DATA PROTECTION & PRIVACY

Switzerland

LEXOLOGY
Getting The Deal Through

Consulting editor
Hunton Andrews Kurth LLP

Data Protection & Privacy

Consulting editors

Aaron P Simpson, Lisa J Sotto

Hunton Andrews Kurth LLP

Quick reference guide enabling side-by-side comparison of local insights into the legislative framework; relevant authorities; treatment of breaches; legitimate processing; data handling responsibilities of PII owners; security obligations; internal controls, including the data protection officer; registration formalities transfer and disclosure of PII; rights of individuals; judicial supervision; specific data processing use cases such as cookies, electronic communications marketing, and cloud services; and recent trends.

Generated 17 July 2023

Table of contents

Contributors

Switzerland

Lukas Morscher
lukas.morscher@lenzstaehelin.com
Lenz & Staehelin

Leo Rusterholz
leo.rusterholz@lenzstaehelin.com
Lenz & Staehelin

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

Switzerland has dedicated data protection laws. At federal level, the Federal Data Protection Act (DPA), together with the Ordinance to the DPA (DPO), governs the processing of what in Switzerland is called 'personal data' (PI) by private parties or federal bodies. Processing of PI 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 (eg, financial markets and telecommunications), which further address the collection and processing of PI:

- the Swiss Code of Obligations sets forth restrictions on the processing of employee data, and Ordinance 3 to the Federal Employment Act limits the use of surveillance and control systems by the employer;
- the Telecommunications Act regulates the use of cookies;
- the Federal Unfair Competition Act regulates unsolicited mass advertising through electronic communications such as email and text messages;
- statutory secrecy obligations, such as banking secrecy (outlined in the Federal Banking Act (the Banking Act)), financial institutions secrecy (outlined in the Federal Act on Financial Institutions (the Financial Institutions Act)), financial market infrastructure secrecy (outlined in the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (the Financial Market Infrastructure Act)) and telecommunications secrecy (outlined in the Telecommunication Act) apply in addition to the DPA;
- in the financial industry, the Banking Act, the Financial Institutions Act, the Financial Market Infrastructure Act and the Federal Act on Combating Money Laundering and Terrorist Financing stipulate specific duties to retain and disclose information;
- in the telecommunications industry, the Federal Act on the Surveillance of Post and Telecommunications stipulates specific duties to retain and disclose information; and
- the Federal Act on Research involving Human Beings (and the corresponding ordinance), the Federal Act on Human Genetic Testing (and the corresponding ordinance), the Federal Act on Electronic Patient Records (and the corresponding ordinance), the Federal Act on Medicinal Products and Medical Devices, the Federal Act on Controlling Communicable Human Diseases and the Federal Act on Registration of Cancer Diseases set out specific requirements for the processing of health-related data.

Switzerland is a signatory 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 108) and its additional protocol of 8 November 2001.

Although Switzerland is not a member of the European Union and, hence, is not directly subject to EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), it has been officially recognised by the European Commission as providing an adequate level of protection for data transfers from the European Union.

The revised DPA, which was already adopted by the Swiss parliament in September 2020 and will enter into force on 1 September 2023, aligns Swiss data protection law with international rules on data protection to comply with the revised

Convention 108 and the GDPR. This will hopefully allow Switzerland to uphold its status as a country adequately protecting PI from an EU perspective, which allows for easier transfer of PI from the European Union and the ratification of the revised Convention 108.

The revised DPO, implementing and specifying the provisions of the revised DPA, will enter into force together with the revised DPA.

Law stated - 31 May 2023

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Federal Data Protection and Information Commissioner (FDPIC) is the federal data protection authority in Switzerland. Also, cantons are competent to establish their own data protection authorities for the supervision of data processing by cantonal and communal bodies.

The FDPIC has no direct enforcement or sanctioning powers against private bodies processing PI. 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 (eg, system errors), if data collections must be registered or if there is a duty to provide information in connection with a cross-border data transfer. To this effect, the FDPIC may request documents, make inquiries and attend data processing demonstrations. Based on these investigations, the FDPIC may recommend that a certain method of data processing be changed or abandoned. However, these recommendations are not binding.

Under the revised DPA, the FDPIC initiates, ex officio or upon notification, an investigation if there are sufficient indications that specific data processing activities could violate data protection rules (unless such violation is of minor significance), and should such investigation reveal a violation, render binding administrative measures, including that:

- processing is fully or partially adjusted, suspended or terminated;
- PI is fully or partially deleted or destroyed; and
- in certain cases, disclosure abroad is deferred or prohibited.

In contrast to most other European data protection authorities, the FDPIC still cannot impose any (administrative) fines.

Law stated - 31 May 2023

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The FDPIC may cooperate with domestic and foreign data protection authorities. This includes a general professional exchange with such authorities related to certain specialist areas or regular cooperation within committees, working groups, conferences, etc. However, the FDPIC does not have a mandate or competence to collaborate with other data protection authorities (whether domestic or foreign) concerning supervision and control of processing activities or to share information with them. A collaboration of the FDPIC with foreign data protection authorities concerning data processing in specific cases may (except for data processing related to judicial and police cooperation or Schengen law respectively) be particularly difficult, as in general, the ordinary course of international judicial assistance must be

followed (subject to applicable specific laws).

Under the revised DPA, federal and cantonal authorities must provide the FDPIC with the information and PI required for the performance of his or her statutory duties. The FDPIC discloses information and PI required for the performance of the statutory duties of:

- Swiss authorities responsible for data protection;
- competent criminal prosecution authorities, in certain instances; or
- federal authorities as well as cantonal and communal police forces for the enforcement of certain data protection related measures.

Further, under the revised DPA, the FDPIC may exchange information and PI with foreign competent data protection authorities for the performance of their respective statutory data protection duties, if:

- reciprocity of administrative assistance is ensured;
- information and PI are only used for the data protection related proceedings forming the basis of the request for administrative assistance;
- the receiving authority undertakes to keep professional, business and manufacturing secrets confidential;
- information and PI are only disclosed to third parties with the transmitting authority's prior approval; and
- the receiving authority undertakes to adhere to the conditions and restrictions imposed by the transmitting authority.

Law stated - 31 May 2023

Breaches of data protection law

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 are generally not criminally sanctioned. However, private parties are liable to a fine of up to 10,000 Swiss francs if he or she wilfully:

- fails to provide information concerning safeguards in the case of cross-border data transfers;
- fails to notify data collections;
- provides information concerning safeguards or notification of data collections and in doing so wilfully provides false information; or
- provides the FDPIC with false information in the course of an investigation or refuses to cooperate.

Also, wilfully carrying out the following actions is punishable by a fine of up to 10,000 Swiss francs upon a complaint:

- refusing to permit a data subject access to their PI or providing him or her with wrong or incomplete information (ie, violating the data subject's right of access);
- failing to inform a data subject about the collection of sensitive PI or personality profiles; and
- failure by certain professionals to keep sensitive PI and personality profiles confidential.

Under the revised DPA, the wilful violations set out above (and many further violations) are subject to a fine of up to

250,000 Swiss francs. Further, professional secrecy will not be limited to the usual bearers of professional secrets but will arguably extend to any profession for which protection of confidentiality of 'secret' PI is essential. Violations of the data protection principles, however, are still not criminally sanctioned.

Law stated - 31 May 2023

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

The FDPIC can carry out investigations under certain circumstances and, based thereon, issue recommendations that are non-binding; hence, there is no need for them to be reviewed by a judicial body. If a recommendation made by the FDPIC is not complied with or is rejected, the FDPIC may refer the matter to the Federal Administrative Court for a decision. The verdicts of the Federal Administrative Court are appealable to the Federal Supreme Court (for a final ruling) both by the FDPIC and the defendant.

Under the revised DPA, the FDPIC may, following an investigation revealing a violation of data protection rules, render binding administrative measures (ie, decisions or orders). The FDPIC's investigative proceedings and subsequent decisions or orders are governed by the Federal Act on Administrative Procedure. Only the federal body or private party against whom the investigations were initiated (but not the data subjects concerned) is a party to such proceedings. The FDPIC (and the federal body or private party) may, however, appeal against the Federal Administrative Court's appeal decision to the Federal Supreme Court for a final ruling.

Law stated - 31 May 2023

SCOPE

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 Federal Data Protection Act (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, except for administrative proceedings of first instance;
- public registers based on private law;
- personal information (PI) processed by state and communal bodies (regulated on the state level); and
- PI processed by the International Committee of the Red Cross.

Law stated - 31 May 2023

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

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 Telecommunications Act;
- the Federal Act on Surveillance of Post and Telecommunications;
- the Federal Act on the Intelligence Service;
- the Federal Unfair Competition Act;
- the Swiss Code of Obligations; and
- Ordinance 3 to the Federal Employment Act, regarding employee monitoring.

Law stated - 31 May 2023

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

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

- the Federal Constitution of the Swiss Confederation;
- the Swiss Civil Code;
- the Federal Act on Consumer Credits;
- Ordinance 3 to the Federal Employment Act (regarding employee monitoring);
- various laws, ordinances and other rules concerning data processing in the financial industry; and
- various laws and ordinances concerning the processing of health data.

Further regulations may apply depending on the given subject matter.

Law stated - 31 May 2023

PI formats

What categories and types of PI are covered by the law?

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

Under the revised DPA, the protection of PI relating to legal entities is removed to ease cross-border disclosure to jurisdictions that do not protect respective PI.

Law stated - 31 May 2023

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The DPA applies to any PI processing that occurs within Switzerland. Also, 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 PI 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).

The revised DPA explicitly states that it applies to facts that have an effect in Switzerland, even if they occur outside Switzerland, and that civil law claims are governed by the Federal Act on International Private Law (subject to any provisions on the territorial scope of the Swiss Criminal Code).

Further, under the revised DPA, controllers with domicile (or residence) abroad must designate a representative in Switzerland if they process PI of persons in Switzerland and such data processing:

- is related to the offering of goods or services or to the monitoring of their behaviour;
- is extensive;
- occurs regularly; and
- involves a high risk to the personality of the data subjects.

Law stated - 31 May 2023

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The DPA applies to any processing of PI. 'Processing' is defined in the DPA as any operation with PI irrespective of the means applied and the procedure. In particular, processing includes the collection, storage, use, revision, disclosure, archiving or destruction of PI. An exemption is made for PI that is processed by an individual 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 (ie, controllers) and mere processors. All persons or entities processing PI are equally subject to the provisions in the DPA and the DPO and have to adhere to the rules set out therein.

The revised DPA introduces a distinction between controllers and processors and attributes duties and responsibilities to each of them separately.

Law stated - 31 May 2023

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

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

Personal information (PI) 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 Federal Data Protection Act (DPA) or non-compliance with these general principles is justified. The disclosure of PI to third parties is generally lawful under the

same conditions. The principles set out in the DPA are:

- PI must be processed lawfully;
- the processing must be carried out in good faith and must be proportionate;
- the collection of PI and, in particular, the purpose of its processing, must be evident to the data subject at the time of collection;
- PI 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 PI must ensure it is accurate;
- PI must be protected against unauthorised processing through adequate technical and organisational measures;
- PI 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
- PI 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 financial market laws); or
- an overriding private or public interest.

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

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

Under the revised DPA (and in contrast to EU Regulation (EU) 2016/679 (the General Data Protection Regulation)), such general concept will not change, ie, processing under the general data processing principles generally remains permitted. A justification (eg, consent or overriding interests) is only required in the case PI is processed contrary to the general data processing principles.

Law stated - 31 May 2023

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

In addition to 'normal' PI, the DPA introduced 'sensitive PI' and 'personality profiles' as special categories of PI that are subject to stricter processing conditions. Sensitive PI 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 PI that permits an assessment of essential characteristics of the personality of an individual.

Certain restrictions apply to the processing of sensitive PI 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 and such like.

Under the revised DPA, genetic data and biometric data (which unequivocally identify an individual) are added to the definition of sensitive PI. Further, extensive processing of sensitive PI is determined to be likely to lead to a high risk to an individual's personality or fundamental rights and thus, requires the performance of a data protection impact assessment.

The revised DPA no longer features personality profiles as a special category of PI. Instead, high-risk profiling (ie, any form of automated PI processing to use such data to assess certain personal aspects relating to an individual that involves a high risk to the personality or fundamental rights of the individual, as it pairs data that enables an assessment of essential aspects of the personality of such individual) requires explicit consent by data subjects concerned.

Under the revised Federal Data Protection Ordinance, controllers and processors must also keep logs when carrying out high-risk profiling or processing sensitive data on a large scale by automated means. The minimum log retention period is one year.

Law stated - 31 May 2023

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Generally, it suffices if the collection of personal information (PI) 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 PI 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 the 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 PI 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 another recordable form.

Under the revised Federal Data Protection Act (DPA), the requirements on transparent information to data subjects are extended significantly (to align them to EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR)) such that active information duties, in general, apply in any instance in which any PI (not just sensitive PI) is processed. In essence, data subjects must (at the time of collection) be informed about the controller's identity and contact information; the purpose of the processing; the identity of recipients (or the categories of recipients) in the case of disclosure to third parties; and the jurisdiction where the data is transferred to and safeguards implemented, as applicable, in the case of cross-border disclosure. Although mostly in line with the GDPR, the revised DPA also requires disclosure of every single jurisdiction where PI is being transferred to. Further, the data subject must be informed about automated individual decisions.

Law stated - 31 May 2023

Exemptions from transparency obligations

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 overriding interests justify not informing the data subject (in the latter case this exception only applies if the PI is not shared with third parties).

If the PI 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.

Similar exceptions apply under the revised DPA.

Law stated - 31 May 2023

Data accuracy

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

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

Law stated - 31 May 2023

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

Other than the general principle that the processing of PI must be proportionate, there are no specific rules on the volume or types of PI that may be collected (at least as regards private parties – special rules apply to federal bodies as regards collection of sensitive PI); however, regular processing of sensitive PI or personality profiles requires registration of the data collection with the Federal Data Protection and Information Commissioner. According to this principle, processing may only be conducted if it is necessary and fits the purpose for which PI is processed. The same applies to the types and volume of PI. Accordingly, the permitted types and volume must be assessed on a case-by-case basis.

Under the revised DPA, PI must be destroyed or anonymised as soon as it is no longer needed for the purpose of the data processing, and extensive processing of sensitive PI requires a data protection impact assessment.

Law stated - 31 May 2023

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Other than the general principle that processing of PI must be proportionate (ie, processing may only be conducted if it is necessary and fits the purpose for which PI is processed), which also applies to the amount and length of time of holding PI, there are no specific rules on the amount or length of time. Accordingly, the permitted amount and length of time of holding PI must be assessed on a case-by-case basis.

Under the revised DPA, PI must be destroyed or anonymised as soon as it is no longer needed for the purpose of the data processing.

Law stated - 31 May 2023

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

According to the DPA, PI may only be processed for the purpose stated or evident at the time of collection or that is provided for by law. The processing purpose must be identifiable to the data subject.

Under the revised DPA, PI may only be obtained for a specific purpose that is identifiable to the data subject and such PI may only be processed in such a manner that is compatible with this purpose.

Use of PI 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. This principle remains unchanged under the revised DPA.

Law stated - 31 May 2023

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

There are no rules on automated decision-making in the DPA.

Under the revised DPA, however, the data subject must be informed about automated individual decisions (ie, any decisions solely based on automated data processing and having legal effects or significantly affecting him or her), whereby the affected individual may generally request to express his or her point of view and have the decision reviewed by a person. The foregoing does not apply if:

- the automated individual decision is directly related to the conclusion or performance of a contract between the controller and the data subject, and the data subject's request is granted; or
- the data subject has expressly consented to the decision being automated.

Law stated - 31 May 2023

SECURITY

Security obligations

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

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

- unauthorised or accidental destruction;
- accidental loss;
- technical faults;
- forgery, theft or unlawful use; and
- the 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 considered:

- 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).

Concerning 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 PI is being processed;
- PI carrier control – preventing unauthorised persons from reading, copying, altering or removing data carriers;
- transport control;
- disclosure control – data recipients to whom PI is disclosed through devices for data transmission must be identifiable;
- storage control;
- access control – the access by authorised persons must be limited to the PI 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 PI was entered at what time and by which person.

The revised Federal Data Protection Act (DPA) provides that the technical and organisational measures must enable controllers and processors to avoid breaches of data security (ie, security breaches leading to unintentional or unlawful losses, deletions, destructions or modifications of PI or disclosure or accessibility of PI to unauthorised persons).

According to the revised Federal Data Protection Ordinance (DPO), controllers and processors must determine the necessary level of protection and implement suitable technical and organisational measures (to be reviewed and adapted, as required) in a risk-based approach, whereby they must consider the types of processed data, purpose, type, extent and circumstances of processing, risks to personality and fundamental rights, current state of the art and implementation costs.

Law stated - 31 May 2023

Notification of data breach

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

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

Special rules may apply in regulated markets (eg, a duty to notify the Swiss Financial Market Supervisory Authority FINMA of data breaches suffered by supervised entities or individuals).

The revised DPA introduces an explicit data breach notification obligation and defines a 'data breach' as a breach of security that results in PI being inadvertently or unlawfully lost, deleted, destroyed, altered or disclosed or made accessible to unauthorised persons. Data breaches that are likely to lead to a high risk to the personality or fundamental rights of the individual concerned must be notified to the FDPIC as quickly as possible. Where necessary for the protection of the individual or if requested by the FDPIC, the controller must also notify the affected individual. Contrary to EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (where data breaches must – where feasible – be notified to the supervisory authority within 72 hours unless the breach is unlikely to result in a risk to the individual's rights and freedoms), the revised DPA does not provide for a firm deadline.

The revised DPO specifies the minimum content of the data breach notification (ie, type of breach; if possible, time and duration, categories of personal data and number of affected data subjects; consequences, including risks, for affected data subjects; measures taken or envisaged to rectify the breach and mitigate the consequences, including risks; and name and contact details of point of contact).

Law stated - 31 May 2023

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Neither the Federal Data Protection Act (DPA) nor the revised DPA provide for any such explicit obligations to implement internal controls to ensure responsibility and accountability or to demonstrate compliance, except in:

- the general data processing obligations, which in various instances entail certain documentation (and, if a data collection must be registered with the FDPIC, include drawing up processing regulations inter alia describing the internal organisation as well as data processing and control procedures);
- the obligation to implement suitable technical and organisational measures to ensure an appropriate level of data security; and
- under the revised DPA – the obligation to implement data processing technically and organisationally in such a manner that the data protection provisions are complied with.

According to the revised Federal Data Protection Ordinance (DPO), controllers and processors must issue (and regularly update) processing regulations for automated data processing, if they process sensitive data on a large scale or carry out high-risk profiling. The regulations must include information on the internal organisation, data processing and control procedures and measures to ensure data security.

Law stated - 31 May 2023

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

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 Federal Data Protection and Information Commissioner (FDPIC) is notified of the appointment of a data protection officer. A list of such business organisations that 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 personal information (PI) 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. 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 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 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 the dismissal of the data protection officer. The data protection officer can be an employee of the data controller or an external person.

Under the revised DPA, to the extent a data protection adviser (who meets certain prerequisites set out in the revised DPA) has been appointed, the consultation of such data protection adviser may substitute the otherwise required consultation of the FDPIC following a data protection impact assessment, as applicable. The controller must notify the FDPIC and publish the contact details of the data protection adviser to benefit from the foregoing. The revised DPO specifies further obligations of the controller with respect to an appointed data protection adviser.

Law stated - 31 May 2023

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Although the owner of a data collection may have to provide available information about the source of collected data to comply with data subjects' right of access, there is no obligation to keep the relevant 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.

The revised DPA introduces a general duty to maintain records of processing activities (which is generally modelled after the corresponding obligation under EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR)) containing all relevant information and at least such information explicitly set out in the revised DPA. Controllers and processors must maintain records of data processing activities under their respective responsibility. Exemptions apply for companies with less than 250 employees in the case of low-risk data processing. The revised DPO specifies that low-risk processing means neither processing of sensitive data on a large scale nor carrying out of

high-risk profiling. In comparison, the GDPR's relief from maintaining data processing records only applies if data is only processed occasionally and no special categories of data or data relating to criminal convictions and offences are processed (at all).

Separately, according to the revised DPO, controllers and processors must keep processing logs and issue processing regulations, if they process sensitive data on a large scale or carry out high-risk profiling.

Law stated - 31 May 2023

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

There are no rules on carrying out risk assessments in the DPA.

Under the revised DPA, however, controllers must perform a data protection impact assessment (DPIA) whenever it appears that an envisaged data processing activity is likely to lead to a high risk to an individual's personality or fundamental rights (eg, in the case of extensive processing of sensitive PI or systematic monitoring of public areas).

The DPIA contains a description of the planned processing, an assessment of the risks to the personality or fundamental rights of the data subject and the protective measures to be taken.

The controller must generally consult with the FDPIC before such processing if the DPIA indicates that the contemplated processing may be of a high-risk nature despite any measures taken (unless a data protection adviser meeting certain statutory requirements has already been consulted).

As per the revised DPO, DPIAs conducted must be retained for at least two years following termination of the respective data processing activity.

Law stated - 31 May 2023

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

In general, PI must be protected against unauthorised processing through adequate technical and organisational measures; however, there is currently no obligation to adopt privacy by design or by default.

The revised DPA introduces the concepts of privacy by design and by default, namely:

- setting up technical and organisational measures to meet data protection regulations and data processing principles from the planning of the processing, which shall be appropriate concerning the state of the art, type and extent of processing and associated risks; and
- ensuring through appropriate predefined settings that data processing is limited to the minimum required by the purpose unless the data subject instructs otherwise.

Law stated - 31 May 2023

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

The owner of a data collection that regularly processes sensitive PI or personality profiles, or regularly discloses personal information (PI) to third parties, must register such data collection with the Federal Data Protection and Information Commissioner (FDPIC).

A data processor that transfers PI outside Switzerland is, under certain circumstances, obliged 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 PI owing to a statutory obligation;
- he or she uses the PI 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 Ordinance to the Federal Data Protection Act, including, among other things:

    - data collections of suppliers or customers, provided they do not contain any sensitive PI or personality profiles;
    - collections of PI that are used exclusively for research, planning and statistical purposes; and
    - accounting records.

In the case of a registration obligation, the collection must be registered before it is created, and the FDPIC must 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 PI 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 PI in the data collection.

The owner of the data collection is under the obligation to keep the data collection registration up to date. Registration is available online. No fees are charged for the registration of a data collection.

Private parties 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.

Under the revised Federal Data Protection Act (DPA), the duty to notify data collections to (and register with) the FDPIC is (at least for private parties) abolished and replaced by the general obligation to keep records of data processing activities and, when sensitive data is processed on a large scale or high-risk profiling is carried out, to keep processing logs and issue processing regulations.

Law stated - 31 May 2023

Other transparency duties

Are there any other public transparency duties?

The database of data collections registered with the FDPIC is publicly available and can be accessed by anyone free of charge online. On request, the FDPIC also provides paper extracts free of charge. Other than the registration of a data collection or the notification to and publication by the FDPIC of the appointment of a data protection officer, as applicable, there are no public transparency duties under Swiss data protection law.

The appointment of a data protection officer results in a release of the duty to register data collections with the FDPIC provided the FDPIC is notified of such an appointment. A list of respective companies and organisations that have appointed a data protection officer is publicly accessible on the FDPIC's website.

The appointment of a data protection adviser under the revised DPA may lead to a release of the duty to consult with the FDPIC following a data protection impact assessment, as applicable, provided the data protection adviser's contact details are notified to the FDPIC and published and such data protection adviser has been consulted. It remains to be seen whether the FDPIC will also make available on its website a list of all companies and organisations that have appointed a data protection adviser under the revised DPA.

Law stated - 31 May 2023

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The processing of personal information (PI) 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 PI solely for the purposes and only under the instructions of the transferor.

Under the revised Federal Data Protection Act (DPA), data subjects must be informed about the identity or categories of recipients in the case of disclosure to third parties. Further, a processor may no longer engage a sub-processor without the prior authorisation of the controller. As per the revised Federal Data Protection Ordinance (DPO), such prior authorisation of sub-processing may be specific or general. In the case of a general authorisation, the processor must inform the controller of contemplated changes in its sub-processors and the controller may object thereto. However, in contrast to EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR), the revised DPA does not prescribe any (minimum) content for a data processing agreement.

Special rules may apply in regulated markets. Circular 2018/03 issued by the Swiss Financial Market Supervisory

Authority FINMA (Outsourcing Circular) applies to banks (including holders of a fintech licence), insurers, reinsurers, securities firms, managers of collective assets with a registered office in Switzerland and Swiss branches of foreign banks, insurers, securities firms and managers of collective assets, as well as fund management companies (with registered office and a head office in Switzerland) and self-managed investment companies with variable capital. Before outsourcing a significant business area, these institutions must comply with detailed requirements (to be applied considering the institutions' size, complexity, structure and risk profile).

Partially consolidated rules on outsourcing also apply to financial institutions governed by the Federal Act on Financial Institutions, including those not subject to the Outsourcing Circular (ie, asset managers and trustees) and financial services providers governed by the Federal Financial Services Act (ie, client advisers and producers and providers of financial instruments), as well as financial market infrastructures governed by the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (ie, stock exchanges, multilateral trading facilities, central counterparties, central securities depositories, trade repositories and payment systems).

Law stated - 31 May 2023

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

Disclosure of PI to third parties must follow the general data processing principles. Non-compliance with such principles must be justified. Disclosure of sensitive PI or personality profiles always requires justification (even if it is conducted in compliance with the general principles).

The communication of PI between companies belonging to the same corporate group is deemed to be a disclosure of PI to third parties.

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

No specific restrictions apply on the selling of PI or sharing of PI for online targeted advertising purposes, subject to the general rules on unsolicited mass advertising.

Under the revised DPA, data subjects must be informed about the identity or categories of recipients in the case of disclosure to third parties.

Law stated - 31 May 2023

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

PI 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 Federal Data Protection and Information Commissioner (FDPIC) has published on its website a list of jurisdictions that provide adequate data protection. The European Economic Area 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 concerning PI of individuals (however, many do not with respect to PI 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, PI may only be transferred outside Switzerland if:

- sufficient safeguards, in particular, contractual clauses, ensure an adequate level of protection abroad;

- 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 PI 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 to protect the life or the physical integrity of the data subject;
- the data subject has made the PI 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.

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 must be notified of such safeguards and may, over a period of 30 days, review the safeguards; although, the data transferor does not have to wait for the result of the FDPIC's review or obtain approval. The FDPIC has pre-approved the European Commission's standard contractual clauses (adopted by the Commission Implementing Decision 2021/914 (EU SCC)) as safeguards, which provide adequate data protection, although they must be adapted to also cover PI of legal entities and further requirements arising out of Swiss data protection law. If PI is transferred based on safeguards that have been pre-approved by the FDPIC, the FDPIC only has to be informed about the fact that such safeguards form the basis of the data transfers (and the safeguards themselves do not need to be filed).

Another 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. The BCRs should address at a minimum the elements covered by the EU SCC.

The cross-border data transfer regime remains largely unchanged under the revised DPA; however, the Federal Council (and no longer the FDPIC) will determine which jurisdictions provide adequate data protection legislation. A list of such jurisdictions is directly appended to the revised DPO. The initial list corresponds to the existing list published by the FDPIC. Further, the duty to notify the FDPIC in the case of cross-border transfer is based on pre-approved standard contractual clauses (SCC) or BCR is removed. However, as per the revised DPO, if data export is based on pre-approved SCC, the exporter must implement appropriate measures to ensure that the importer complies with such SCC. Also, a cross-border transfer may be justified by direct connection to the conclusion or performance of a contract between the controller and a third party in the interest of the data subject (whereas under the current regime, the data subject must be a party to the contract justifying transfer or substituting consent). Consent as a justification has been slightly amended, such that consent must be explicit. As one of the very few rules going beyond the requirements of the GDPR, every jurisdiction to which PI is transferred to and safeguards implemented or exemptions applied, as applicable, must be disclosed to the data subjects (irrespective of whether or not such destination jurisdiction provides for adequate data protection legislation).

Law stated - 31 May 2023

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 (as, for example, the EU SCC does).

Law stated - 31 May 2023

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

No statutory localisation requirements arise from the DPA (or revised DPA). However, special rules as regards localisation may apply in regulated markets. In particular, Circular 2018/03, issued by the Swiss Financial Market Supervisory Authority FINMA (Outsourcing Circular), provides that the data necessary for restructuring or resolving the financial institutions subject to the Outsourcing Circular must at all times be accessible in Switzerland (ie actually be stored or mirrored in Switzerland). Thus, exclusive hosting abroad, even if access at all times is ensured, would not meet this requirement.

Law stated - 31 May 2023

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI 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 personal information (PI) 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 PI 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 PI processed;
- other parties involved with the data collection; and
- the recipients of the PI.

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, the owner of the data collection must inform the data subject of the time 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 PI 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 before the request and no legitimate interest in the repeated provision of information can be shown, whereby, in particular, a modification of the PI 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.

Law stated - 31 May 2023

Other rights

Do individuals have other substantive rights?

The Federal Data Protection Act (DPA) further provides for the following rights for data subjects:

- the right of rectification;
- the right of erasure; and
- the right to object to the processing or disclosure of PI.

Further, if it is impossible to demonstrate whether PI 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.

The revised DPA introduces a general right of data portability (ie, a right to receive own PI in a commonly used electronic format, where the processing is carried out by automated means and based on consent or occurs in direct connection with the conclusion or performance of a contract; and a right to request transfer of such PI to another controller if it does not involve a disproportionate effort).

Law stated - 31 May 2023

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 the surrender of profits based on the violation of his or her privacy and may request that the rectification or destruction of the PI or the judgment be notified to third parties or be published.

Law stated - 31 May 2023

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 Federal Data Protection and Information Commissioner (FDPIC) does not have the authority to enforce such individual rights by him or herself.

Under the revised DPA, the FDPIC's enforcement authority is significantly increased and it may, for example, upon request by a data subject, initiate an investigation and, based thereon, render certain binding administrative measures aimed at the processing operations and to restoring compliance with the data protection provisions (eg, adjustment, suspension or termination of processing, destruction or deletion of PI, and granting of access to PI as requested by the data subject). However, it may not award any monetary damages or compensation or impose any fines or other sanctions.

Law stated - 31 May 2023

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

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

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

Law stated - 31 May 2023

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there 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 another online service), which installs the cookie on the user's computer (or another 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 information page or 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.

Law stated - 31 May 2023

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Switzerland adopted a full consent opt-in regime concerning unsolicited mass advertisement through telecommunications (eg, email, text, multimedia messaging service, fax or automated telephone calls). Under 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 personal information (PI) 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.

Law stated - 31 May 2023

Targeted advertising

Are there any rules on targeted online advertising?

There are no specific rules on targeted online advertising, other than the general rules on unsolicited mass advertisement; however, under the revised Federal Data Protection Act (DPA), such analysis and subsequent advertising may under certain circumstances amount to a high-risk profiling, requiring explicit consent by the data subjects concerned (or even a data protection impact assessment).

Law stated - 31 May 2023

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

There are no specific rules on the use of sensitive PI for marketing purposes, other than the general rules applicable to the processing of sensitive PI.

Law stated - 31 May 2023

Profiling

Are there any rules regarding individual profiling?

Under the revised DPA, high-risk profiling (ie, any form of automated PI processing to use such data to assess certain personal aspects relating to an individual that involves a high risk to the personality or fundamental rights of the individual, as it pairs data that enables an assessment of essential aspects of the personality of such individual) requires explicit consent by the data subjects concerned.

Law stated - 31 May 2023

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

There are no rules specifically applicable to cloud services. In general, PI must be protected by appropriate technical and organisational measures against unauthorised processing regardless of where it is stored. Anyone processing PI must ensure its protection against unauthorised access, its availability and its integrity. Further, the use of cloud services constitutes an outsourced processing service if the PI is not encrypted during its storage in the cloud and, in the case the servers of the cloud are located outside Switzerland and the PI is not encrypted during its transfer and storage, an international transfer of PI. Additionally, the Federal Data Protection and Information Commissioner has published on its website a non-binding guide outlining the general risks and data protection requirements of using cloud services.

Law stated - 31 May 2023

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

In September 2020, the Swiss parliament adopted a revision of the Federal Data Protection Act (DPA). The revised DPA largely follows the regime provided by EU Regulation (EU) 2016/679 (the General Data Protection Regulation) (GDPR) with some reliefs and very limited 'Swiss finishes' (as in rules that go beyond the requirements of the GDPR). The revised DPA should allow Switzerland to uphold its status as a country adequately protecting personal information (PI) from an EU perspective, thereby allowing for easier transfer of PI from the European Union into Switzerland. The revised corresponding Ordinance (DPO), implementing and specifying the provisions of the revised DPA, was adopted by the Swiss Federal Council on 31 August 2022. The revised DPA and revised DPO will enter into force on 1 September 2023.

Law stated - 31 May 2023

Jurisdictions

Australia	Piper Alderman
Austria	Knyrim Trieb Rechtsanwälte
Belgium	Hunton Andrews Kurth LLP
Brazil	Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados
Canada	.
Chile	Magliona Abogados
China	Mayer Brown
France	Aramis Law Firm
Germany	Hoffmann Liebs Fritsch & Partner
Greece	GKP Law Firm
Hong Kong	Mayer Brown
Hungary	VJT & Partners
India	AP & Partners
Indonesia	SSEK Law Firm
Ireland	Walkers
Italy	ICT Legal Consulting
Japan	Nagashima Ohno & Tsunematsu
Jordan	Nsair & Partners - Lawyers
Malaysia	SKRINE
Malta	Fenech & Fenech Advocates
New Zealand	Anderson Lloyd
Pakistan	S.U.Khan Associates Corporate & Legal Consultants
Poland	Kobylanska Lewoszewski Mednis
Portugal	Morais Leitao Galvao Teles Soares da Silva and Associados
Serbia	BDK Advokati

South Africa	Covington & Burling LLP
South Korea	Bae, Kim & Lee LLC
Switzerland	Lenz & Staehelin
Taiwan	Formosa Transnational Attorneys at Law
Thailand	Formichella & Sritawat Attorneys at Law
Turkey	Turunç
United Arab Emirates	Bizilance Legal Consultants
United Kingdom	Hunton Andrews Kurth LLP
USA	Hunton Andrews Kurth LLP