Data Security and Cybercrime

Jurisdiction snapshot

Trends and climate

Would you consider your national data protection laws to be ahead or behind of the international curve?

Switzerland

Walder Wyss

Under Swiss law, data protection and data privacy are considered constitutional rights. Compliance with the respective provisions is crucial for all undertakings processing personal data. As a rule, Swiss legislation provides a data protection level that is similar to that under the EU Data Protection Directive. In certain respects, Swiss data protection law clearly goes beyond EU law – in particular, as regards the protection of data pertaining to legal entities. However, particularly with respect to cybersecurity legislation, Switzerland is less advanced than other European countries.

Back to top

Are any changes to existing data protection legislation proposed or expected in the near future?

Switzerland

Walder Wyss

The Data Protection Act is currently under revision. A major objective of the reform is to enable Switzerland to access the revised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (Convention 108), which is also under further revision. In addition, a closer alignment with EU data protection regulations is envisaged (in particular, in view of the recently approved EU General Data Protection Regulation). Among its key goals, the reform seeks to strengthen the position of the data protection and information commissioner and improve the enforcement mechanisms.

The revision process is still at an early stage. As the proposed amendment will be subject to extensive debates in Parliament and potentially a national referendum, it is hard to predict whether, when and to what extent it will finally be adopted and enter into force.

In addition, the Act on the Supervision of Postal and Telecommunication Services and the Act regarding Intelligence Services have undergone revision. The respective amendments aim to increase the scope of the surveillance of individuals – in particular, as regards the prevention of terrorism. Both reforms were, in principle, adopted by Parliament, but may be subject to a national referendum.

Back to top

Legal framework

Legislation

What legislation governs the collection, storage and use of personal data?

Switzerland

Walder Wyss

Data protection is regulated on both the federal and cantonal level. As regards the collection, storage, use and any other processing activities relating to personal data (also referred to as 'processing') performed by private persons (including private legal entities), the (Federal) Data Protection Act forms the core legislation. The rules contained in the act are further specified in the implementing Federal Ordinance on the Data Protection Act. However, further data protection provisions governing particular issues (eg, the processing of employee or medical data) are spread throughout a large number of legislative acts.

Back to top

Contributors

Switzerland

Jürg Schneider
Walder Wyss

Legal updates

Switzerland

Martin Zobl
Walder Wyss

Legal updates

Scope and jurisdiction

Who falls within the scope of the legislation?

Switzerland

Walder Wyss

The Data Protection Act applies to the processing of personal data by both private persons (including private legal entities) and federal administrative bodies.

Back to top

What kind of data falls within the scope of the legislation?

Switzerland

Walder Wyss

The Data Protection Act applies to all information relating to an identified or identifiable person. Under Swiss data protection law, the term 'person' encompasses both individuals and legal entities.

Back to top

Are data owners required to register with the relevant authority before processing data?

Switzerland

Walder Wyss

No general requirement for registration exists. However, controllers of data files that regularly process sensitive personal data or personality profiles, or regularly disclose personal data to third parties (including affiliates) for such third parties' own purposes, must register the respective data files with the data protection and information commissioner before they are opened. However, the duty of registration is subject to several exceptions set out in the Data Protection Act and the Ordinance on the Data Protection Act.

Back to top

Is information regarding registered data owners publicly available?

Switzerland

Walder Wyss

Yes, the list of registered data files can be accessed online (www.datareg.admin.ch/).

Back to top

Is there a requirement to appoint a data protection officer?

Switzerland

Walder Wyss

No such requirement exists. However, if the controller of data files chooses to appoint a data protection officer and notifies such appointment to the data protection and information commissioner, he or she need not register his or her files. A data protection officer has various duties, including independently monitoring internal compliance with data protection regulations and maintaining a list of all data files.

Back to top

Enforcement

Which body is responsible for enforcing data protection legislation and what are its powers?

Switzerland

Walder Wyss

The data protection and information commissioner is the responsible federal authority for supervising both private undertakings and federal public bodies. As regards the private sector, the commissioner is empowered to investigate cases on his or her own initiative or at the request of a third party if there is a possibility that methods of data processing are infringing the privacy of a large number of persons. In this context, the commissioner may request files, obtain information and arrange for processed data to be shown to him or her. Based on the investigation, the commissioner may

issue recommendations to the relevant data processor (eg, to change or abandon certain methods of processing). That said, the commissioner does not have enforcement powers. If a recommendation issued by the commissioner is not complied with or is rejected, he or she may refer the matter to the Swiss Federal Administrative Court. The Federal Administrative Court's decision can be appealed before the Swiss Federal Supreme Court.

In regulated sectors, authorities have extended investigative powers within their field of competence. For example, the Swiss Financial Market Supervisory Authority can appoint independent experts to conduct audits of supervised persons and entities, which must provide these experts with all information and documents required to carry out their tasks.

In addition, a data subject whose personality rights have been violated has a civil claim against the alleged perpetrator, on the basis of which he or she can file a lawsuit with the competent court. Further, a small number of violations of the data protection rules constitute criminal offenses.

Back to top

Collection and storage of data

Collection and management

In what circumstances can personal data be collected, stored and processed?

Switzerland

Walder Wyss

Anyone processing personal data must adhere to the following principles and rules contained in the Data Protection Act:

- The principle of good faith – personal data must be processed in good faith. In particular, it may not be collected by misrepresentation or deception.
- The principle of proportionality – the processing of personal data must be necessary for the intended purpose and reasonable in relation to the infringement of privacy.
- The principle of purpose limitation – personal data may be processed only for the purpose indicated at the time of collection, that is evident from the circumstances or that is provided for by law.
- The principle of transparency – the collection of personal data and, in particular, the purposes of its processing must be evident to the data subject concerned. As long as this is the case, the principle of transparency does not necessarily entail a specific disclosure obligation towards the data subject.
- The principle of data accuracy – personal data must be accurate and kept up to date.
- The principle of data security – adequate technical and organisational security safeguards must be taken against unauthorised or unlawful processing of personal data.
- The principle of lawfulness – the processing of personal data must not violate any legal provisions (including provisions outside the Data Protection Act) which are, directly or indirectly, intended to protect the personality rights of the data subjects.

Justification is not necessarily required for the processing of personal data. However, justification is required if processing amounts to a breach of the privacy rights of data subjects. In particular, a data handler must not:

- process personal data in contravention of one of the data protection principles set out in the Data Protection Act;
- process data against the data subject's express wish; or
- disclose sensitive personal data or personality profiles to third parties for such parties' own purposes.

Normally, no breach of privacy rights will exist if the data subject has made the data generally available and has not expressly restricted its processing.

Back to top

Are there any limitations or restrictions on the period for which an organisation may (or must) retain records?

Switzerland

Walder Wyss

Given the aforementioned proportionality principle, personal data must not be retained longer than necessary for the purpose of processing. However, applicable regulations on the safekeeping of records (eg, accounting or tax-related provisions) may provide for longer retention periods.

Back to top

Do individuals have a right to access personal information about them that is held by an organisation?

Switzerland

Walder Wyss

Individuals can request the controller of a data file to provide information regarding whether any data concerning them is being processed. The controller must inform the individual of:

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

If the controller of a data file has a third party process personal data, the obligation to provide information essentially remains with the controller. However, the third-party processor must provide information if it does not disclose the identity of the controller or if the controller is not domiciled in Switzerland.

The Data Protection Act provides a number of exceptions to a data subject's right to request information.

Back to top

Do individuals have a right to request deletion of their data?

Switzerland

Walder Wyss

Data subjects are entitled to request the deletion of their personal data to the extent that the processing of such data is unlawful. Further, data subjects may request that incorrect data be corrected. Correction requests may include the deletion of data that cannot be corrected otherwise.

Back to top

Consent obligations

Is consent required before processing personal data?

Switzerland

Walder Wyss

In general, a data subject's consent is not required in order for data processing to be admissible. However, consent may justify data processing that would otherwise be unlawful. To the extent that the lawfulness of data processing is based on the consent of the data subject, consent must be given voluntarily and on provision of adequate information in order to be valid. As far as sensitive personal data or personality profiles are concerned, consent must be given explicitly.

Back to top

If consent is not provided, are there other circumstances in which data processing is permitted?

Switzerland

Walder Wyss

As described above, consent may be required to justify data processing that would otherwise be unlawful. In addition, data processing may be justified by an overriding private or Swiss public interest or by a Swiss legal provision.

Pursuant to the Data Protection Act, an overriding private interest of the person processing the data will be considered if it:

- processes personal data in direct connection with the conclusion or performance of a contract and the personal data is that of a contractual party;
- competes for business with, or wants to compete for business with, another person and for this purpose processes personal data without disclosing the data to third parties for such third parties' own purposes;
- processes data which is neither sensitive personal data nor a personality profile in order to verify the creditworthiness of another person, and discloses such data to third parties for the third parties' own purposes, provided that the data is required for the conclusion or performance of a contract with the data subject;
- processes personal data on a professional basis, exclusively for publication in the edited section of a periodically published medium;
- processes personal data for purposes not relating to a specific person – in particular, for the purposes of research, planning and statistics – and publishes the results in such a manner that does not allow the identification of the data subjects; and
- collects data on a person being a public figure to the extent that the data relates to that person's role as a public figure.

This list is not exhaustive. It should be assessed on a case-by-case basis whether and to what extent an overriding private interest exists.

Back to top

What information must be provided to individuals when personal data is collected?

Switzerland

Walder Wyss

It follows from the principle of transparency that the collection of personal data and, in particular, the purpose for its processing must be evident to the data subject concerned. As long as this is the case, the principle of transparency does not necessarily entail a specific disclosure obligation towards the data subject.

However, data subjects must be notified of the collection of sensitive personal data or personality profiles (as defined in the Data Protection Act). This duty also applies where the data is not directly collected from the data subject, but rather from third parties. As a minimum, the information provided must include the following:

- the controller of the data file;
- the purpose of the processing; and
- the categories of data recipient if there is a planned disclosure of data to third parties for the third parties' own purposes.

If the data is not collected directly 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 to a third party. The duty to provide information is subject to a limited number of exceptions which are set out in the Data Protection Act.

Back to top

Data security and breach notification

Security obligations

Are there specific security obligations that must be complied with?

Switzerland

Walder Wyss

According to the Data Protection Act, adequate technical and organisational security safeguards must be taken against unauthorised or unlawful processing of personal data. Such measures are further specified in the Federal Ordinance on the Data Protection Act, which requires that systems which process personal data comply with state of the art technical standards in terms of protecting against:

- unauthorised or accidental destruction or loss;
- technical flaws;
- forgery;
- theft or unlawful access;
- copying;
- use alteration; and
- other kinds of unauthorised processing.

More specific requirements apply to systems featuring automated processing of personal data – in particular, regarding appropriate access, disclosure, storage and usage controls.

Back to top

Breach notification

Are data owners/processors required to notify individuals in the event of a breach?

Switzerland

Walder Wyss

Although there is no general obligation to notify data subjects, in the event of a breach, notification may become necessary in some cases due to the general data protection principles, particularly the principle of good faith. The necessity and the scope of such information will depend on the circumstances – in particular, the gravity of the breach and the necessity to prevent any damages and potential abuse of the disclosed data.

In addition, there are a number of sector and infrastructure-specific notification duties, particularly relating to financial services, telecoms, aviation, the railway industry and nuclear energy.

Back to top

Are data owners/processors required to notify the regulator in the event of a breach?

Switzerland

Walder Wyss

To date, no such requirement exists under the Data Protection Act. However, the revised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe contains a duty to notify the supervisory authority of data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects. As Switzerland intends to access the revised treaty, a similar provision may be included in the Data Protection Act in the course of the pending revision process.

Back to top

Electronic marketing and internet use

Electronic marketing

Are there rules specifically governing unsolicited electronic marketing (spam)?

Switzerland

Walder Wyss

Yes, sending spam is prohibited by the Act against Unfair Competition and, as such, is subject to criminal penalties. According to the act, anyone will be considered to be acting unfairly if they send or arrange to send mass advertising using telecommunications with no direct connection to the requested content and in the process fail to:

- obtain the prior consent of customers;
- indicate the correct sender; and
- refer to an easy, free of charge possibility to refuse.

However, anyone who, when selling goods, works or services, obtains customers' contact information and indicates the possibility of refusal will not be considered to be acting unfairly if they send mass advertising for their own or similar goods, works and services to such customer without the latter's consent.

Back to top

Cookies

Are there rules governing the use of cookies?

Switzerland

Walder Wyss

Since 2007 the use of cookies has been regulated by Article 45c, Letter (b) of the Telecommunications Act of April 30 1997. According to this article, website operators must inform users about the use of cookies and their purpose. In addition, they must explain how cookies can be rejected (ie, how cookies can be deactivated in users' browsers). In contrast to EU countries, Switzerland follows the opt-out principle. However, to the extent that cookies collect sensitive personal data or personality profiles, the Data Protection Act applies and explicit consent of the data subject may be required.

Back to top

Data transfer and third parties

Cross-border data transfer

What rules govern the transfer of data outside your jurisdiction?

Switzerland

Walder Wyss

Under the Data Protection Act, a disclosure of personal data abroad is prohibited if such disclosure could seriously endanger the personality rights of the data subjects concerned, in particular due to the absence of legislation that guarantees adequate protection for personal data. The data protection and information commissioner has published a non-binding list of countries which provide an adequate level of data protection with respect to individuals. In general, EU member states and EEA countries that have implemented EU Directive 95/46/EC are considered to provide an adequate level of data protection with respect to personal data pertaining to individuals and thus appear on the list.

Disclosures to non-EU or non-EEA countries must be assessed on a case-by-case basis to determine whether the respective country provides an adequate level of data protection. The same applies to all cross-border disclosures of personal data pertaining to legal entities, including transfers to EU and EEA countries.

Arguably, the mere fact that some countries lack specific data protection legislation covering legal entities does not necessarily result in a 'serious danger' for the personality rights of the legal entities concerned. Further, it can be reasonably argued that adequate protection may also be guaranteed through other kinds of legislation. That said, some legal scholars and the commissioner have taken a different stand on these issues and it is not certain if Swiss courts would follow the more liberal approach in this matter.

In the absence of legislation offering an adequate level of data protection, personal data may be transferred abroad only if:

- sufficient safeguards – particularly contractual clauses (eg, EU Model Contract clauses adapted to Swiss law requirements) – ensure an adequate level of protection abroad (Exception A);
- the data subject has given its consent in a specific case;
- the processing is directly connected with the conclusion or performance of a contract and the personal data is that of a contractual party;
- disclosure is essential in the specific case either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
- disclosure is required in the specific case in order to protect the life or physical integrity of the data subject;
- the data subject has made the data 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 the persons involved are subject to data protection rules that ensure an adequate level of protection (so-called 'binding corporate rules') (Exception G).

In addition, in the case of sufficient safeguards (Exception A) and disclosures made under binding corporate rules (Exception G), the data protection and information commissioner must be informed of the safeguards taken or the adopted binding corporate rules.

Once the commissioner has been informed of the safeguards adopted (Exception A), all subsequent transfers of the same category of data to the same categories of recipient under the same safeguards and for the same processing purposes are covered without requiring additional notification(s). If personal data is transmitted on the basis of model contracts or standard clauses that have been drawn up or approved by the commissioner, general information about the use of such contracts or clauses is sufficient.

Similarly, once the first transfer has been notified under Exception G, additional disclosures need not be notified if they take place within the same legal person or company, or between legal persons or companies that are under the same management, provided that the data protection rules continue to ensure an adequate level of protection. .

Back to top

Are there restrictions on the geographic transfer of data?

Switzerland

Walder Wyss

See above.

Back to top

Third parties

Do any specific requirements apply to data owners where personal data is transferred to a third party for processing?

Switzerland

Walder Wyss

Anyone may assign the processing of personal data to third parties by agreement or by law if:

- the data is processed only on behalf of and in accordance with the instructions of the assignor; and

- such assignment is not prohibited by a statutory or contractual duty of confidentiality.

In addition, the assignor must ensure that the third party guarantees data security.

Back to top

Penalties and compensation

Penalties

What are the potential penalties for non-compliance with data protection provisions?

Switzerland

Walder Wyss

If a recommendation made by the data protection and information commissioner in the course of an investigation is not complied with or is rejected by the affected data processor, the commissioner may refer the matter to the Swiss Federal Administrative Court. Both the commissioner and the affected data processor have the right to appeal against such a decision before the Swiss Federal Supreme Court. However, these administrative procedures do not directly result in a penalty. Likewise, the commissioner has no power to issue fines.

However, to the extent that a violation of the Data Protection Act amounts to a criminal offense, the competent criminal judge may fine private persons up to Sfr10,000.

Back to top

Compensation

Are individuals entitled to compensation for loss suffered as a result of a data breach or non-compliance with data protection provisions by the data owner?

Switzerland

Walder Wyss

Yes, data subjects (including legal entities) can request compensation for moral sufferings and payment of damages or the handing over of profits arising from violations of their privacy rights. However, experience has shown that it is often difficult for data subjects to prove actual damage suffered as a result of privacy infringements.

Back to top

Cybersecurity

Cybersecurity legislation, regulation and enforcement

Has legislation been introduced in your jurisdiction that specifically covers cybercrime and/or cybersecurity?

Switzerland

Walder Wyss

No dedicated cybersecurity or cybercrime legislation has been adopted in Switzerland to date, nor are there any plans to address the issue comprehensively in a legal instrument. Cybersecurity and cybercrime are instead governed by a patchwork of rules contained in various acts and emanating from regulators' guidance.

Back to top

What are the other significant regulatory considerations regarding cybersecurity in your jurisdiction (including any international standards that have been adopted)?

Switzerland

Walder Wyss

According to the Data Protection Act, personal data must be protected against unauthorised processing through adequate technical and organisational measures. Enforcement of the data security principles is – to a large extent – in the hands of the concerned organisations and, eventually, the civil courts. As regards data security, the data protection and information commissioner has become active only in a limited number of cases.

Under the Telecommunications Act, the Federal Office for Communications is responsible for implementing the

administrative and technical requirements pertaining to the security and availability of telecoms services, which includes notifying the regulator in the event of security incidents.

On January 1 2016 the new Federal Act on Financial Market Infrastructure (FinfrAct) entered into force. The new act governs the organisation and operation of financial market infrastructures (eg, stock exchanges, multilateral trade systems, central deposits or payment systems). Among other things, FinfrAct requires robust IT systems capable of deploying effective emergency responses and ensuring business continuity. As further specified in the implementing ordinance to FinfrAct, the systems must be designed to:

- ensure the availability, confidentiality and integrity of data;
- enable reliable access controls; and
- provide features to detect and remedy security incidents.

As regards international standards relating to cybersecurity in particular (eg, ISO 27001:2013), adherence to such standards is not mandatory in Switzerland. However, given that these standards are a relevant tool for assessing compliance with best practices, many undertakings tend to undergo certification voluntarily.

In addition, manufacturers of data processing systems or programs, as well as private undertakings that process personal data, may submit their systems, procedures and organisations to an accredited independent certification body for evaluation on a voluntary basis. Adherence to International Organisation for Standardisation standards is a prerequisite for certification.

Back to top

Which cyber activities are criminalised in your jurisdiction?

Switzerland

Walder Wyss

The following activities related to cybersecurity are punishable under the Penal Code:

- unauthorised obtaining of data;
- unauthorised access to a data processing system;
- damage to data;
- computer fraud;
- breach of secrecy or privacy through the use of an image-carrying device;
- obtaining personal data without authorisation;
- industrial espionage; and
- breach of the postal or telecoms secrecy.

Further crimes related to cybersecurity are defined in the Telecommunications Act.

Back to top

Which authorities are responsible for enforcing cybersecurity rules?

Switzerland

Walder Wyss

The data protection and information commissioner is, among other things, responsible for supervising private undertakings with respect to compliance with data protection law. The Federal Office for Communications is responsible for implementing the requirements set out in the Telecommunications Act. Financial market infrastructures are under the regulatory surveillance of Financial Market Supervisory Authority.

Back to top

Cybersecurity best practice and reporting

Can companies obtain insurance for cybersecurity breaches and is it common to do so?

Switzerland

Walder Wyss

Insurance coverage for cybersecurity breaches has been available for only a few years, but has become increasingly popular. The offered coverage varies significantly and includes, for example, the loss or theft of data, damages due to hacking and malware and the unwanted publication of data.

Back to top

Are companies required to keep records of cybercrime threats, attacks and breaches?

Switzerland

Walder Wyss

To date, no general requirements to keep such records have been enacted. However, in some industries, sector-specific regulations exist.

Back to top

Are companies required to report cybercrime threats, attacks and breaches to the relevant authorities?

Switzerland

Walder Wyss

Notwithstanding any sector-specific regulations, companies affected by cyberattacks are encouraged (albeit not required) to notify incidents to the Reporting and Analysis Centre for Information Assurance (MELANI). Companies can file a report with a simple message on MELANI's website in an anonymised form.

Back to top

Are companies required to report cybercrime threats, attacks and breaches publicly?

Switzerland

Walder Wyss

Not in general. However, in the event that a large number of data subjects are affected, the data processing principles may exceptionally result in a factual duty to report the incident publicly – in particular, if the data subjects concerned cannot be informed individually.

Back to top

Criminal sanctions and penalties

What are the potential criminal sanctions for cybercrime?

Switzerland

Walder Wyss

The penalties for committing a cybercrime range from relatively low fines to imprisonment, depending on the gravity of the violation.

Back to top

What penalties may be imposed for failure to comply with cybersecurity regulations?

Switzerland

Walder Wyss

Notwithstanding any sector and industry-specific regulations, failure to comply with pertinent cybersecurity regulations (arising from data protection law) does not directly trigger any penalties. However, if an affected company does not comply with or rejects a recommendation issued by the data protection and information commissioner in the course of an investigation, the matter may be referred to the Swiss Federal Administrative Court for a decision.

Failure to comply with a ruling from the regulatory authorities (including courts) may be subject to criminal or administrative penalties depending on the applicable statute in question.

Back to top

Law stated date

Correct as of

Please state the date of which the law stated here is accurate.

Switzerland

Walder Wyss

April 22 2016.

Back to top