is, on complaint, punishable by a fine of up to 10,000 Swiss francs:

- the data subject's right of access by refusing to allow access or by providing wrong or incomplete information;
- the duty to inform the data subject on the collection of sensitive PII or personality profiles; and
- the duty of confidentiality of certain professionals to keep sensitive PII and personality profiles.

The preliminary draft of the revised DPA (see 'Update and trends') foresees a fine of up to 500,000 Swiss francs for the wilful breach of the obligations set forth above and further obligations set forth in the DPA. A negligent breach is intended to be sanctioned with a fine of up to 250,000 Swiss francs. Further, wilful breach of professional secrecy shall be punishable by imprisonment of up to three years or monetary penalty. This new sanction will not be limited to the usual bearers of professional secrets (such as banks under article 47 Banking Act, securities dealers under article 43 Stock Exchange Act, financial market infrastructures under article 147 Financial Market Infrastructure Act or attorneys, auditors, doctors, etc, under article 321 Swiss Penal Code) but extend to any profession for which protection of confidentiality is essential.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The DPA does not apply to:

- deliberations of the Federal Parliament and parliamentary committees;
- pending civil proceedings, criminal proceedings, international mutual assistance proceedings and proceedings under constitutional or administrative law, with the exception of administrative proceedings of first instance;
- public registers based on private law;
- PII processed by state and communal bodies (regulated on state level); and
- PII processed by the International Committee of the Red Cross.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The DPA does not cover the interception of communications, electronic marketing or monitoring and surveillance. These issues are dealt with in the following laws:

- the Swiss Federal Telecommunications Act;
- the Swiss Federal Act on Surveillance of Postal Traffic and Telecommunication;
- the Swiss Federal Act on Intelligence Services (scheduled to enter into force in 2017);
- the Swiss Federal Unfair Competition Act;
- the Swiss Federal Code of Obligations; and
- Ordinance 3 to the Employment Act (regarding employee monitoring).

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Additional regulations concerning PII protection can be found in the following laws:

- the Swiss Federal Constitution;
- the Swiss Federal Civil Code;
- the Swiss Federal Act on Consumer Credits;
- various laws and other rules concerning banking (eg, the Anti-Money Laundering Act or the Outsourcing Circular, issued by the Swiss Financial Market Supervisory Authority (FINMA)); and
- various laws concerning health data (eg, the Swiss Federal Electronic Patient Records Act which entered into force on 15 April 2017).

Further regulations may apply depending on the given subject matter.

7 PII formats

What forms of PII are covered by the law?

The DPA and DPO apply to any data relating to an identified or identifiable person (natural persons or legal entity), irrespective of its form. A person is identifiable if a third party having access to the data on the person is able to identify such person with reasonable efforts.

The preliminary draft of the revised DPA (see Update and trends) foresees to remove the protection of personal data relating to legal entities in order to ease cross-border disclosure to jurisdictions that do not protect respective personal data.

8 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The DPA applies to any PII processing that occurs within Switzerland. In addition, if a Swiss court decides on a violation of privacy by the media or other means of public information (eg, the internet), the DPA may apply (even if the violating PII processing occurred outside Switzerland) if the data subject whose privacy was violated chooses Swiss law to be applied. Swiss law may be chosen as the applicable law if:

- the data subject has his or her usual place of residence in Switzerland (provided the violator should have expected the results of the violation to occur in Switzerland);
- the privacy violator has a business establishment or usual place of residence in Switzerland; or
- the result of the violation of privacy occurs in Switzerland (provided the violator should have expected the results of the violation to occur in Switzerland).

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners?

The DPA applies to any processing of PII. 'Processing' is defined in the DPA as any operation with PII irrespective of the means applied and the procedure. In particular, processing includes the collection, storage, use, revision, disclosure, archiving or destruction of PII. An exemption is made for PII that is processed by a natural person exclusively for personal use and is not disclosed to third parties.

Unlike in EU countries, there is no specific distinction between 'owners' of a data collection and mere 'processors'. All persons or entities processing personal data are equally subject to the provisions in the DPA and the DPO and have to adhere to the rules set out therein.

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

PII must always be processed (this includes its holding) lawfully. The processing is lawful if it is either processed in compliance with the

general principles set out in the DPA or non-compliance with these general principles is justified. The disclosure of PII to third parties is generally lawful under the same conditions. The principles set out in the DPA are:

- PII must be processed lawfully;
- the processing must be carried out in good faith and must be proportionate;
- the collection of PII and, in particular, the purpose of its processing, must be evident to the data subject at the time of collection;
- PII may only be processed for the purpose indicated at the time of collection, which is evident from the circumstances, or that is provided for by law;
- anyone who processes PII must ensure it is accurate;
- PII must be protected against unauthorised processing through adequate technical and organisational measures;
- PII must not be transferred outside Switzerland if the privacy of the data subjects would thereby be seriously endangered, in particular due to the absence of legislation that guarantees adequate protection; and
- PII must not be processed against the explicit will of the data subject.

Non-compliance with these principles may be justified by:

- the data subject's consent (given voluntarily and after adequate information);
- the law (eg, duty to disclose information as required under the Banking Act); or
- an overriding private or public interest.

According to the DPA, an overriding interest of the person processing the PII can, in particular, be considered if that person:

- processes PII directly related to the conclusion or the performance of a contract and the PII is that of the contractual party;
- processes PII about competitors without disclosing it to third parties;
- processes PII that is neither sensitive PII nor a personality profile (for these categories, see question 11) in order to verify the creditworthiness of the data subject provided that such data is only disclosed to third parties if it is required for the conclusion or the performance of a contract with the data subject;
- processes PII on a professional basis exclusively for publication in the edited section of a periodically published medium;
- processes PII for purposes not relating to a specific person, in particular for the purposes of research, planning statistics, etc, provided that the results are published in such a manner that the data subject may not be identified; and
- collects PII on a person of public interest, provided the data relates to the public activities of that person.

11 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

In addition to 'normal' PII, the DPA introduced 'sensitive PII' and 'personality profiles' as special categories of PII that are subject to stricter processing conditions. Sensitive PII is data on:

- religious, ideological, political or trade union-related views or activities;
- health, the intimate sphere or the racial origin;
- social security measures; or
- administrative or criminal proceedings and sanctions.

A personality profile is a collection of PII that permits an assessment of essential characteristics of the personality of a natural person.

There are certain restrictions applying to processing sensitive PII and personality profiles in addition to the general principles:

- the reasons that serve as justification to process such data in violation of the general principles are more limited (eg, consent may only be given explicitly, not implicitly);
- disclosure – even if in compliance with the general principles – requires justification; and
- additional requirements depending on the specific case (eg, information duties, obligations to register data collections).

Also, there are more stringent rules in certain subject matters, such as employment law, health, telecommunications, finance, etc. (See questions 5 and 6.)

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Generally, it suffices if the collection of PII and, in particular, the purpose of its processing, is evident to the data subjects from the circumstance of collection. However, in the case of collection of sensitive PII or personality profiles, the owner of such collection is obliged to actively inform the data subject at least of the following:

- the identity of the owner of the data collection;
- the purpose of the data processing; and
- the categories of data recipients if disclosure is intended.

This duty to actively provide information also applies if the data is collected from third parties.

The data subject has to be informed before the PII is collected. If the data is not collected from the data subject, the data subject must be informed at the latest when the data is stored or if the data is not stored, on its first disclosure. The information does not have to be provided in a specific form. For evidentiary purposes, however, the information should be provided in writing or in another recordable form.

The preliminary draft of the revised DPA (see 'Update and trends') foresees that the FDPIC must be notified in case of unlawful processing or loss of personal data (see question 20). The data subject shall also be informed about unlawful processing or loss of personal data if it is necessary to protect his or her privacy or if the FDPIC so requests. Further, the data subject shall be informed about automated decisions (ie, decisions taken solely on the basis of automated data processing) that produce legal effects concerning him or her, and given the opportunity to comment on such decisions and processed PII.

13 Exemption from notification

When is notice not required?

There are certain exceptions to this duty to inform, for example, if providing the information would result in the violation of overriding interests of third parties or if the data collection owner's own overriding interests justify not informing the data subject (in the latter case this exception only applies if the PII is not shared with third parties).

If the PII has not been obtained directly from the data subject, but rather from a third party, the owner of the data collection must, nevertheless, provide the information stated above, except if:

- the data subject has already been informed thereof;
- the storage or disclosure is expressly provided for by law; or
- the provision of information is not possible at all, or only with disproportionate inconvenience or expense.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

See question 34 et seq.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

Anyone who processes PII must ensure that the data is accurate and take all reasonable measures to ensure that PII, which, in view of the purpose of its collection is or has become incorrect or incomplete, is either corrected or destroyed.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Other than the general principle that processing of PII must be proportionate, there are no rules on amount or duration of its holding. According to this principle, processing may only be conducted in so far as it is necessary and fits the purpose for which PII is processed. The same applies to the duration. Accordingly, the permitted amount and duration must be assessed on a case-by-case basis.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

According to the DPA, PII may only be processed for the purpose stated or evident at the time of collection or that is provided for by law.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Use of PII for other purposes than those stated or apparent at the time of collection or provided for by law constitutes a breach of a general principle of the DPA, which is only permissible in the case of appropriate justification (see question 10).

Security

19 Security obligations

What security obligations are imposed on PII owners and service providers that process PII on their behalf?

PII must be protected by appropriate technical and organisational measures against unauthorised processing. Anyone processing PII or providing a data communication network must ensure the protection against unauthorised access, the availability and the integrity of the data. In particular, the PII must be protected against the following risks:

- unauthorised or accidental destruction;
- accidental loss;
- technical faults;
- forgery, theft or unlawful use; and
- unauthorised alteration, copying, access or other unauthorised processing.

The technical and organisational measures must be adequate and must be reviewed periodically. In particular, the following criteria must be taken into account:

- the purpose of the data processing;
- the nature and extent of the data processing;
- an assessment of the possible risks to the data subjects; and
- the current state of the art (especially currently available technology).

In relation to automated data processing, the owner of the data collection must take the appropriate technical and organisational measures to achieve, in particular, the following goals:

- data access control – unauthorised persons must be denied access to facilities in which PII is being processed;
- PII carrier control – preventing unauthorised persons from reading, copying, altering or removing data carriers;
- transport control;
- disclosure control – data recipients to whom PII is disclosed by means of devices for data transmission must be identifiable;
- storage control;
- access control – the access by authorised persons must be limited to the PII that they require to fulfil their task; and
- input control – in automated systems, it must be possible to carry out a retrospective examination of what PII was entered at what time and by which person.

The preliminary draft of the revised DPA (see Update and trends) foresees that appropriate measures shall be taken to avoid breaches of privacy (privacy by design) and data-protection-friendly presets shall be provided (privacy by default).

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

There is no general data security breach notification obligation under Swiss data protection law. As a rule, it would contravene general principles of tort law to provide for an obligation of the violator to proactively inform the damaged person or persons. Nevertheless, the FDPIC has advised lawmakers to oblige providers of social networking sites to inform data subjects of data breaches.

The preliminary draft of the revised DPA (see 'Update and trends') foresees an explicit obligation of data breach notifications (see question 12).

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The appointment of a data protection officer is not mandatory in Switzerland. However, the registration of data collections is not required if the owner of a data collection has appointed a data protection officer that independently monitors data protection compliance within the owner's business organisation and maintains a list of data collections.

The data protection officer must have the necessary knowledge of:

- Swiss data protection law and how it is applied in practice;
- the information technology and technical standards applied by the owner of the data collection; and
- the organisational structure of the owner of the data collection and the particularities of the data processing performed by the owner of the data collection.

The appointment of a data protection officer will only result in a release of the duty to register data collections if the FDPIC is notified of the appointment of a data protection officer. A list of such business organisations who have appointed a data protection officer is publicly accessible on the FDPIC's website.

The data protection officer has two main duties. First, the data protection officer audits the processing of PII within the organisation and recommends corrective measures if he or she finds that the data protection regulations have been violated. He or she must not only assess compliance of the data processing with the data protection requirements on specific occasions, but also periodically. The auditing involves an assessment of whether the processes and systems for data processing fulfil the data protection requirements, and whether these processes and systems are in fact enforced in practice. If the data protection officer takes note of a violation of data protection regulations, he or she must recommend corrective measures to the responsible persons within the organisation and advise them on how to avoid such violations in the future. The data protection officer does not, however, need to have direct instruction rights.

Second, the data protection officer maintains a list of the data collections that would be subject to registration with the FDPIC. The list must be kept up to date. Unlike the data collections registered with the FDPIC, the internal data collections do not have to be maintained electronically nor must they be available online. However, they must be made available on request to the FDPIC and to data subjects.

The data protection officer must:

- carry out his or her duties independently and without instructions from the owner of the data collections;
- have the resources required to fulfil his or her duties; and
- have access to all data collections and all data processing, as well as to all information that he or she requires to fulfil his or her duties.

There is no particular protection against dismissal of the data protection officer. The data protection officer can be an employee of the data controller or an external person.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

Although the owner of a data collection may have to provide available information about the source of collected data (see question 34), there is no obligation to actually keep the according records. However, if such information would be deleted upon receiving an inquiry by a data subject, this could be deemed to be breaching the principle of good faith.

Registration and notification

23 Registration

Are PII owners and/or processors of PII required to register with the supervisory authority? Are there any exemptions?

The owner of a data collection that regularly processes sensitive PII or personality profiles, or regularly discloses PII to third parties, has the obligation to register such data collection with the FDPIC.

A data processor that transfers PII outside Switzerland is, under certain circumstances, obligated to notify the FDPIC of the data protection safeguards put in place.

The owner of a data collection is not required to register a data collection if:

- he or she processes PII owing to a statutory obligation;
- he or she uses the PII exclusively for publication in the edited section of a periodically published medium and does not pass any data to third parties without prior information;
- he or she has designated a data protection officer;
- he or she has acquired a data protection quality mark under a certification procedure; or
- it falls within a list of further exceptions by the Federal Council set out in the DPO, including, among other things:
- data collections of suppliers or customers, provided they do not contain any sensitive PII or personality profiles;
- collections of PII that are used exclusively for research, planning and statistical purposes; and
- accounting records.

24 Formalities

What are the formalities for registration?

In the case of a registration obligation, the collection has to be registered before it is created and the FDPIC has to be informed by the owner of the data collection about:

- his or her name and address;
- the name and complete designation of the data collection;
- the person against whom the right of access may be asserted;
- the purpose of the data collection;
- the categories of PII processed;
- the categories of data recipients; and
- the categories of persons participating in the data collection, namely, third parties who are permitted to enter and modify PII in the data collection.

The owner of the data collection is under the obligation to keep the data collection registration up to date. Online registration is possible at www.datareg.admin.ch. No fees are charged for registration of a data collection.

25 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Private persons are, as owners of a data collection, subject to a fine of up to 10,000 Swiss francs if:

- they wilfully fail to register the data collection;
- they wilfully provide false information in registering the data collection; or
- they wilfully and continuously fail to update the registration information.

The preliminary draft of the revised DPA imposes fines of up to 500,000 Swiss francs in case of breach of any duty under the DPA (such as information, notification and cooperation duties, compliance measures, etc), including the failure to make or maintain an entry on the register. A negligent failure is sanctioned by a fine of up to 250,000 Swiss francs (see question 3 and 'Update and trends').

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Swiss law does not provide for the FDPIC to refuse an entry on the register.

27 Public access

Is the register publicly available? How can it be accessed?

The database of data collections registered with the FDPIC is publicly available and can be accessed by anyone free of charge via the internet at www.datareg.admin.ch. On request, the FDPIC also provides paper extracts free of charge.

28 Effect of registration

Does an entry on the register have any specific legal effect?

Registering a data collection with the FDPIC does not have additional legal effects.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The processing of PII may be transferred to a third party if the transferor ensures that the third party will only process data in a way that the transferor is itself entitled to and if no statutory or contractual secrecy obligations prohibit the processing by third parties. The transferor must ensure that the third party will comply with the applicable data security standards.

Although this is not a statutory requirement, data processing should be outsourced to third parties by written agreement only. Such agreement will typically require the third party to process the PII solely for the purposes of, and only under the instructions of, the transferor.

Special rules may apply in regulated markets. Circular 2008/7 relating to outsourcing issued by the FINMA applies to banks and securities dealers organised under Swiss law, including Swiss branches of foreign banks and securities dealers, which are subject to FINMA supervision. Before outsourcing a significant business area, these institutions must comply with the detailed measures set out in the circular, including:

- mandatory information of bank customers affected by the outsourcing;
- careful selection, instruction and control of the supplier; and
- conclusion of a written contract with the supplier setting out, among other things, the supplier's obligation to comply with professional secrecy rules.

FINMA is currently in the process of revising its Circular 2008/07 and has provided a revised draft thereof for consultation to the public (see Update and trends). The revision encompasses, among others, the removal of any reference to data protection and customer-focused requirements (in particular with respect to comprehensive information duties and the extraordinary termination right, which aspects are now governed by the respective federal acts only).

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

For general requirements regarding disclosing of PII, sensitive PII and personality profiles, see questions 10 and 11. It should be noted that even the communication of PII between companies belonging to the same corporate group is deemed to be disclosure of PII to third parties. Only transmission to an outsourcing provider (see question 29 for requirements) does not constitute such disclosure.

Regularly disclosing information contained in a PII collection entails a registration obligation for such collections.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

PII may only be transferred outside Switzerland if the privacy of the data subject is not seriously endangered, in particular, due to the absence of legislation that guarantees adequate protection in the jurisdiction where the receiving party resides. The FDPIC has published on its website a list of jurisdictions that provide adequate data protection (www.edoeb.admin.ch/themen/00794/00827/index.html?lang=en). The EEA countries and Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, Monaco, New Zealand and Uruguay are generally considered to provide an adequate level of data protection as regards PII of individuals (however, many do not with regard to PII of legal entities), while the laws of all other jurisdictions do not provide adequate data protection.

In the absence of legislation that guarantees adequate protection, PII may only be transferred outside Switzerland if:

- sufficient safeguards, in particular, contractual clauses, ensure an adequate level of protection abroad (see below for details);
- the data subject has consented in the specific case;
- the processing is directly connected with the conclusion or the performance of a contract and the PII is that of a contractual party;
- disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
- disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject;
- the data subject has made the PII generally accessible and has not expressly prohibited its processing; or
- disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules (ie, binding corporate rules) that ensure an adequate level of protection (see below for details).

Data transfer agreements or data transfer clauses are regularly used in practice. It is the responsibility of the data transferor to ensure that an agreement is concluded that sufficiently protects the rights of the data subjects. The data transferor is free to decide whether or not to make use of a standard form. The FDPIC provides a model data transfer agreement (owner of a data collection to a data processor), which can be accessed on its website. The model data transfer agreement is based on Swiss law and reflects to a large extent the standard contractual clauses of the European Commission for data transfers. Further, the FDPIC has pre-approved the European Commission's standard contractual clauses for data transfers and the model contract of the Council of Europe as safeguards, which provide adequate data protection, although it is unclear whether they must be adapted to also cover PII of legal entities and the protection of personality profiles.

An acceptable method for ensuring adequate data protection abroad are binding corporate rules (BCRs) that sufficiently ensure data protection in cross-border data flows within the same legal person or company or between legal persons or companies that are under the same management. The owner of the data collection must notify the BCRs to the FDPIC. BCRs should address at a minimum the elements covered by the model data transfer agreement provided by the FDPIC.

The preliminary draft of the revised DPA (see 'Update and trends') foresees BCRs to be approved (not only notified to the FDPIC).

The US–Swiss Safe Harbor Framework, established in 2009, was considered to provide adequate protection for the transfer of personal data from Switzerland to the US. In its decision of 6 October 2015 the CJEU held that the US-EU Safe Harbor Framework does not provide adequate protection for the transfer of personal data abroad. Even though that decision only concerns the US–EU Safe Harbor Framework and is not directly applicable to Switzerland, the FDPIC declared that the US-Swiss Safe Harbor Framework can no longer be considered to provide adequate protection.

In February 2017, Switzerland and the US agreed on a new framework for the transfer of personal data from Switzerland to the US called the Swiss-US Privacy Shield, thereby replacing the US-Swiss Safe Harbor Framework. US companies processing personal data may self-certify to the Swiss-US Privacy Shield with the US Department of Commerce and thus publicly commit to comply with the new framework. Switzerland acknowledges that the level of protection of personal data for such certified US companies is adequate. As a result, Swiss companies are able to transfer personal data to those US business partners without the need to procure the consent of each data subject or to put additional measures in place.

32 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

As stated in question 31, PII may be transferred outside Switzerland to a jurisdiction that does not provide for adequate data protection based on safeguards that ensure adequate protection such as contractual clauses or binding corporate rules; however, the FDPIC must be notified of such safeguards. The FDPIC may, during a period of 30 days, review the safeguards, though the data transferor does not have to wait for the result of the FDPIC's review or obtain approval. Moreover, if PII is transferred outside Switzerland on the basis of safeguards that have been pre-approved by the FDPIC (eg, the model data transfer agreement issued by him or her), the FDPIC only has to be informed about the fact that such safeguards form the basis of the data transfers.

The preliminary draft of the revised DPA (see 'Update and trends') foresees an extension of the review period from 30 days to six months.

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

In the case of service providers, onwards transfer is only permissible under the same conditions as the initial transfer abroad, otherwise, the owner of the data collection in Switzerland may be breaching DPA provisions. Accordingly, when transferring data abroad under a data transfer agreement, this point should be addressed explicitly (like, eg, the FDPIC's model data transfer agreement does).

Rights of individuals

34 Access

Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Any data subject may request information from the owner of a data collection as to whether PII concerning him or her is being processed (right of access). If this is the case, the data subject has the right to be informed about:

- all available PII in the data collection concerning the data subject, including available information on the source of the data;
- the purpose and, if applicable, the legal basis of the processing;
- categories of PII processed;
- other parties involved with the data collection; and
- the recipients of the PII.

The owner of a data collection must generally comply with requests by a data subject and provide the requested information in writing within 30 days of the receipt of the request. If it is not possible to provide the information within such time period, the owner of the data collection must inform the data subject of the time period during which the information will be provided.

Moreover, a request may be refused, restricted or delayed if:

- a formal law so provides;
- it is required to protect the overriding interests of third parties; or
- it is required to protect an overriding interest of the owner of the data collection, provided that the PII is not shared with third parties.

An access request must usually be processed free of charge. As an exception, the owner of the data collection may ask for an appropriate share of the costs incurred if:

- the data subject has already been provided with the requested information in the 12 months prior to the request and no legitimate interest in the repeated provision of information can be shown,

whereby, in particular, a modification of the PII without notice to the data subject constitutes a legitimate interest; or
- the provision of information entails an exceptionally large amount of work.

The share of the costs may not exceed 300 Swiss francs. The data subject must be notified of the share of the costs before the information is provided and may withdraw its request within 10 days.

35 Other rights

Do individuals have other substantive rights?

The DPA further provides for the following rights for data subjects:
- right of rectification;
- right of erasure; and
- right to object to the processing or disclosure of PII.

Further, if it is impossible to demonstrate whether PII is accurate or inaccurate, the data subject may also request the entry of a suitable remark to be added to the particular piece of information or data.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Violations of the DPA may be asserted by the data subject in a civil action against the violator. The data subject may file claims for damages and reparation for moral damages or for the surrender of profits based on the violation of his or her privacy and may request that the rectification or destruction of the PII or the judgment be notified to third parties or be published.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

In the case of breach, a data subject needs to exercise these rights by itself through civil action. The FDPIC does not have the authority to enforce such individual rights by him or herself (see question 2 for details on the FDPIC's competences).

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The most important derogations, exclusions and limitations have been mentioned above. As previously stated, depending on the subject matter, there may be additional regulations applicable that can have significant impact on the general data protection rules, adding to them, modifying them or even exempting them from application.

Supervision

39 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

The FDPIC's recommendations are non-binding, hence, there is no need for them to be reviewed by a judicial body. The verdicts of the Federal Administrative Court, which may ensue when the owner of a data collection refuses to follow such recommendation (see question 2), on the other hand, are appealable to the Federal Supreme Court both by the FDPIC as well as the defendant.

Update and trends

The DPA is currently being revised. Changes are in particular expected in the area of information, documentation and notification obligations, automated decisions and criminal penalties. The consultation ended on 4 April 2017. The consultation report is pending and the wording of the new DPA is still subject to change. A final version of the revised DPA is not expected to enter into force before 2018.

FINMA is currently in the process of revising its Circular 2008/7 and has provided a revised draft thereof for consultation to the public. The revision encompasses, among others, the removal of any reference to data protection and customer-focused requirements, the abolition of facilitated intragroup outsourcings, new requirements regarding systemically important banks, and the introduction of an explicit obligation to keep an inventory of all outsourced services and to ensure accessibility in Switzerland at all times of any data necessary in the event of restructuring, resolution and liquidation. The consultation ended on 31 January 2017, and the revised circular was expected to enter into force on 1 July 2017. However, the consultation report has not yet been released and therefore the detailed wording remains subject to change. In consequence, the circular could not enter into force as early as originally anticipated but will in due course.

Specific data processing

40 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The use of cookies is generally permissible, provided that the operator of the website (or other online service), which installs the cookie on the user's computer (or other device) informs the user about:
- the use of cookies;
- the purpose of the use; and
- the user's right to refuse cookies.

There is no statutory requirement or judicial practice concerning form, but prevailing opinion considers such information to be sufficient if it is placed on a data protection or a questions and answers sub-page or similar. The cookie banners or pop-ups, which are often seen on websites of other European countries nowadays, seem to be dispensable, although this has not yet been subject to judicial review.

41 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

In 2007, Switzerland adopted a full consent opt-in regime with respect to unsolicited mass advertisement by means of telecommunications (eg, email, SMS/MMS, fax or automated telephone calls). Pursuant to this law, the sender of an unsolicited electronic mass advertisement must seek the concerned recipient's prior consent to receive such mass advertisement and indicate in the advertisement the sender's correct contact information and a cost- and problem-free method to refuse further advertising. If a supplier collects PII relating to his or her customer in connection with a sales transaction, the supplier may use such data for mass advertisement for similar products or services if the customer has been given the option to refuse such advertisement (opt out) at the time of sale. The law does not specify for how long the supplier may use such customer data obtained through a sales transaction for mass advertisement. A period of about one year from the time of sale seems adequate.

42 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

There are no rules specifically applicable to cloud services. In general, personal data must be protected by appropriate technical and organisational measures against unauthorised processing regardless of where it is stored. Anyone processing personal data must ensure its protection against unauthorised access, its availability and its integrity (see question 19). Further, the use of cloud services constitutes an

outsourced processing service if the personal data is not encrypted during its storage in the cloud (for requirements in this regard, see question 29 et seqq) and, in case the servers of the cloud are located outside Switzerland and the personal data is not encrypted during its transfer and storage, an international transfer of personal data (for requirements in this regard, see question 31 et seq). Additionally, the FDPIC has issued a non-binding guide outlining the general risks and data protection requirements of using cloud services (www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=en).

LENZ & STAEHELIN

Lukas Morscher **lukas.morscher@lenzstaehelin.com**
Leo Rusterholz **leo.rusterholz@lenzstaehelin.com**

Brandschenkestrasse 24
8027 Zurich
Switzerland

Tel: +41 58 450 80 00
Fax: +41 58 450 80 01
www.lenzstaehelin.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Commercial Contracts
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law