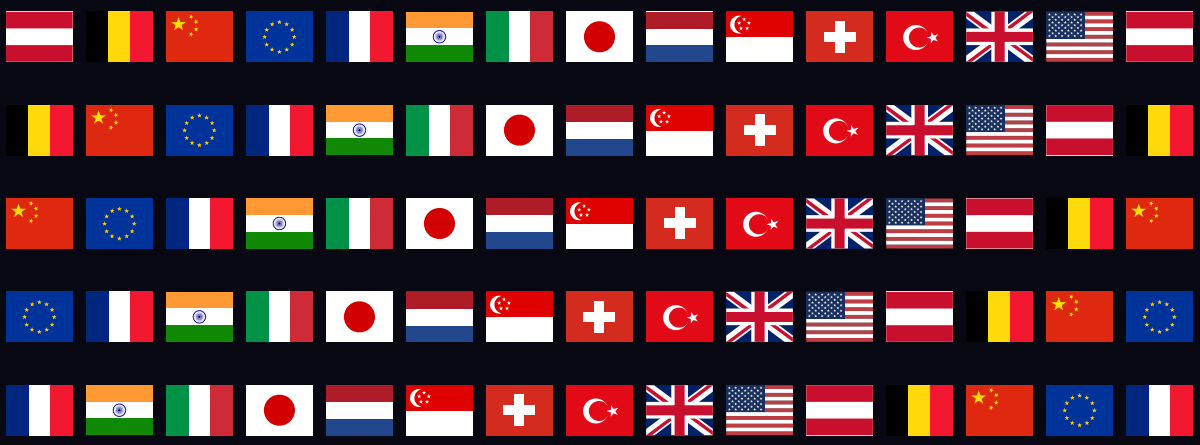
CYBERSECURITY

Switzerland



LEXOLOGY
Getting The Deal Through

Consulting editor
Ropes & Gray LLP

Cybersecurity

Consulting editors

Edward R McNicholas, Fran Faircloth

Ropes & Gray LLP

Quick reference guide enabling side-by-side comparison of local insights, including into the applicable legal and regulatory framework; best practices, including information sharing and insurance; enforcement, including relevant regulatory authorities, notification obligations, penalties, and avenues of private redress; threat detection and reporting; and recent trends.

Generated 13 July 2023

Table of contents

Contributors

Switzerland

Michael Isler
michael.isler@walderwyss.com
Walder Wyss Ltd

walderwyss attorneys at law

Jürg Schneider
juerg.schneider@walderwyss.com
Walder Wyss Ltd

Hugh Reeves
hugh.reeves@walderwyss.com
Walder Wyss Ltd

LEGAL FRAMEWORK

Legislation

Summarise the main statutes and regulations that regulate or promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

No overarching cybersecurity legislation has been adopted in Switzerland to date, and there are also no plans to comprehensively address the issue in a bespoke legal instrument. Rather, cybersecurity is and will remain regulated by a patchwork of various acts and regulatory guidance. Currently, the sole clear exception to this rule is the Information Security Act of 18 December 2020 (ISA), which should enter into force in the course of 2023. It will lead to the repeal of the Ordinance on the Protection against Cyber Risks in the Federal Administration (CyRV) of 27 May 2020, which entered into force on 1 July 2020. The CyRV, and the upcoming ISA, governs the organisation of the federal administration from a cyber risks protection standpoint. It, therefore, regulates the tasks of federal cybersecurity bodies, provides for a competence centre – the National Cyber Security Centre (NCSC) – and moreover regulates various compliance aspects regarding external service providers that contract with the federal administration. The ISA is expected to include a reporting obligation for cyberattacks on critical infrastructure. Victims of such attacks will have to report them to the NCSC.

The following list sets out the most relevant legislative instruments dealing explicitly or implicitly with cybersecurity in the private sector (ie, excluding the ISA and current CyRV, as they primarily pertain to the federal administration).

Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime (CCC) entered into force in Switzerland on 1 January 2012 and imposes the following main obligations on member states with respect to cybercrime:

- harmonisation of substantive criminal laws;
- adoption of expedient investigation and prosecution measures; and
- establishment of a fast and effective regime of international cooperation.

Switzerland's adherence to the CCC brought about some light amendments to the Swiss Penal Code (SPC) and the Federal Act on International Mutual Assistance in Criminal Matters to render domestic law compliant with the prerequisites of the convention.

Federal Data Protection Act

The Federal Data Protection Act (FDPA) governs the protection of personal data, as well as data security, which is, under Swiss law, a core tenet of cybersecurity.

On 1 September 2023, the revised FDPA will enter into force, bringing about significant changes to data protection in general, with the aim of more closely aligning the FDPA with the GDPR. In particular, legal entities will no longer benefit from dedicated data protection, transparency will be strengthened, data breaches will have to be notified in most cases and the criminal sanctions for offences against the FDPA will be bolstered. As far as data security is concerned, however, the matter has not been specifically or exhaustively addressed as a standalone subject and, rather, will remain part of the subject matter of the revised FDPA and its ordinance (as is the case under current law). In working on the topic of data security, the legislator sought to add some further requirements in the revised FDPA but only did so cautiously, as the Swiss legislator follows a 'technologically neutral' approach and only seldom discusses specific

technologies; this allows Swiss laws to remain relevant over time, but also arguably limits the legislator to rather general considerations as opposed to detailed technical requirements.

Federal Telecommunications Act

Pursuant to article 48a of the Federal Telecommunications Act (TCA) and article 96 of the corresponding Ordinance on Telecommunications Services (OTS), the Federal Office of Communications (OFCOM) is responsible for implementing the administrative and technical requirements pertaining to the security and availability of telecommunications services, which includes notification of the regulator in the event of security incidents. This body of laws includes rules against unsolicited messaging and spamming as well as provisions on addressing resources seek to minimise risks of cybercriminality. Importantly, a recent revision (that entered into force on 1 January 2023) adds increased network security requirements, primarily by means of anti-piracy and anti-tampering, as well as a requirement on 5G operators (networks and services) to implement an information security management system. Moreover, the Federal Act on the Surveillance of Postal and Telecommunications Traffic of 6 October 2010 governs information requests and real-time and retroactive monitoring of postal and telecommunications traffic.

In addition, the Federal Act on the Intelligence Service governs the monitoring of data streams to and from Switzerland to fulfil antiterrorism and national security objectives. In this respect, on 25 September 2020, Parliament adopted a new act on police measures for combatting terrorism. This law, which grants the authorities extensive powers – including online surveillance – to combat terrorism, was approved during a nationwide referendum in June 2021, and entered into force on 1 June 2022.

Further, pursuant to article 15 of the Ordinance on Internet Domains (which has been revised, with entry into force of the revised text on 1 January 2021), the registry for the '.ch' top-level domain (currently the SWITCH foundation) is required, if requested by an OFCOM-accredited body, to combat cybercrime or to block domain names if there are reasonable grounds to suspect that they are being used to access sensitive data using illegal methods (phishing) or to distribute harmful software (malware). The only organisation entitled to accomplish this task is the NCSC, as it now incorporates the former Reporting and Analysis Centre for Information Assurance.

Federal Act on Financial Market Infrastructure

The Federal Act on Financial Market Infrastructure (FinMIA), which entered into force on 1 January 2016, regulates the organisation and operation of financial market infrastructures, such as stock exchanges, multilateral trade systems, central deposits and payment systems. Article 14 of the FinMIA demands robust IT systems that are capable of deploying effective emergency responses and ensuring business continuity. The obligations are further detailed in article 15 of the implementing ordinance of the FinMIA. The systems must be designed to:

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

Financial market infrastructures are under the regulatory surveillance of the Swiss Financial Market Supervisory Authority (FINMA).

The FinMIA is the first sector-specific federal act applicable to private undertakings that expressly acknowledges the high dependency of essential infrastructure on information technology and the vulnerability to which it is exposed, owing to the interconnectivity of the market players' systems.

Law stated - 23 February 2023

Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Historically, the focal zone of regulatory activity in the area of cybersecurity in Switzerland is the financial sector. In the aftermath of the financial crisis, the banking sector suffered from severe data leaks, albeit not primarily as a result of cyberattacks, which have greatly increased awareness of the importance of data security in general. Consequently, FINMA amended its Circular 2008/21 on the operational risks of banks by adding a chapter on the security of electronic data. Annex 3 to the Circular accordingly sets forth a number of principles and guidelines on proper risk management related to the confidentiality of client-identifying data stored electronically. FINMA makes it clear that state-of-the-art data security standards and procedures, as well as proper incident management, are pivotal. The main message conveyed is that cybersecurity must become a matter of top management attention. FINMA further enhanced the required security standards through an amendment of Circular 2008/21, with effect from July 2017. Specifically, management is required to implement a cyber risk management concept, which also entails regular vulnerability assessments and penetration tests. Circular 2008/21 has been playing a key role in shaping the cybersecurity practices of Swiss financial institutions. For it to remain relevant, FINMA revised this circular with Circular 2023/01 on the Operational Risks and Resilience at Banks.

Another important instrument of financial sector oversight relevant to cybersecurity is FINMA Circular 2018/3 regarding outsourcing at banks and insurance companies. It increases the transparency of the outsourced tasks by introducing an inventory of these tasks. Further, the (financial) institution and the service provider must draw up a security framework to ensure that the outsourced function can continue to be performed in an emergency. In contrast to prevailing trends in regulatory activity and contrary to the previous version of the Circular, the Circular does not contain provisions on data protection to avoid duplication with the FDPA.

Another emphasis lies on the protection of critical infrastructure from cyberthreats, such as in the electricity, transportation and telecommunications sectors. The healthcare sector has also received increasing attention recently, in particular, regarding the vulnerability of medical devices connected to the internet as well as in relation to the implementation of the electronic patient record. In this respect, it has been pointed out that a decentralised approach as adopted in Switzerland, despite its apparent disadvantages in terms of efficiency and interconnectivity, reduces the risk of a single point of failure and as such enhances data security. However, in small and medium-sized enterprises, cybersecurity has still not made it to the agenda of many board meetings as an item of strategic importance; it continues to be treated as a mere technicality. Nevertheless, there is a growing awareness among these enterprises that cybersecurity should become a top-level concern and must be addressed on a permanent and dynamic basis.

Law stated - 23 February 2023

Has your jurisdiction adopted any international standards related to cybersecurity?

Adherence to international standards related to cybersecurity (such as ISO 27001:2022) is not mandatory in Switzerland. However, many undertakings are undergoing certification voluntarily, and those standards also serve as a benchmark when it comes to compliance with best practices as, for example, imposed by the regulator in the financial sector or by customers outsourcing their information and communications technology operations to third parties.

Further, pursuant to article 13 of the FDPA, the manufacturers of data processing systems or programs, as well as private undertakings that process personal data, may submit their systems, procedures and organisations to be evaluated by an accredited independent certification body on a voluntary basis. If they do so (which is very rare), abidance by the standards of ISO 27001:2013 is a prerequisite for this certification.

Law stated - 23 February 2023

What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

As a matter of principle, responsibility for cybersecurity lies with the data processing organisation and not with the individuals entrusted with the task. Starting in September 2023, however, the FDPA criminalises failure to comply with certain minimum data security requirements. Indeed, pursuant to article 61 of the FDPA, intentional violations of such data security requirements may lead to a fine of up to 250,000 Swiss francs. In other words, the private persons who are deemed at fault for a wilful violation of data security face a high fine imposed by the competent criminal prosecution authorities.

The ultimate responsibility for the overall strategy as regards cybersecurity, particularly the determination of the appropriate internal organisation as well as the adoption of the necessary directives, processes and controls, is vested in the board of directors of the company. This is certainly the case with respect to cyber risks that may have an impact on the accuracy of the company's financial statements and, therefore, need to be monitored by an internal control system, which forms part of the statutory audit scope but may arguably be extended beyond that. Given the increasing importance and awareness of cybersecurity, the problem can no longer be simply delegated to the IT department. In this context, pursuant to article 754 of the Swiss Code of Obligations, the members of the board of directors and other executive directors are personally liable both to the company and to the individual shareholders and creditors for any loss or damage arising from any intentional or negligent breach of their duties. Hence, personal liability of the responsible individuals may materialise if a company suffered loss because of a severe data breach that resulted from a lack of appropriate internal cybersecurity controls and procedures.

Law stated - 23 February 2023

How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

The CyRV, which is not an overarching law but rather targets structural and organisational matters within the federal administration, defines 'cybersecurity' as follows in article 3a: 'The situation in which the processing of data, in particular the exchange of data between persons and organisations via information and communication infrastructures, operates as intended' (authors' translation).

Traditionally, because Swiss legislation is technologically neutral and instead mostly relies on general rules and definitions, cybersecurity is usually closely associated with the notion of data security, being specified that data security is not a comprehensively defined notion and should rather be seen as an evolving concept.

The national strategy reports on cyber risks adopted by the federal government in 2012 and 2018 define cybersecurity as protection from disruptions of and attacks against information and communication infrastructures. Hence, the term would embrace both pertinent operational reliability and extraneous vulnerability concerns.

In line with the scope of application of the CCC, it can be argued that, outside heavily regulated sectors, the inclusion of cybersecurity provisions in legislation is equated with defence against cybercrime, namely repressive sanctions and procedures in relation to crimes committed via the internet, whereas preventive security measures are dealt with as a secondary concern of data privacy.

Law stated - 23 February 2023

What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

Pursuant to article 8 of the FDPA, personal data (ie, all information relating to an identified or identifiable natural person) must be protected against unauthorised processing through adequate technical and organisational measures, commensurate with the type of personal data being processed. Given these vague requirements, and even though the FDPA stipulates minimum protective measures, there is a large margin of discretion as to what these minimum requirements would precisely entail.

Even in heavily regulated sectors, such as critical infrastructures, the minimum protective measures are rarely defined. The organisations running the infrastructure are deemed best positioned to assess and implement the actual level of cybersecurity needed for their specific operations and risk exposures. The government would only intervene where self-regulation fails. However, the national cyber risk strategy acknowledges a desire and need to devise more authoritative cybersecurity standards. An interesting observation is that the competitive landscape would not allow the adoption of more stringent (and costly) security requirements on a national level without simultaneous international harmonisation.

Law stated - 23 February 2023

Scope and jurisdiction

Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

There is no specific legislation in Switzerland that deals with cyberthreats to intellectual property. Nevertheless, article 39a of the Swiss Federal Copyright Act prohibits the circumvention of effective technological measures for the protection of works and other protected subject matter (digital rights management (DRM)). DRM refers to technologies and devices such as access control, copy control, encryption, scrambling and other modification mechanisms intended and suitable for preventing or limiting the unauthorised use of intellectual property. It is unlawful to manufacture, import, offer, transfer or otherwise distribute, rent, give for use and advertise; possess for commercial purposes, devices, products or components; or provide services that purport the circumvention of DRM.

These prohibitions may not be enforced against persons who are permitted to circumvent DRM by virtue of statutory permission, such as the use of copyrighted work for private purposes or other statutory fair use limitations. It is against this background that the federal government established a surveillance office that monitors and reports on the effects of DRM and acts as a liaison between user and consumer groups. Given its mandate, the surveillance office focuses on the abusive use of DRM systems by the industry rather than on cyberthreats to intellectual property.

Law stated - 23 February 2023

Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The upcoming ISA will bring about a clear framework surrounding the cyber security mechanisms in place to protect critical infrastructures and the responses in case of cyber attacks.

That said, the current regulation of cybersecurity in critical infrastructure is fragmented and inconsistent. Although some legislative instruments deal with protection against cyber risks, they generally lack a precise definition of the required security measures. The same conclusion was reached by a report dealing with the national strategy for the protection of critical infrastructure, which was endorsed by the government in 2012 and revised in 2017 for the years

2018 to 2022, though the latter revised report does note a positive legislative trend towards better resilience and clearer security measures.

The primary responsibility to establish suitable controls and procedures lies with the organisations operating critical infrastructure. In the case of the need for governmental intervention, it would, in the majority of cases, be the competent regulator's task to define the appropriate measures. For instance, OFCOM may issue technical and administrative regulations concerning the handling of information security, the obligation to report faults in the operation of networks and other measures that make a contribution to the security and availability of telecommunications infrastructures and services (article 96, paragraph 2 OTS). In the financial sector, it is up to FINMA to adopt the necessary measures by way of circulars and regulatory notices (article 7 of the Financial Market Supervision Act).

The regulatory activities are seconded by the NCSC, which is a multidisciplinary body sponsored by the federal government and, inter alia, responsible for counselling a closed circle of roughly 140 operators of critical infrastructure in cybersecurity issues by:

- informing them of cyber incidents and threats;
- providing analyses for early detection and evaluation of cyberattacks and incidents; and
- examining malicious code.

The primary purposes of the NCSC are to provide dedicated competencies and skills in the cybersecurity area, serve as a contact point for the government, the media and the general public and raise awareness around matters of cybersecurity and the related risks.

Law stated - 23 February 2023

Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Pursuant to telecommunications secrecy governed by article 43 of the TCA, any person who is or was entrusted with providing tasks pertaining to telecommunications services must not disclose information relating to subscribers' communications or give anyone else the opportunity to do so. The range of addressees of telecommunications secrecy is very broad and encompasses not only telecommunications operators but also all stakeholders that are active in the delivery of telecommunications services, including any auxiliaries entrusted in full or in part with the provision of telecommunications services on behalf of service providers.

Telecommunications secrecy prohibits not only disclosure of communications content (including peripheral data) to third parties but also the interception of such content by the addressees of the telecommunications themselves, subject to the following limitative exemptions:

- lawful interception in accordance with the prerequisites of the Federal Act on the Surveillance of Postal and Telecommunications Traffic;
- filtering of malicious content causing damage to the telecommunications network (viruses, etc) and unsolicited mass advertising; and
- processing of peripheral data for billing and debt collection purposes.

Telecommunications secrecy does not provide for a clear exemption with respect to filtering of malicious content. However, according to article 321-ter, paragraph 4 of the SPC, breach of telecommunications secrecy for the sake of

preventing damage is justified and, therefore, not subject to prosecution. However, pursuant to article 49 of the TCA, the falsification or suppression of information by a person involved in the provision of telecommunications services constitutes a criminal offence. In a synthesis of these two partially contradicting provisions, the following conditions will apply:

- the filtering must be carried out in an automatic manner to the effect that no individual is capable of taking notice of the content of the information; and
- the objective of the filtering process must be confined to the suppression of the malicious code.

Suppression of the entire message is only permissible if:

- there are no other means of preventing the malicious code from being transmitted; and
- the sender and the intended recipient of the message are informed about the suppression.

Law stated - 23 February 2023

What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

The following cybercrimes are sanctioned pursuant to the SPC:

- unauthorised obtaining of data (article 143);
- unauthorised access to a data processing system (article 143-bis);
- damage to data (article 144-bis);
- computer fraud (article 147);
- breach of secrecy or privacy through the use of an image-carrying device (article 179-quater);
- obtaining personal data without authorisation (article 179-novies);
- industrial espionage (article 273);
- breach of the postal or telecommunications secrecy (article 321-ter); and
- others, for which general provisions can apply, such as fraud (article 146).

Further, the TCA stipulates criminal sanctions where private information received through means of a telecommunication device is used or disclosed to third parties without permission (article 50 TCA), or of the establishment or operation of a telecommunications installation with the intention to disturb telecommunications or broadcasting (article 51 TCA). In addition, the processing of data on external devices by means of transmission using telecommunications techniques without informing users thereof is prohibited (article 45c TCA) and constitutes a misdemeanour. Lastly, the transmission of mass advertising through telecommunication channels (spam) constitutes an act of unfair competition and is criminalised as such.

Law stated - 23 February 2023

How has your jurisdiction addressed information security challenges associated with cloud computing?

Although cloud services have become increasingly popular in Switzerland, there are no specific hard-law provisions with regard to the security requirements of cloud computing. Accordingly, the general data protection provisions apply.

If personal data is processed in the cloud by a provider, the processing regularly qualifies as data processing by a third party on behalf of the principal. As such, the processing of personal data may be outsourced to a cloud provider by agreement or by law if the data is processed only in the manner permitted for the principal itself and the outsourcing is not prohibited by a statutory or contractual duty of confidentiality. Moreover, the principal must ensure that the provider guarantees appropriate data security. Depending on the sensitivity of the data processed in the cloud, this may entail an obligation of the principal to conduct security audits, which will often be unrealistic in a cloud setting. In practice, principals will largely rely on the cloud providers' data security certifications; however, they provide no guarantee that the provider in practice heeds these respective security controls and procedures.

Additionally, cloud computing will frequently entail cross-border disclosure of personal data. Personal data must not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular owing to the absence of legislation in the country of import that guarantees an adequate level of data protection. However, even in the absence of comparable privacy legislation, cross-border disclosure through cloud services is generally permissible if sufficient alternative safeguards (in particular, contractual clauses) substitute for an adequate level of data protection.

Law stated - 23 February 2023

How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

There are no particular cybersecurity regulations specifically applicable to foreign organisations doing business in Switzerland. Under Swiss conflict of law rules, a foreign organisation generally needs to observe the provisions of the FDPA if it processes personal data in Switzerland or if data subjects resident in Switzerland are affected, even if the organisation is domiciled abroad. As a general rule, sectorial regulatory requirements pertaining to data security must be observed by Swiss branches or representations of foreign organisations.

Law stated - 23 February 2023

BEST PRACTICE

Increased protection

Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The National Cyber Security Centre (NCSC) and its precursor, the Reporting and Analysis Centre for Information Assurance, adopted recommendations for small and medium-sized enterprises with regard to best practices for removing malware, cleaning up websites, protecting industrial control systems and content management systems, securing e-banking and countering distributed denial-of-service attacks. They are partially based on recommendations issued by the US Industrial Control Systems Cyber Emergency Response Team.

Law stated - 23 February 2023

How does the government incentivise organisations to improve their cybersecurity?

Apart from the services provided by the Cyber Security Delegate and the NCSC, the government also has a stake in the public-private partnership Swiss Cyber Experts, which is an alliance of cybersecurity experts in the information and communications technology and sciences industries and the public and private sectors. The Swiss Internet Security

Alliance is a similar project that aims to reduce the infection rate of devices within Switzerland. Further, cybersecurity projects occasionally receive a grant from Innosuisse, which is a federal innovation promotion agency responsible for encouraging science-based innovation in Switzerland by providing financing, professional advice and networks. Moreover, the government has set up a 'cyber defence campus' at the federal technology institutes (ie, ETH in Zurich and the Swiss Federal Institute of Technology (EPFL) in Lausanne).

Law stated - 23 February 2023

Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The pertinent industry norms, such as ISO 27001:2022, can be obtained from the Swiss Association for Standardisation . Further, the NCSC provides some additional guidance.

Law stated - 23 February 2023

Are there generally recommended best practices and procedures for responding to breaches?

Victims of cyberattacks are encouraged to share information and to report incidents to the supporting units maintained by the federal government (to the NCSC, which issues alerts and helps to coordinate the response to cyberattacks).

Law stated - 23 February 2023

Voluntary information sharing

Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Victims of cyberattacks are encouraged to notify incidents to the NCSC. The report can be made by a simple message on the NCSC's website and may be submitted anonymously. The NCSC looks to be a central point of contact in all matters relating to cybersecurity and is therefore the primary (federal) governmental body in this respect.

Law stated - 23 February 2023

How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The national strategy for the protection of Switzerland against cyber risks, which was first adopted by the government in 2012 and updated in 2018, has identified a desire within the industry for intensified cooperation between the public authorities, the private sector and operators of critical infrastructure to mitigate cyber risks. Stakeholders expect increased consistency in the elaboration of standards and procedures to be devised in a cooperative manner. The government also holds that the primary responsibility to fight cyberattacks lies with each responsible organisational unit individually, and the authorities are only supposed to interfere if public interests are at stake or if the relevant risks cannot be addressed at the competent subordinate level. In line with this strategy, the government is a stakeholder in private initiatives dedicated to the enhancement of cybersecurity awareness and defence schemes.

Law stated - 23 February 2023

Insurance

Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

At the beginning of 2013, the first insurance company started to offer insurance for cybersecurity in Switzerland. Since then, several Swiss insurance companies have followed this example and offer coverage for cyber risks. The risks covered by this insurance vary and include, for example, the loss or theft of data, unwanted publication of data, damage resulting from hacking and malware, or costs ensuing from investigations or crisis management as a result of cybercrime.

Law stated - 23 February 2023

ENFORCEMENT

Regulation

Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

On a general scale, the following authorities are primarily responsible for enforcing cybersecurity regulations affecting the private sector:

- the Federal Data Protection and Information Commissioner (FDPIC), who is responsible for the supervision of private undertakings with regard to their compliance with the Federal Data Protection Act (FDPA); and
- the Cybercrime Coordination Unit Switzerland, which forwards cases of incoming reports to the appropriate prosecution authorities in Switzerland and abroad (ie, the police and public prosecutors in charge of prosecuting cybercrimes), it being specified that the Cyber Security Delegate and the National Cyber Security Centre also serve as valuable contact points for matters pertaining to cyber security and cyber risks.

On a sectoral level, the authorities entrusted with regulatory oversight are also responsible for enforcing compliance of the regulated undertakings with cybersecurity rules. In crisis situations affecting critical infrastructure, the special task force for information assurance would intervene. It is composed of decision-makers from the public and private sectors dealing with critical infrastructures. The latter are involved in power supply, emergency and rescue services, banks and insurance companies, telecommunications, transport and traffic, and public health (including water supply), as well as the government and public administrations.

Law stated - 23 February 2023

Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

A distinction must be drawn between the general economy and regulated sectors.

On a general level, the FDPIC is endowed with powers to investigate cases on his or her own initiative or at the request of a third party. This could, for instance, be the case if a specific undertaking processing a large volume of sensitive personal data is suspected of neglecting data security obligations. The FDPIC has an investigative authority and various enforcement powers, such as issuing injunctions (eg, to cease certain data processing, provide information, prohibit cross-border disclosures and implement data security measures).

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

Law stated - 23 February 2023

What are the most common enforcement issues and how have regulators and the private sector addressed them?

Switzerland has experienced increased exposure to cyber incidents in recent years, with ransomware and identity theft being among the top issues. More specifically, the Reporting and Analysis Centre for Information Assurance – now part of the National Cyber Security Centre (NCSC) – observed an increase of incidents concerning ransomware, including the expansion of ransomware as a service, as well as usurpation of the names of various federal authorities or companies (such as the Swiss Post and Swisscom). Ransomware attacks, targeting private entities of all sizes, as well as public bodies, has become a common occurrence and will remain a core focus of cybersecurity activities for the years to come.

On a judicial level, the expectations of expedited international cooperation in combatting cybercrime propagated by the Budapest Convention on Cybercrime (CCC) suffered a setback by a landmark decision handed down by the Swiss Federal Supreme Court in January 2015: the judges ruled that cantonal prosecutors were not empowered to bypass judicial assistance and order Facebook to release the IP history of its users by virtue of article 32 of the CCC. With respect to cybersecurity regulations, FINMA has been regularly updating its rules on the treatment of electronic client data by banks. These amendments have enhanced cybersecurity awareness in the financial sector. More recently, in a July 2020 decision, the Federal Supreme Court ruled that, in a client-bank relationship, clients bear the (contractually allocated) risk of being hacked, save for cases of the bank's gross negligence. This specific matter involved a situation where a third party hacked into the client's email accounts and sent inaccurate transfer orders to the bank.

Law stated - 23 February 2023

What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

Switzerland currently does not have a general duty to notify of cybersecurity breaches; any reporting is currently done on a voluntary basis, typically via the NCSC. On 24 August 2022, The Swiss government is nevertheless contemplating the introduction of reporting duties for cyber incidents affecting critical national infrastructures as part of the draft Information Security Act, expected to enter into force in mid-2023. Under the contemplated setup, operators of critical infrastructures would need to notify the NSCS of certain cyber attacks within 24 hours from detection; the NCSC would serve as a single centralised point of contact.

From 1 September 2023 onwards, the FDPA will impose a duty to report violations of data security that have a likelihood of inducing a high risk for the personality or the fundamental rights of a data subject. This duty to report does not systematically call for the data subjects to be informed but applies only if the FDPIC orders it or if it is necessary to protect the data subject.

Sector-specific regulations may nonetheless call for notification, as is the case in the banking sector where FINMA Circular 2008/21 (and its upcoming replacement Circular 2023/01) requires that banks implement a clear communication strategy in case of grave incidents pertaining to the confidentiality of client-identifying data.

Law stated - 23 February 2023

Penalties for non-compliance with cybersecurity regulations

What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The FDPA contains provisions under which failure to follow the basic data security requirements may lead to a criminal fine.

Failure to comply with rulings of regulatory authorities may constitute a criminal offence or entail administrative sanctions depending on the applicable statute.

Law stated - 23 February 2023

What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

In regulated sectors, failure to submit a required report to the regulatory authority may be prosecuted as a crime or entail administrative sanctions depending on the applicable statute. The reporting obligation under the FDPA (starting 1 September 2023), if not heeded, may lead to criminal penalties. Moreover, failure to implement the minimal requirements for data security is criminally sanctioned by a fine.

Law stated - 23 February 2023

How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Victims of cyberattacks may seek redress in a civil action against the tortfeasor. This may be the cybercriminal or the entity that has failed to comply with appropriate data security standards and procedures. Since class actions do not exist in Switzerland, private individuals whose data have been hacked will, in most cases, be incapable of asserting financial damages in an amount that merits a claim. The FDPA provides that if the basic data security measures were not implemented, a criminal complaint may be filed by the injured party, which may lead to a criminal fine.

Law stated - 23 February 2023

THREAT DETECTION AND REPORTING

Policies and procedures

What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Personal data must be protected against unauthorised processing through adequate technical and organisational measures. These measures are set forth in more detail in the the (revised) Ordinance to the Federal Act on Data Protection (FDPO). Any system in which personal data is processed must live up to appropriate state-of-the-art technical standards in terms of protection against the risk of 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 are imposed on systems that feature automated processing of personal data. Those systems must, in particular, ensure appropriate access, disclosure, storage and usage controls. The revised FDPO contains some bolstered requirements around data security, but it does not, however, define specific technical requirements.

Sector-specific regulations and guidance may contain more detailed technical requirements or recommendations.

Law stated - 23 February 2023

Describe any rules requiring organisations to keep records of cyberthreats or attacks.

From September 2023, the FDPA will likely imply clear record-keeping in respect of cyberattacks (especially to the extent these resulted in a breach), as certain data breaches will have to be notified.

Law stated - 23 February 2023

Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

From 1 September 2023, the FDPA will provide for a duty to notify data breaches to the Federal Data Protection and Information Commissioner (FDPIC). The revised rules call for data controllers to notify the FDPIC as soon as possible if a data breach has occurred and when the breach is likely to result in a high risk to the privacy or the fundamental rights of the data subject. Conversely, the data processors must notify all breaches of data security to the data controller as soon as possible. This breach notification mechanism will not systematically require informing the data subjects, as this step shall only be required when necessary for the protection of the data subject or if requested by the FDPIC.

Notification duties specific to certain sectors and critical infrastructures include the following:

- financial services sector: mandatory notification to the Swiss Financial Market Supervisory Authority without delay regarding events of material relevance for the supervision of the relevant supervised entity;
- telecommunications sector: notification to National Emergency Operations Centre (NEOC) (no longer to the Federal Office of Communications) of faults in the operation of telecommunications networks that could affect at least 10,000 customers;
- aviation sector: notification to the Federal Office of Civil Aviation in the event of safety-related data breaches;
- railway industry: notification to the Federal Department of the Environment, Transport, Energy and Communications in the event of severe incidents; and
- nuclear sector: notification to the Swiss Federal Nuclear Safety Inspectorate in the event of safety-related data breaches.

Law stated - 23 February 2023

Time frames

What is the timeline for reporting to the authorities?

Sector-specific provisions may require the affected entity to report any relevant cybersecurity incidents without delay. The FDPA provides that the reporting of data security breaches that are likely to result in a high risk to the personality rights or the fundamental rights of the data subjects should occur 'as soon as possible', whereas regarding upcoming draft legislation for breaches affecting critical infrastructure, a 24-hour period from attack discovery is being considered.

Law stated - 23 February 2023

Reporting

Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

The FDPA (as of 1 September 2023) contains rules on the notification of data breaches. Pursuant to these rules, the data controller may be required to inform the data subjects of the breach if the information should prove necessary for the protection of the data subject or if it is requested by the FDPIC.

Law stated - 23 February 2023

UPDATE AND TRENDS

Recent developments and future changes

What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

One main challenge to the development of cybersecurity regulations is the speed at which cyberthreats evolve. This renders legislating on the subject rather difficult for Parliament. The international dimension of cybersecurity (eg, the involvement of foreign operatives) would also constitute an obstacle to the implementation of the criminal provisions contained in any dedicated cybersecurity law.

The current Swiss approach relies to a broad extent on providing private actors with helpful contact points and resources, with the ultimate aim of mitigating to the greatest extent possible the impact of any cyberthreat on national infrastructures, local businesses and the general public. This is leading the government to bolster its resources, both financially and in terms of personnel. Across-the-board sharing of information and interaction with the science and research domains should also occur on a more regular basis, paving the way for a transversal and interdisciplinary approach to cybersecurity. If not already the case, companies should make a habit of ensuring they implement proper cybersecurity practices and train their personnel accordingly. They should also interact with the ad hoc bodies, in particular the National Cyber Security Centre and the Cyber Security Delegate, to promptly share any relevant information.

Law stated - 23 February 2023

LAW STATED DATE

Correct On

Give the date on which the information above is accurate.

23 February 2023

Law stated - 23 February 2023

Jurisdictions

Austria	MGLP Rechtsanwälte | Attorneys-at-Law
Belgium	NautaDutilh
China	Fangda Partners
European Union	Taylor Wessing
France	ADSTO
India	AZB & Partners
Italy	ICT Legal Consulting
Japan	TMI Associates
Netherlands	Eversheds Sutherland (International) LLP
Singapore	Drew & Napier LLC
Switzerland	Walder Wyss Ltd
Turkey	Paksoy
United Kingdom	Simmons & Simmons
USA	Ropes & Gray LLP