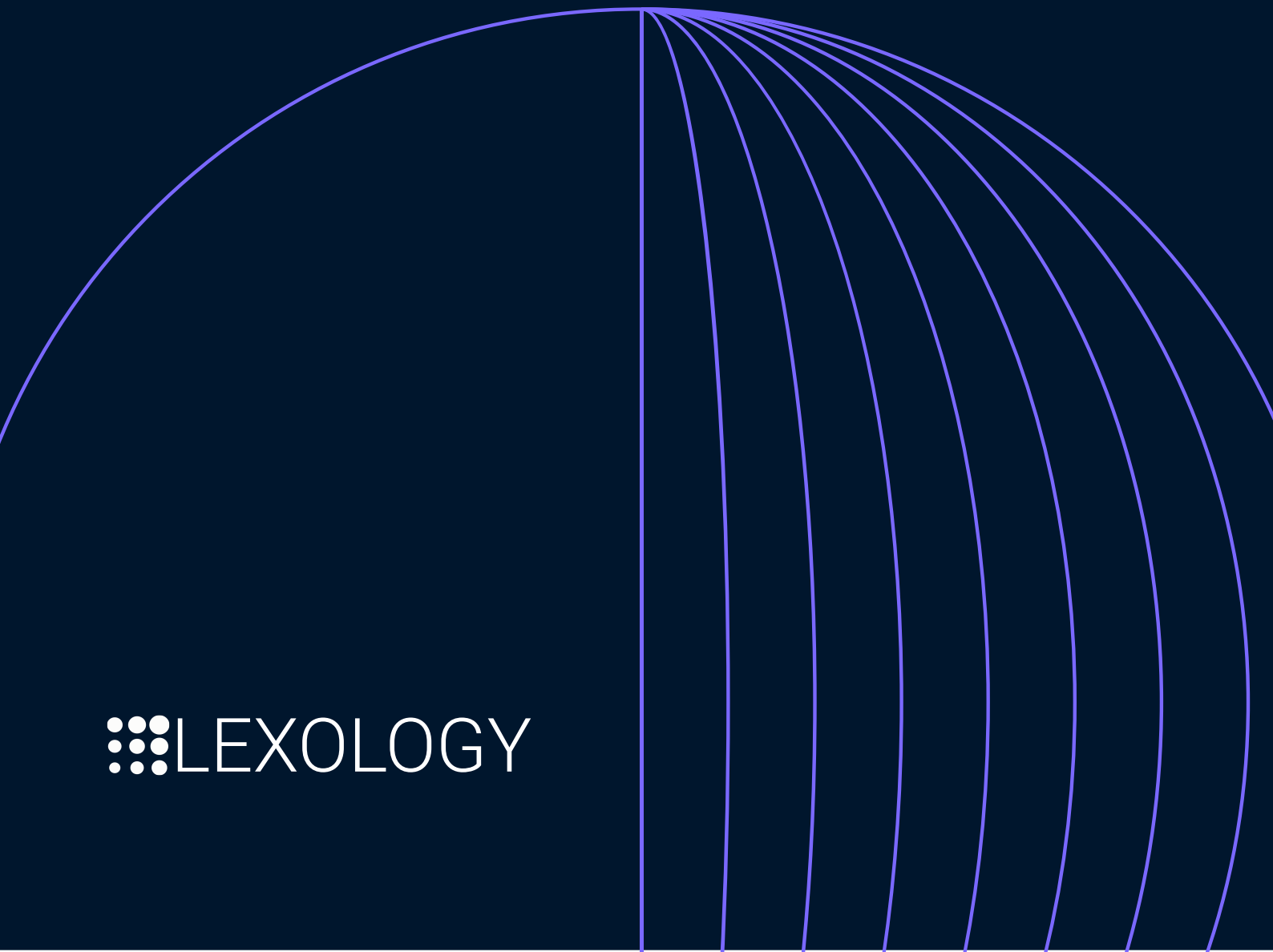
PANORAMIC

DATA PROTECTION & PRIVACY

Switzerland



LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: July 12, 2024

Contents

Data Protection & Privacy

SHARING AND CROSS-BORDER TRANSFERS OF PI

RIGHTS OF INDIVIDUALS

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

SPECIFIC DATA PROCESSING

UPDATE AND TRENDS

Contributors

Switzerland

Lenz & Staehelin

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

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. On 1 September 2023, the substantially revised Federal Data Protection Act (DPA), together with the revised Ordinance to the DPA (DPO), entered into force, which governs the processing of what in Switzerland is called 'personal data' (PI) by private parties or federal bodies. The revision reflects technological advancements and aligns Swiss data protection laws with international data protection standards. 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 Telecommunications 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.

Law stated - 31 Mai 2024

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 the power to initiate, 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 cannot impose any (administrative) fines.

Law stated - 31 Mai 2024

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 DPA contains specific provisions regarding the FDPIC's cooperation with domestic and foreign data protection authorities.

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, 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 Mai 2024

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, as well as, among others, failures to notify data breaches, conduct a data protection impact assessment or maintain a record of processing activities, are generally not criminally sanctioned. However, private parties are criminally liable to a fine of up to 250,000 Swiss francs if they wilfully:

- violate information duties (including the duty to inform on automated individual decision-making) and access rights by providing false or incomplete information;
- fail to inform the data subject in accordance with the information duties (including the duty to inform on automated individual decision-making) or to provide the required information in accordance with the information duties;
- violate the duty to cooperate by providing false information to or refusing to cooperate with the FDPIC in the course of an investigation;
- disclose PI to a jurisdiction not providing for adequate data protection legislation without reliance on any of the statutory safeguards or exemptions;
- engage a processor in violation of statutory or contractual secrecy obligations or the statutory requirements as to the scope of processing or data security;
- fail to comply with the minimum data security requirements set out in the DPO; or
-

disclose secret PI of which they have become aware in the performance of their profession, which requires knowledge of such data, or in the performance of their work for (or training at) a person subject to such secrecy.

The fine is generally imposed on the individual responsible for data processing within a company (not on the legal entity acting as controller or processor), as the sanctions are criminal in nature and not administrative (as in the EEA). This also means that only cantonal law enforcement authorities (rather than the FDPIC) are competent to prosecute such violations. If a fine of no more than 50,000 Swiss francs is envisaged and if the investigation of the individual culprits would require disproportionate investigative measures, the authorities may refrain from prosecuting the individual and order the company to pay the fine.

Law stated - 31 Mai 2024

Judicial review of data protection authority orders

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

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 Mai 2024

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:

- personal information (PI) processed by an individual exclusively for personal use;
- PI processed by the Federal Parliament and parliamentary committees in connection with their deliberations;
- PI processed by institutional beneficiaries under the Host State Act, which enjoy immunity in Switzerland (eg, the International Committee of the Red Cross);
- court proceedings and proceedings governed by federal procedural laws, except for administrative proceedings of first instance;
-

public registers based on private law, in particular the access to these registers and the data subject's rights, which are governed by the special provisions of the applicable federal law, unless such special provisions do not contain any rules related thereto; and

- PI processed by cantonal and communal bodies (regulated at the cantonal level).

Law stated - 31 Mai 2024

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 the Surveillance of Post and Telecommunications;
- the Federal Act on the Intelligence Service;
- the Federal Unfair Competition Act;
- the Swiss Code of Obligations;
- Ordinance 3 to the Federal Employment Act, regarding employee monitoring; and
- the Federal Act on the General Part of Social Security Law, regarding surveillance of social-security benefit claimants.

Law stated - 31 Mai 2024

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 Mai 2024

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 individual, 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.

Law stated - 31 Mai 2024

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 facts that have an effect in Switzerland, even if they occur outside Switzerland (impact principle).

With regard to civil law claims, the Federal Act on Private International Law (PILA) applies. Pursuant to the PILA, 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 also 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).

In addition, any provisions on the territorial scope of the Swiss Criminal Code remain reserved.

Finally, under the 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 Mai 2024

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, recording, storage, use, revision, disclosure, archiving, deletion or destruction of PI.

The DPA distinguishes between the roles of 'controllers' and 'processors' and attributes duties and responsibilities to each of them separately. The term 'controller' refers to private parties or federal bodies that alone or jointly with others decide on the purpose and means of the processing of PI. Processors are private parties or federal bodies that process PI on behalf of the controller.

Law stated - 31 Mai 2024

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. In contrast to the EU Regulation (EU) 2016/679 (the General Data Protection Regulation), the processing of PI by private parties in compliance with the general data processing principles set out in the Federal Data Protection Act (DPA) is generally permitted (only federal bodies require a legal basis for processing). A justification is only required in the case PI is processed contrary to the general data processing principles. Therefore, the processing of PI by private parties is lawful if it is either processed in compliance with the general data processing principles 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;
- PI may only be collected for a specific purpose that is evident to the data subject and such collected PI may only be processed in a manner that is compatible with the original purpose;
- PI must be destroyed or anonymised as soon as it is no longer required for the purpose of the processing;
- anyone who processes PI must ensure it is accurate and take all appropriate measures to correct, delete or destroy data that is incorrect or incomplete with regard to the purpose of collection or processing;
- if the consent of the data subject is required, such consent is only valid if given voluntarily for one or more specific processing instance(s) based on appropriate

information. Consent must be explicit for the processing of sensitive PI, high-risk profiling by a private person or profiling by a federal body;

- controllers and processors must ensure through suitable technical and organisational measures a level of data security appropriate to the risks;
- PI must not be processed against the explicit will of the data subject; and
- sensitive PI must not be disclosed to any third parties.

Non-compliance with these principles may be justified by:

- the data subject's consent (given voluntarily and after appropriate 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 controller or processor can, in particular, be considered if they:

- process PI directly related to the conclusion or the performance of a contract and the PI is that of the contractual party;
- process PI about competitors without disclosing it to third parties, whereby disclosures between group companies are exempted;
- process PI to verify the creditworthiness of the data subject, who is at least 18 years of age, provided that such data is not older than 10 years, only disclosed to third parties if it is required for the conclusion or the performance of a contract with the data subject and neither constitutes sensitive PI nor leads to high-risk profiling;
- process PI on a professional basis exclusively for publication in the edited section of a periodically published medium or the PI serves exclusively as a personal working tool and is not published;
- process PI for purposes not relating to a specific person, in particular, for research, planning and statistics, provided that the PI is anonymised as soon as the purpose of the processing allows for it (or, if anonymisation is impossible or requires disproportionate effort, appropriate measures prevent identification of the data subject), sensitive PI is disclosed to third parties in such a manner that the data subject may not be identified (or, if this is not possible, it is ensured that third parties only process such data for purposes unrelated to the data subject's person), and the results are published in such a manner that the data subject may not be identified; or
- collect PI on a person of public interest, provided the data relates to the public activities of that person.

Law stated - 31 Mai 2024

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 sets forth 'sensitive PI' as a special category of PI and 'high-risk profiling' as a processing activity, which 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 affiliation to a race or ethnicity;
- genetic data;
- biometric data which unequivocally identifies a natural person;
- social security measures; or
- administrative or criminal proceedings and sanctions.

High-risk profiling refers to any form of automated PI processing to use such data to assess certain personal aspects relating to an individual that poses a high risk to the personality or fundamental rights of the individual, as it pairs data that enables an assessment of the essential aspects of the personality of such individual.

Certain restrictions apply to the processing of sensitive PI and high-risk profiling by private parties 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);
- controllers and processors must keep logs (for a minimum retention period of one year) and draw up regulations when carrying out high-risk profiling or processing sensitive PI on a large scale by automated means; and
- additional requirements depending on the specific case (eg, 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).

Further, disclosure of sensitive PI to third parties, even if in compliance with the general processing principles, requires justification.

Additional restrictions on the processing of sensitive PI and profiling apply to federal bodies.

Finally, there are more stringent rules in certain subject matters, such as employment law, health, telecommunications, finance and the like.

Law stated - 31 Mai 2024

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?

Under the Federal Data Protection Act (DPA), the controller is required to appropriately inform the data subjects of the collection of personal information (PI), including if such data is collected from third parties. The controller must provide data subjects, at the time of the collection, with any information that is necessary to exercise his or her rights under the DPA and ensure the transparent processing of PI. At a minimum, data subjects must be informed about:

- the identity and contact information of the controller;
- the contact information of the data protection advisor, if any;
- the identity and contact information of the Swiss representative, if any;
- the purpose of the processing;
- the identity of recipients (or the categories of recipients) in the case of disclosure to third parties;
- the jurisdiction where the data is transferred to and safeguards implemented or exemptions relied on, as applicable, in the case of cross-border disclosure (although mostly in line with the EU Regulation (EU) 2016/679 (the General Data Protection Regulation), the DPA also requires disclosure of every single jurisdiction where PI is being transferred to, irrespective of whether such destination jurisdiction provides for adequate data protection legislation); and
- automated individual decisions, if any.

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.

Law stated - 31 Mai 2024

Exemptions from transparency obligations

When is notice not required?

There are certain exceptions to this duty to inform, in which no or only limited information is required, in particular if:

- the data subject already has the information;
- processing is required by law;
- the controller is a private person bound by a statutory secrecy obligation;
- the controller can rely on certain media privileges;
- informing the data subject is not possible or would require a disproportionate effort in case of indirect collection of PI (ie, the PI has not been obtained directly from the data subject);
- the information defeats the purpose of the processing; or
- providing the information would result in the violation of overriding interests of third parties or the controller's overriding private interests justify not informing the data subject (in the latter case this exception only applies if the PI is not disclosed to third parties, whereby disclosures between group companies are exempted).

In addition, no information on automated individual decisions must be provided to a data subject if:

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

Law stated - 31 Mai 2024

Data accuracy

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

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

Law stated - 31 Mai 2024

Data minimisation

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

Other than the general principles that the processing of PI must be proportionate and that PI must be destroyed or anonymised as soon as it is no longer required for the purpose of the processing, there are generally no specific rules on the types or volume of PI that may be collected (at least as regards private parties – special rules apply to federal bodies as regards the collection of sensitive PI and profiling). However, processing of sensitive PI or high-risk profiling may be subject to certain additional requirements depending on the specific case (eg, to rely on consent as justification, such consent may only be given explicitly; controllers and processors must keep logs and draw up regulations when carrying out high-risk profiling or processing sensitive PI on a large-scale by automated means; extensive processing of sensitive PI is determined to be likely to require the performance of a data protection impact assessment; and disclosure of sensitive PI, even if in compliance with the general principles, requires justification). Accordingly, the permitted types and volume of PI must be assessed on a case-by-case basis.

Law stated - 31 Mai 2024

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 principles that the processing of PI must be proportionate and that PI must be destroyed or anonymised as soon as it is no longer required for the purpose of

the processing, there are no specific rules on the amount or length of time of holding PI. Accordingly, the permitted amount and length of time of holding PI must be assessed on a case-by-case basis.

Law stated - 31 Mai 2024

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 collected for a specific purpose that is evident 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.

Law stated - 31 Mai 2024

Automated decision-making

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

Under the DPA, 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 natural 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 explicitly (and voluntarily based on appropriate information) consented to the decision being automated.

Law stated - 31 Mai 2024

SECURITY

Security obligations

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

Under the Federal Data Protection Act (DPA), controllers and processors must ensure through suitable technical and organisational measures (TOM) a level of data security

appropriate to the risks. Such TOM must enable breaches of data security (ie, security breaches leading to unintentional or unlawful losses, deletions, destructions or modifications of personal information (PI) or disclosure or accessibility of PI to unauthorised persons) to be avoided and are further specified in the Federal Data Protection Ordinance (DPO).

According to the DPO, controllers and processors must:

- determine the extent to which PI must be protected, which must be assessed according to the nature of PI being processed and the purpose, nature, extent and circumstances of the processing; and
- implement suitable TOM appropriate to the risk (for the data subject's personality or fundamental rights), which must be assessed according to the causes of the risk, main threats, measures taken or planned to reduce the risk, and probability and seriousness of a data security breach despite the measures taken or planned.

When determining the TOM, the state of the art and implementation costs must also be considered. The extent to which PI must be protected, the risk as well as the TOM as such must be reviewed throughout the period of processing and the TOM must be adapted, as necessary.

Also, under the DPO, controllers and processors must adopt the TOM to ensure, depending on the extent of protection required, that the data being processed are:

- only accessible to authorised persons (confidentiality);
- available when they are required (availability);
- not altered without authorisation or unintentionally (integrity); and
- processed in a traceable manner (traceability).

Each of the above is further detailed in the DPO.

Law stated - 31 Mai 2024

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?

The DPA sets forth data breach notification obligations 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 by the controller to the Federal Data Protection and Information Commissioner (FDPIC) as quickly as possible (a processor, in turn, is required to inform the controller as quickly as possible). 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 DPA does not provide for a firm deadline.

According to the DPO, the notification to the FDPIC by the controller must contain the following information:

- the nature of the breach;
- if possible, the time and duration as well as the categories and approximate numbers of PI and data subjects concerned;
- the consequences, including risks, for data subjects;
- the measures taken or envisaged to rectify the breach and mitigate the consequences, including risks; and
- the name and contact details of the point of contact.

Where necessary for the protection of the data subject or if requested by the FDPIC, the controller must also notify the affected data subject. Under certain conditions set out in the DPA (eg, statutory secrecy obligations) such notification may be limited, deferred or dispensed with.

In addition, controllers are required to document data breaches, including a description of the facts and effects of the data breach as well as the measures taken, and store such documentation for at least two years from the date of notification to the FDPIC.

Finally, 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).

Law stated - 31 Mai 2024

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?

The Federal Data Protection Act (DPA) does not 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;
- the obligation to implement suitable technical and organisational measures to ensure a level of data security appropriate to the risks;
- the obligation to implement data processing technically and organisationally in such a manner that the data protection provisions are complied with; and
- the obligation to maintain records of processing activities.

Further, according to the Federal Data Protection Ordinance (DPO), controllers and processors must issue (and regularly update) processing regulations for automated data processing if they process sensitive personal information (PI) 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 Mai 2024

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 (except for federal bodies). However, the DPA provides for the possibility of a voluntary appointment of a data protection officer (referred to as 'data protection advisor') by private controllers. By designating a data protection advisor who meets certain prerequisites set out in the DPA, the consultation of such data protection advisor may substitute the otherwise required consultation of the Federal Data Protection and Information Commissioner (FDPIC) following a data protection impact assessment, as applicable. To benefit from the foregoing, the controller must publish the data protection advisor's contact details and notify the FDPIC thereof. A reporting portal for notifying contact details is publicly accessible on the FDPIC's website.

The data protection advisor serves as the contact point for data subjects and the authorities responsible for data protection in Switzerland. Further tasks include, in particular, training and advising the controller in matters of data protection and providing support on applying the data protection regulations.

Further, the data protection advisor must:

- exercise its functions towards the controller in a professionally independent manner and may not be bound by any instructions;
- not carry out any activities that are incompatible with its tasks; and
- have the required expertise.

The DPO specifies further obligations of the controller with respect to the appointment of a data protection advisor.

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

Law stated - 31 Mai 2024

Record-keeping

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

The DPA provides for 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 DPA. Controllers and processors must maintain records of processing activities under their respective responsibility (and only federal bodies are required to file their records of processing activities with the FDPIC). Exemptions apply for companies with fewer than 250 employees in the case of low-risk data processing. The DPO specifies that low-risk processing means neither processing of sensitive PI on a large scale nor the 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 DPO, controllers and processors must keep processing logs and issue processing regulations if they process sensitive PI on a large scale or carry out high-risk profiling by automated means.

Law stated - 31 Mai 2024

Risk assessment

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

Under the DPA, 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). In certain cases set out in the DPA, private controllers are exempt from the obligation to perform a DPIA (eg, if a private controller performs the relevant processing activity based on a statutory obligation).

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 advisor meeting certain statutory requirements has already been consulted).

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

Law stated - 31 Mai 2024

Design of PI processing systems

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

The DPA sets forth 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 Mai 2024

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?

Under the Federal Data Protection Act (DPA), there is no obligation for private parties to notify or register their data processing activities with the Federal Data Protection and Information Commissioner (FDPIC). Only federal bodies are required to file their records of processing activities with the FDPIC, a failure of which, however, entails no penalty.

Law stated - 31 Mai 2024

Other transparency duties

Are there any other public transparency duties?

Other than the publication of the appointment of a data protection advisor, as applicable, there are no public transparency duties under Swiss data protection law for private parties. Only federal bodies are required to file their records of processing activities with the FDPIC, which are publicly available and can be accessed by anyone free of charge on the FDPIC's website.

Law stated - 31 Mai 2024

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?

Under the Federal Data Protection Act (DPA), 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.

In the case of disclosure of PI to third parties, data subjects must be informed about the identity or categories of recipients. Further, a processor may not engage a sub-processor without the prior authorisation of the controller. As per the 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), the 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 a 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 Mai 2024

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 to recipients that are not processors always requires justification (even if it is conducted in compliance with the general principles). Further, data subjects must be informed about the identity or categories of recipients in the case of disclosure to third parties.

The communication of PI between companies belonging to the same corporate group is deemed to be a disclosure of PI to third parties, unless explicitly indicated otherwise for specific provisions in each individual case.

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.

Law stated - 31 Mai 2024

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

PI may only be transferred outside Switzerland if the Federal Council has determined that the legislation of the jurisdiction concerned guarantees an adequate level of protection. The Federal Council's list of jurisdictions that provide adequate data protection is set out in Appendix 1 to the DPO. The European Economic Area countries and Andorra, Argentina, Canada, the Faroe Islands, Gibraltar, Guernsey, the Isle of Man, Israel, Jersey, Monaco, New Zealand, United Kingdom and Uruguay are generally considered to provide an adequate level of data protection concerning PI, while the laws of all other jurisdictions do not provide adequate data protection. As regards transfers of PI to the USA, the Federal Data Protection and Information Commissioner (FDPIC) has taken note of the EU-US Data Privacy Framework, which has been recently negotiated and implemented between the EU and the USA and for which the European Commission adopted its adequacy decision on 10 July 2023. Switzerland and the USA are currently in negotiations regarding a Swiss-US Data Privacy Framework.

In the absence of the above determination by the Federal Council, PI may only be transferred outside Switzerland if an adequate level of data protection is guaranteed by:

- an international treaty;
- data protection clauses in a contract between the controller or the processor and the contractual counterparty, which were notified to the FDPIC in advance;
- specific guarantees prepared by a competent federal body, which were notified to the FDPIC in advance;
- standard contractual clauses previously approved, issued or recognised by the FDPIC; or
- binding corporate rules (BCRs) that were previously approved by either the FDPIC or a foreign competent data protection authority of a jurisdiction that guarantees an adequate level of protection.

In derogation of the above, PI may also be disclosed abroad in the following cases:

- the data subject has explicitly consented to disclosure;
- the processing directly relates to the conclusion or performance of a contract between the controller and the data subject, or between the controller and a third party in the interest of the data subject;
- disclosure is required to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before a court or other competent foreign authority;
- disclosure is necessary to protect the life or the physical integrity of the data subject or a third party and it is not possible to obtain the consent of the data subject within an appropriate period of time;

- the data subject has made the PI generally accessible and has not expressly prohibited its processing; or
- the data originate from a statutory register, which is accessible to the public or to persons with a legitimate interest, provided that the statutory requirements for access are met in the individual case.

The FDPIC has approved the European Commission's standard contractual clauses (adopted by the Commission Implementing Decision 2021/914 (EU SCC)), provided that the necessary adaptations and amendments required under Swiss data protection law are made. Pursuant to the DPO, if PI is transferred based on such approved standard contractual clauses (SCC), the transferor must implement appropriate measures to ensure that the recipient complies with such SCC.

If PI is transferred based on safeguards that have been pre-approved by the FDPIC (eg, approved SCC or BCRs), the FDPIC does not need to be notified about the fact that such safeguards form the basis of the data transfers.

Law stated - 31 Mai 2024

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?

Onwards transfers of PI is only permissible under the same conditions as the initial transfer abroad, otherwise, the controller or processor in Switzerland may be breaching DPA provisions. Further, under the DPA, a processor may not engage a sub-processor without the prior authorisation of the controller (while such prior authorisation may be specific or general, as specified in the DPO). Accordingly, when transferring PI abroad under a data transfer agreement, these points should be addressed explicitly (as, for example, the EU SCC does).

Law stated - 31 Mai 2024

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. 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 Mai 2024

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 controller as to whether personal information (PI) concerning him or her is being processed (right of access), which cannot be waived in advance. If this is the case, the data subject shall receive the information required to assert his or her rights and to ensure transparent data processing. The data subject has the right to be informed about, at least:

- the identity and contact details of the controller;
- the PI being processed;
- the purpose of the processing;
- the retention period or, if not possible, the criteria used to determine such period;
- the information available on the source of the PI, if the controller has not obtained the PI directly from the data subject;
- the existence of automated individual decisions and the logic on which such decisions are based, if any;
- the recipients or categories of recipients of the PI, if any; and
- the jurisdiction where the data is transferred to and safeguards implemented or exemptions relied on, as applicable, in the case of cross-border disclosure, if any.

The controller must generally comply with requests by a data subject and provide the requested information in writing within 30 days of receipt of the request. If it is not possible to provide the information within such time, the controller 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 (eg, statutory secrecy obligations);
- it is required to protect the overriding interests of third parties;
- the request is evidently unfounded, in particular, if the data subject pursues a purpose unrelated to data protection interests or the request is evidently of a frivolous nature; or
- it is required to protect an overriding private interest of the controller, provided that the PI is not shared with third parties, whereby disclosures between group companies are exempted.

An access request must usually be processed free of charge. As an exception, the controller may ask for an appropriate share of the costs incurred if the provision of information entails

disproportionate effort. 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. If the data subject does not confirm the request within 10 days, the request shall be deemed withdrawn without incurring any costs.

Law stated - 31 Mai 2024

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;
- the right to object to the processing or disclosure of PI; and
- the right of data portability (ie, a right to receive their 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).

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.

Law stated - 31 Mai 2024

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 Mai 2024

Enforcement

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

In the case of a breach, a data subject generally needs to exercise these rights by itself through civil action. However, the Federal Data Protection and Information Commissioner (FDPIC) 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 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). The FDPIC may not, however, award any monetary damages or compensation or impose any fines or other sanctions.

Law stated - 31 Mai 2024

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 Mai 2024

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) that 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 Mai 2024

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 Mai 2024

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 Federal Data Protection Act (DPA), such analysis and subsequent advertising may under certain circumstances amount to high-risk profiling, requiring explicit consent of the data subjects concerned (if consent serves as justification to process PI), keeping logs of and drawing up regulations for such processing (if conducted by automated means), or performance of a data protection impact assessment.

Law stated - 31 Mai 2024

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 Mai 2024

Profiling

Are there any rules regarding individual profiling?

Under the 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 poses 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) by private parties

requires explicit consent by the data subjects concerned (if consent serves as justification to process PI).

In addition, pursuant to the Federal Data Protection Ordinance (DPO), private controllers and processors must keep logs and draw up regulations when carrying out high-risk profiling by automated means.

Law stated - 31 Mai 2024

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, controllers and processors must ensure through suitable technical and organisational measures a level of data security appropriate to the risks, regardless of where the PI is stored. Anyone processing PI must ensure its protection against unauthorised access as well as its availability, integrity and traceability.

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 that 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 Mai 2024

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), which, together with the revised Ordinance to the DPA (DPO), entered into force on 1 September 2023. 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 allowed Switzerland to uphold its status as a country adequately protecting personal information (PI) from an EU perspective (which was renewed on 15 January 2024), thereby allowing for continued easier transfer of PI from the European Union into Switzerland.

Law stated - 31 Mai 2024