Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

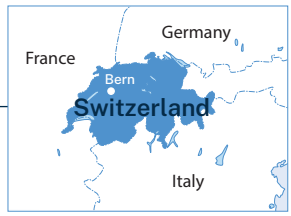
Cybersecurity 2026

Definitive global law guides offering comparative analysis from top-ranked lawyers

Switzerland: Law and Practice & Trends and Developments

David Vasella, Jürg Schneider, Hugh Reeves and Yannick Caballero Cuevas
Walder Wyss Ltd

SWITZERLAND



Law and Practice

Contributed by:
David Vasella, Jürg Schneider, Hugh Reeves and Yannick Caballero Cuevas
Walder Wyss Ltd

Contents

1. General Overview of Laws and Regulators p.4
1.1 Cybersecurity Regulation Strategy p.4
1.2 Cybersecurity Laws p.4
1.3 Cybersecurity Regulators p.6

2. Critical Infrastructure Cybersecurity Regulation p.7
2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.7
2.2 Critical Infrastructure Cybersecurity Requirements p.7
2.3 Incident Response and Notification Obligations p.7
2.4 State Responsibilities and Obligations p.7

3. Operational Resilience in the Financial Sector p.8
3.1 Scope of Financial Sector Operational Resilience Regulation p.8
3.2 ICT Service Provider Contractual Requirements p.8
3.3 Key Operational Resilience Obligations p.8
3.4 Operational Resilience Enforcement p.9
3.5 International Data Transfers p.9
3.6 Threat-Led Penetration Testing p.10

4. Cyber-Resilience p.10
4.1 Cyber-Resilience Legislation p.10
4.2 Key Obligations Under Legislation p.10

5. Security Certification for ICT Products, Services and Processes p.11
5.1 Key Cybersecurity Certification Legislation p.11

6. Cybersecurity in Other Regulations p.11
6.1 Cybersecurity and Data Protection p.11
6.2 Cybersecurity and AI p.11
6.3 Cybersecurity in the Healthcare Sector p.12

Walder Wyss Ltd was established in Zurich in 1972 and has since grown at record speed. Today, the firm has about 300 legal experts and approximately 150 support staff in six offices in Switzerland's economic centres. It is an agile firm that is approachable, adapts to clients quickly and does not hide behind formality. Because it is fully integrated, partners bring in those people who have the greatest expertise and are best-suited for a particular task. This helps avoid silos and ensures that work is carried out efficiently. Walder Wyss was the first large Swiss firm to strongly focus on tech, including data protection. The firm has one of the largest and most experienced teams in this area and advises clients in all sectors on Swiss data law, including technology, privacy, AI and IT.

Authors

David Vasella is a partner in the regulated markets, competition, tech and IP team at Walder Wyss. He advises Swiss and international companies and authorities on questions concerning data and technology law. David specialises in data use, data and technology-related contracts, data security matters, cloud projects, data protection compliance and artificial intelligence. He regularly gives talks and writes for publications, for example, on datenrecht.ch, a Swiss platform on data law. He is a certified information privacy professional and manager (CIPP/E, CIPM), fellow of information privacy (FIP) and AI governance professional (AIGP).

Jürg Schneider is a partner in the regulated markets, competition, tech and IP team at Walder Wyss. His practice areas include information technology, data protection and outsourcing. Jürg has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international contexts. His competencies regarding data protection include drawing up data protection concepts and strategies for companies, leading and assisting compliance projects regarding implementation of privacy legislation for Swiss and international companies, and advising clients in regulated sectors (banking, insurance, healthcare, etc) on data protection requirements as well as cybersecurity.

Hugh Reeves is a partner in the regulated markets, competition, tech and IP team at Walder Wyss. He advises clients on technology transactions, commercial contracts, telecommunications, intellectual property and digitalisation. Hugh is active in the areas of data protection and e-commerce and assists clients with their entry or expansion into the Swiss market.

Yannick Caballero Cuevas is an associate in the regulated markets, competition, tech and IP team at Walder Wyss, working in both the Lausanne and Geneva offices. He advises clients on data protection law, IT contracts, and regulatory issues relating to technology, including artificial intelligence.

Contributed by: David Vasella, Jürg Schneider, Hugh Reeves and Yannick Caballero Cuevas, **Walder Wyss Ltd**

Walder Wyss Ltd

Seefeldstrasse 123
8008 Zurich
Switzerland

Tel: +41 586 585 858
Fax: +41 586 585 959
Email: reception@walderwyss.com
Web: www.walderwyss.com

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

Switzerland is a federation comprising 26 federated states (cantons) as well as a federal government. This leads to a layered body of laws as well as, at times, a decentralised official cybersecurity approach. Cybersecurity in Switzerland remains closely tied to the area of data protection. Cybersecurity is frequently perceived as an off-shoot – or even a synonym – of data security, which, as the name suggests, targets the security and resilience of data processing and storage activities.

A further manifestation of the government's interest in cybersecurity is another governmental venture, the Digital Switzerland Strategy. The Digital Switzerland Strategy sets guidelines for Switzerland's digital transformation, and is updated annually by the Swiss Federal Council, each time with three focus topics. It is binding on the federal administration and provides guidance for other stakeholders involved in digitalisation. The first Digital Switzerland Strategy was published in 2016, and updates arrived in 2018, 2020, 2023, 2024 and 2025. On 12 December 2025, the Swiss Federal Council adopted the updated Digital Switzerland Strategy for 2026.

In 2023, the Swiss Federal Council approved the new Digital Administration Switzerland Strategy 2024–27, which defines the fields of action to be prioritised in order for the Confederation, the cantons, and cities and municipalities to jointly determine how the digital transformation of administrations is to be driven forward. A second strategy approved by the Swiss Federal Council is the Digital Federal Administration Strategy, which creates a framework for digital transformation projects in the federal administration.

1.2 Cybersecurity Laws

On a federal level, the Swiss Constitution of 18 April 1999 protects the right to privacy, in particular the right to be protected against misuse of personal data (Article 13). The collection and use of personal data by private bodies are regulated at the federal level and are mainly governed by the Federal Data Protection Act (FADP) and its ordinances, including the Data Protection Ordinance (DPO).

Data processing by public bodies is governed by the FADP for federal bodies, which includes private organisations performing public tasks such as health insurance providers, pension funds and many others, and by cantonal (for example, the Information and Data Protection Act of the Canton of Zurich) and communal laws for cantonal and communal bodies.

The FADP was revised in order to implement the revised Council of Europe's Convention 108, and to more closely align with the EU General Data Protection Regulation (GDPR). The revised FADP and DPO entered into force on 1 September 2023.

While the FADP and the GDPR are similar in their approach and purpose, there are notable differences. For example, there is a data breach notification obligation under the FADP, similar to that under the

GDPR, but the trigger for notifying a personal data breach to the Swiss data protection authority, the Federal Data Protection and Information Commissioner (FDPIC), is "high risk", whereas, under the GDPR, any relevant risk requires notification. On 6 February 2025, the FDPIC published non-binding guidance on breach notification obligations under the FADP, which was subsequently updated on 23 April 2025. Another key difference is the level of activity by the relevant authorities: while many supervisory authorities within the European Economic Area (EEA) are more active, providing guidance and/or enforcing the GDPR, the FDPIC is generally reluctant to take a decisive stance and rarely provides guidance for private actors. However, the FDPIC has initiated several investigations under the revised FADP.

The FADP and the DPO provide for a general requirement to ensure an appropriate level of data security in relation to personally identifiable information. The revised FADP calls for state-of-the-art data security measures, without specifying specific technical standards. However, a specific security requirement is the obligation to keep logs to ensure that data operations are logged by federal authorities and private actors that process sensitive data on a large scale or carry out "high-risk profiling", a form of profiling that leads to personality profiles. These logs must be relatively granular and must be kept for at least one year, separately from the productive environment. In addition, the revised legislation imposes on controllers and processors, under certain conditions, a duty to notify data security breaches to the FDPIC, and potentially to data subjects. Additional compliance and documentation measures, such as data protection impact assessments and records of processing activities, as well as an obligation to maintain processing regulations, have also been introduced.

The Information Security Act (ISA) of 18 December 2020, which entered into force on 1 January 2024, governs information security practices within the federal government and its administrative bodies. Under the ISA, several ordinances further specify and implement information security requirements and also repeal (inter alia) the Ordinance on the Protection against Cyber Risks in the Federal Administration (CyRV). Importantly, a significant feature of the ISA is the introduction of a reporting obligation for cyber-attacks for public authorities such as universities; federal, cantonal and municipal agencies; intercantonal, cantonal and intercommunal organisations; and providers of critical infrastructures, for example in the energy, finance, healthcare, insurance, transport, communication and IT sectors. In-scope organisations must report cyber-attacks to the National Cyber Security Centre (NCSC) within 24 hours, where the relevant thresholds and definitions are met. This reporting obligation entered into force on 1 April 2025.

Apart from the ISA, cybersecurity remains mostly regulated by a patchwork of various acts and regulatory guidance, which deal explicitly or implicitly with cybersecurity in the private sector. These laws include:

- the Budapest Convention on Cybercrime (CCC), which entered into force in Switzerland on 1 January 2012 and imposes a harmonisation of Switzerland's criminal legislation as well as speedy international co-operation mechanisms;
- the FADP;
- the Federal Telecommunications Act (TCA) of 30 April 1997, including its ordinances, which – as of 1 January 2023 – contain specific information security and network threat resilience requirements; and
- the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (FinMia) of 19 June 2015 – the banking and financial markets legislation also led the financial markets regulator, the Swiss Financial Markets Supervisory Authority (FINMA), to issue various circulars and regulatory notices.

However, the Swiss government has given cybersecurity increasing attention in the past few years, and the absence of an overarching ad hoc law on cybersecurity may appear misleading given the importance and national relevance of this topic. Nonetheless, this conclusion is unlikely to lead the Swiss legislator (Parliament) to issue any additional topical legislation on cybersecurity in the near future. On the contrary, the federal government has been following the National Strategy for the Protection of Switzerland against Cyber Risks (NCS).

The NCS was last updated in April 2023. The strategy sets out the objectives and measures with which the federal government and the cantons, together with the business community and universities, intend to counter cyber threats. A steering committee has been established to plan and co-ordinate the implementation of the strategy. The revised NCS builds on the previous strategies, adding content and precision. It defines 17 measures, each contributing to five strategic objectives, namely:

- self-empowerment (Switzerland is to expand its position as one of the world's leading knowledge, education and innovation locations in cybersecurity);
- securing digital services and infrastructures (Switzerland is to implement measures to strengthen cyber-resilience);
- ensuring effective detection, prevention, management and defence against cyber-incidents (Switzerland is to ensure the capacities and organisational structures needed to quickly identify cyber threats and incidents, and minimise damage, are in place);
- combating and prosecuting cybercrime effectively (Switzerland is to expand its ability to identify and prosecute threat actors); and
- maintaining a leading role in international co-operation (Switzerland is to foster an open, free and secure cyberspace and compliance with international law in the digital space).

However, the NCS does not foresee the implementation of a dedicated cybersecurity legislation, instead focusing on modernising various pre-existing laws. The updated NCS is testament to the continued growth in relevance of cybersecurity in Switzerland, as well as perhaps the increased global threat posed by cyber-risks.

On 14 May 2025, the Swiss Federal Council took note of the first implementation report on the National Cyber Strategy, which provides an overview of progress made to strengthen national cybersecurity efforts in Switzerland. Prepared by the NCS Steering Committee in collaboration with the NCSC, the report highlighted tangible advancements, including the establishment of key co-ordination structures, the rollout of ongoing initiatives, the launch of new projects, and a strengthened international profile for Switzerland in the field of cybersecurity.

1.3 Cybersecurity Regulators

The FDPIC is a body established at the federal level under the FADP. The FDPIC supervises compliance with the FADP and other federal data protection legislation by federal bodies and advises private bodies. On its own initiative, or at the request of a third party, the FDPIC may carry out investigations into data processing by private bodies. In addition, each canton has its own data protection authority, which is generally competent to supervise cantonal and communal bodies (but not private parties, which are subject to the FDPIC's authority). Other regulators – for example, FINMA – may play a role in the enforcement of data protection (see the following).

It is also worth mentioning here that the key official actor in the cybersecurity area is the NCSC, the English designation of the Bundesamt für Cybersicherheit (BACS), the federal office integrated within the Federal Department of Defence, Civil Protection and Sport (DDPS). Indeed, in an effort to centralise the administrative activities in this area, other actors such as the Reporting and Analysis Centre for Information Assurance (MELANI), GovCert and the Cybercrime Coordination Unit (CYCO) became an integral part of the NCSC. It therefore serves as the federal government's competence centre for cybersecurity and acts as the primary point of contact for business, public authorities, educational institutions, and the public on all cyber-related matters. Tasks include raising public awareness, receiving reports on cyber-incidents and supporting operators of critical infrastructures in managing these incidents. Protection of the federal administration against cyber-attacks is now a key task of a new specialist unit within the new State Secretariat for Security Policy (Sepos), also within the DDPS.

The FADP does not provide an official role for NGOs and self-regulatory organisations (SROs). Such organisations would not, for example, have a right to bring a civil claim against a company perceived to be in breach of privacy laws. However, there are a number of organisations that promote privacy, including several consumer protection organisations, although

they do not perform these tasks on the basis of a legal mandate.

The NCSC is the key official actor in the cybersecurity area. GovCERT.ch is the computer emergency response team (CERT) for Switzerland. Its tasks include supporting the critical IT infrastructure in Switzerland in dealing with cyber threats. It maintains close relationships with other CERT organisations, thereby seeking to promote the exchange of cyber-threat-related information. Furthermore, the FDPIC retains strong prerogatives given the absence of standalone cybersecurity legislation.

Given the federal system in Switzerland, it should also be borne in mind that other cantonal and inter-cantonal bodies serve the purpose of information sharing. This is notably the case for the inter-cantonal Swiss Criminality Prevention Service (the SKP and PSC under its German or French and Italian acronyms, respectively). This service seeks to facilitate inter-cantonal police co-ordination as well as crime prevention measures.

FINMA is the competent authority in the banking and financial sectors. As part of its statutory mission, and in the course of supervising regulated financial entities, FINMA may also request compliance with applicable data protection and data security regulations.

The Federal Office of Communications (OFCOM) is the federal office responsible for the proper implementation of the legal and technical requirements in the communications realm and plays a particularly important role in the area of telecommunications. In the area of unfair competition, the State Secretariat for Economic Affairs (SECO) acts for the Swiss Confederation in civil and criminal proceedings if matters of public interest are at stake.

In addition, the following authorities may also be competent, albeit indirectly, in the cybersecurity area:

- the Federal Office of Civil Aviation (in case of safety-related data breaches in the aviation sector);
- the Federal Nuclear Safety Inspectorate (in case of sector-related data breaches);
- the Federal Department of the Environment, Transport, Energy and Communications (DETEC), especially in regard to the national railway industry; and
- Swissmedic, which receives notifications of serious incidents that can include incidents relating to software as a medical device.

2. Critical Infrastructure Cybersecurity Regulation

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

The ISA imposes a breach reporting obligation in the event of cyber-attacks affecting critical infrastructures. Moreover, the Federal Office for National Economic Supply (FONES) published a minimum information and communication technology (ICT) standard document as well as an ICT self-assessment tool directed at operators of critical infrastructures. This document rests, in part, on the requirements of the relatively ubiquitous National Institute of Standards and Technology (NIST) framework to which it refers.

2.2 Critical Infrastructure Cybersecurity Requirements

Concerning critical infrastructure cybersecurity requirements, see **2.1 Scope of Critical Infrastructure Cybersecurity Regulation**.

2.3 Incident Response and Notification Obligations

Concerning incident response and notification obligations, see **2.1 Scope of Critical Infrastructure Cybersecurity Regulation**.

2.4 State Responsibilities and Obligations

Concerning state responsibilities and obligations, see **2.1 Scope of Critical Infrastructure Cybersecurity Regulation**.

3. Operational Resilience in the Financial Sector

3.1 Scope of Financial Sector Operational Resilience Regulation

FINMA, as the financial markets supervisory authority, frequently adopts and adapts various circulars and notices. In particular, Circular 2023/01 Operational Risks and Resilience – Banks, is central to all banks' cybersecurity practices laying out principles and guidelines on proper risk management in relation to client-identifying data (CID). It requires banks and investment firms to report certain cyber-attacks within 24 hours of becoming aware of them and to submit a full report within 72 hours.

FINMA Circular 2018/3 on Outsourcing by Banks and Insurers is another essential text as it contains rules on the security of data in an outsourcing context.

In the banking and financial markets sector, the regulator, FINMA, supervises the relevant actors (namely banks, insurance companies, financial institutions, collective investment schemes and fund management companies) and plays a role in the cybersecurity realm. Indeed, given the importance of the financial industry in Switzerland, data security and cybersecurity are core concerns. FINMA publishes an annual risk monitor as an overview of risks seen as particularly significant, and both the 2023 and the 2025 versions highlight that cyber-risks remain one of the biggest operational risks and note a trend towards malware attacks targeting external service providers.

In case of a breach of the sectoral rules, FINMA has a varied toolbox of enforcement measures. These include the revocation of licences to practice, fines or even custodial sentences. FINMA also occasionally, and for preventative purposes, relies on a "naming and shaming" strategy, meaning that the perpetrator of any offence against the regulatory rules is publicly named.

3.2 ICT Service Provider Contractual Requirements

As mentioned in **2.1 Scope of Critical Infrastructure Cybersecurity Regulation**, the ISA imposes a breach reporting obligation in the event of cyber-attacks affecting critical infrastructures. Moreover, FONES published a minimum ICT standard document as well as an ICT self-assessment tool directed at operators of critical infrastructures. This document rests, in part, on the requirements of the relatively ubiquitous NIST framework to which it refers.

3.3 Key Operational Resilience Obligations

Concerning key operational resilience obligations, see also **1.1 Cybersecurity Regulation Strategy** and **1.2 Cybersecurity Laws**. On 7 June 2024, FINMA published supervisory guidance 03/2024 on cyber-risks, which includes:

- findings from FINMA's cyber-risk supervision, including deep dives at banks;
- information on scenario-based cyber-exercises in accordance with Circular 2023/1 Operational Risks and Resilience; and
- clarifications of FINMA Guidance 05/2020 on the reporting requirement for cyber-attacks.

The clarifications relate to the reporting obligation under Article 29 (2) of the Financial Market Supervision Act, which requires supervised institutions to report certain material incidents to FINMA. It builds on earlier FINMA guidance, Guidance 03/24 and Guidance 05/2020. FINMA clarifies its expectations as follows.

Deadline for Reporting

FINMA confirms that the relevant institution has 24 hours from the moment a cyber-attack is discovered to report it to FINMA (see the following for information about the commencement of this window). Within these initial 24 hours, the institution must carry out an initial assessment of the criticality, with the aim of assessing whether the cyber-attack requires a report to FINMA. The "actual" report must then be made within a total of 72 hours via FINMA's survey and application platform (EHP).

Expectations for the Initial Report

FINMA states that timeliness is of the essence for the initial report. There are no specific expectations in terms of form or content, and initial reports can also be withdrawn later.

The initial report may be made informally, for example by e-mail or telephone. The aim is to reflect the then-known facts on the basis of the initial assessment. It may, of course, be the case that further clarifications show that the initial report would not have been mandatory. Institutions can therefore withdraw their initial reports at any time, giving them an incentive to err on the side of caution.

If an institution is also subject to the reporting requirement under the ISA, as revised, the initial report can be submitted through the relevant authority, the NCSC. To the extent known, the NCSC will forward the report to FINMA – if the reporting institution chooses this option – automatically and without filtering, so presumably immediately. The actual report must then continue to be submitted via the EHP.

Expectations for the Actual Report

FINMA Guidance 05/2020 requires a final root cause report for reports of cyber-attacks with a severity level of "medium" or more, which at a minimum contains the internal or external investigation or forensic report (further requirements can be found in FINMA Guidance 05/2020). As FINMA has now clarified, the root cause report should include the following aspects for the "high" and "serious" severity levels:

- the reason for the success of the cyber-attack;
- the impact of the attack on compliance with regulatory requirements, the institution's operations and its clients; and
- the mitigating measures introduced to address the effects of the attack.

For cyber-attacks categorised as "serious", evidence and analyses of the crisis organisation's ability to function must be included in the submission.

Calculation of Deadlines

FINMA has confirmed its existing practice: where an attack is detected by an outsourcing provider to the institution, the 24-hour window starts when the provider becomes aware of the attack, shortening the time left for the institution, in order to treat institutions that have not outsourced any functions equally to others.

When calculating the deadlines for the initial report and follow-up reports, only official banking days count. An exception applies to attacks with the "serious" severity level. In this case, the deadline for the initial report also applies outside of banking days. FINMA must be interpreted here as meaning that this does not apply to the deadline for the follow-up report.

It should be noted that FINMA did not formally align its guidance with the EU Digital Operational Resilience Act (DORA) or its level II and level III legislation, although they are similar in several regards.

3.4 Operational Resilience Enforcement

Concerning operational resilience enforcement, see **1.1 Cybersecurity Regulation Strategy** and **1.2 Cybersecurity Laws**.

3.5 International Data Transfers

The FADP aims to protect the personality rights and fundamental rights of natural persons whose personal data is processed. As a consequence, the FADP contains provisions on how this protection is to be guaranteed when data is transferred abroad, for instance to a state that does not offer the same level of data protection as Switzerland.

Controllers or processors may transfer personal data abroad if the Swiss Federal Council has determined that the legislation of the relevant state or international body guarantees an adequate level of protection. Therefore, the Swiss Federal Council determines, in a binding manner, to which countries the export of data is permitted.

On the other hand, in the absence of such a decision by the Swiss Federal Council, personal data may be disclosed abroad only if appropriate protection is guaranteed. Thus, at least one of the following conditions must be fulfilled:

- an international treaty;
- data protection provisions of a contract between the controller or the processor and its contracting partner, which were communicated beforehand to the FDPIC;

- specific safeguards prepared by the competent federal body and communicated beforehand to the FDPIC;
- standard data protection clauses previously approved, established or recognised by the FDPIC; and
- binding corporate rules (BCRs) on data protection that were previously approved by the FDPIC, or by a foreign authority that is responsible for data protection and belongs to a state that guarantees adequate protection.

Mechanisms or Derogations That Apply to International Data Transfers

The FADP provides that personal data may not be disclosed abroad if this would seriously endanger the personality of the data subjects. Such a serious threat to the personality rights of the data subjects may arise if the exporting state does not have legislation that guarantees an adequate level of data protection. However, a transfer of data to such a state may be permitted if one of the foregoing conditions is fulfilled.

Regarding the standard contractual clauses (SCCs) published by the EU Commission, the FDPIC formally recognised the SCCs for international transfers from Switzerland to third states, but only if certain changes are agreed to account for Swiss law (and the fact that Switzerland is not an EEA member state).

For data transfers subject to the GDPR only, the non-amended SCCs may be used. Therefore, the parties should determine whether only the FADP or both the FADP and the GDPR apply to the transfer in question.

The EU SCCs require a "transfer impact assessment" (TIA). This also applies to Swiss companies if they use the EU SCCs (under the GDPR as well as under the FADP). As part of a TIA, the Swiss data exporter must check in each specific case whether the laws of the recipient country regarding official access in the recipient country (eg, for the purpose of national security or criminal prosecution) and the rights of the data subjects are compatible with Swiss data protection law and Swiss constitutional principles.

In addition, Switzerland has recently implemented the Swiss-US Data Protection Framework (DPF). It remains to be seen if the DPF will stand, and for now, many companies opt to use the SCCs in addition to relying on the DPF.

Finally, the FDPIC has pointed out that internal company data protection regulations – ie, BCRs – cannot be a substitute for the conclusion of a SCC if transfers are made outside of a group of companies subject to the BCRs.

3.6 Threat-Led Penetration Testing

Swiss legislation does not currently provide for threat-led penetration testing (TLPT) requirements, except that FINMA expects banks and securities dealers to carry out regular penetration testing (per its Circular 2023/1 Operational Risks). In addition, Swiss financial entities may be subject to DORA requirements if they operate within the EU or have connections with EU-based financial institutions or their clients. Likewise, Swiss companies affiliated with EU financial entities that provide intra-group ICT services to their EU counterparts are also covered by DORA for these activities. Furthermore, DORA applies to Swiss ICT service providers as soon as they plan to offer their services to relevant financial entities within the EU. Finally, although Swiss data protection legislation does not expressly call for penetration testing, it can be mandatory to the extent it is a minimum security requirement in specific circumstances.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

Concerning cyber-resilience legislation, see **1.1 Cybersecurity Regulation Strategy** and **1.2 Cybersecurity Laws**.

4.2 Key Obligations Under Legislation

Concerning key obligations under legislation, see **1.1 Cybersecurity Regulation Strategy** and **1.2 Cybersecurity Laws**.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

The FADP regulates the issue of certification in Article 13. Software and system suppliers, as well as data controllers and their subcontractors, can have their products validated by an independent, accredited body. These certifications attest to their compliance with the requirements of the FADP.

In addition to ensuring compliance with data protection standards, these certifications offer a number of advantages. According to Article 22 (5) of the FADP, a data controller who adheres to a code of conduct or holds a certification may be exempted from carrying out an otherwise-required data protection impact assessment. These certifications can also be used as a basis for authorising data transfers abroad, even when the recipient country does not offer a level of data protection deemed adequate (Article 12 of the DPO). However, certification mechanisms have so far been little used in Swiss law.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

Concerning cybersecurity and data protection, see also **1.2 Cybersecurity Laws**. The only truly overarching body of laws is the federal legislation on data protection, namely the FADP and its implementing ordinances, in particular the DPO. The FADP and the DPO contain provisions on data security, but the Swiss legislator relies on a technologically neutral approach, with the result that these rules on data security remain rather abstract and do not refer to any specific technology, or any specific standard or technical requirement, except for the obligation to keep logs of certain higher-risk processing activities. Under the FADP, an intentional failure to implement certain minimum technical and organisational measures may incur liability for a criminal fine against the responsible individuals of up to CHF250,000, although there is a debate as to whether there are any binding minimum measures.

The ISA of 18 December 2020, which entered into force on 1 January 2024, governs information security practices within the federal government and its administrative bodies. Under the ISA, several ordinances further specify and implement information security requirements and also repeal (inter alia) the CyRV. Importantly, a significant feature of the ISA is the introduction of a reporting obligation for cyber-attacks for public authorities such as universities; federal, cantonal and municipal agencies; inter-cantonal, cantonal and intercommunal organisations; and providers of critical infrastructures, for example in the energy, finance, healthcare, insurance, transport, communication and IT sectors. In-scope organisations must report cyber-attacks to the NCSC within 24 hours, where the relevant thresholds and definitions are met.

As a more general consideration, the policy discussions in Switzerland in recent years have shown that cybersecurity is progressively evolving from what once was a purely technical consideration into a mainstream legal topic. Cybersecurity is now not only part of the legal discussions surrounding data protection and data security (in various areas, such as finance and telecommunications), but is also a focus of other branches of the law, such as insurance law.

Moreover, the policy discussions at the federal level are not expected to lead, in the short term, to any overarching cybersecurity law. However, the topic remains highly dynamic and strongly dependent on international developments. Given Switzerland's size and geographical location, prompt legal developments in the area of cybersecurity are a real possibility.

6.2 Cybersecurity and AI

Concerning cybersecurity and AI, see also **6.1 Cybersecurity and Data Protection**. In Switzerland, there is currently no overarching regulation on the use of AI.

The FDPIC has published statements and non-binding guidelines on how to address data protection matters in these areas. For example, the FDPIC pointed out that the FADP is directly applicable to AI-based data processing, and the FDPIC expects manufacturers, providers and users of AI systems to ensure transparency concerning the purpose, functionality, and data sources of AI-based processing.

Further, sector-specific regulations address particular data protection issues. For example, the Swiss government has also created a general frame of reference for the use of AI within the federal administration, and FINMA issued binding guidelines on outsourcing and data security for the financial and insurance sector, as well as Guidance 08/2024 on governance and risk management relating to the use of AI by banks and financial institutions, in which it sets out its supervisory expectations.

The following FADP safeguards can be applied to AI systems.

- Privacy by design/privacy by default – the data controller is obliged to implement technical and organisational measures to ensure that processing complies with data protection requirements right from the outset.
- Obligation to carry out an impact assessment – where the planned processing is likely to pose a high risk to data subjects or their fundamental rights, the data controller must first carry out a data protection impact analysis. A high risk exists in particular in the case of large-scale processing of sensitive data or systematic surveillance of large parts of the public domain.
- Transparency obligation for automated decisions – the data controller must inform the data subject of any decision taken exclusively on the basis of automated personal data processing that has legal effects on the data subject or significantly affects him or her. The data subject also has the right to express his or her point of view and to demand that the decision be reviewed by a natural person. These measures do not apply where the data subject has expressly consented to the decision being taken by automated means, or where the decision is directly related to the conclusion or performance of a contract and the data subject's request is met. If the automated decision is made by a federal body, such body must qualify it as such. The right of the data subject to express his or her point of view and to demand that the decision be reviewed by a natural person does not apply when the data subject does not have to be heard before the decision is made. When exercising his or her right of access, the data subject receives, in particular, information concerning the existence of an automated decision and the logic on which the decision is based.
- Requirement for a formal legal basis – federal bodies are only entitled to process personal data if a legal basis is given. The legal basis must be laid down in a law in the formal sense in three cases, namely:
  (a) the processing of sensitive data (for example biometric and genetic data);
  (b) profiling (as defined by the FADP); and
  (c) when the purpose or method of processing is likely to cause serious harm to the fundamental rights of the data subject.

The use of AI may therefore require a formal legal basis, even in the absence of sensitive data or profiling, if the processing method (eg, automated decision) is likely to seriously affect the fundamental rights of the data subject.

Finally, on 12 February 2025, DETEC and the Federal Department of Foreign Affairs (FDFA) presented an overview to the Swiss Federal Council of possible regulatory approaches to AI. On the basis of this overview, the Swiss Federal Council has decided on a Swiss regulatory approach for AI based on three objectives: strengthening Switzerland's location for innovation; safeguarding the protection of fundamental rights, including economic freedom; and increasing public trust in AI. To achieve these objectives, the Swiss Federal Council has set the following key steps for the future: incorporation of the Council of Europe's AI Convention (which Switzerland signed on 27 March 2025) into Swiss law; sector-specific legislation as far as required (cross-sector regulation, to be limited to central areas relevant to fundamental rights); and non-binding measures.

6.3 Cybersecurity in the Healthcare Sector

Concerning cybersecurity in the healthcare sector, see **6.1 Cybersecurity and Data Protection**.

Trends and Developments

Contributed by:
David Vasella, Jürg Schneider, Hugh Reeves and Yannick Caballero Cuevas
Walder Wyss Ltd

Walder Wyss Ltd was established in Zurich in 1972 and has since grown at record speed. Today, the firm has about 300 legal experts and approximately 150 support staff in six offices in Switzerland's economic centres. It is an agile firm that is approachable, adapts to clients quickly and does not hide behind formality. Because it is fully integrated, partners bring in those people who have the greatest expertise and are best-suited for a particular task. This helps avoid silos and ensures that work is carried out efficiently. Walder Wyss was the first large Swiss firm to strongly focus on tech, including data protection. The firm has one of the largest and most experienced teams in this area and advises clients in all sectors on Swiss data law, including technology, privacy, AI and IT.

Authors

David Vasella is a partner in the regulated markets, competition, tech and IP team at Walder Wyss. He advises Swiss and international companies and authorities on questions concerning data and technology law. David specialises in data use, data and technology-related contracts, data security matters, cloud projects, data protection compliance and artificial intelligence. He regularly gives talks and writes for publications, for example, on datenrecht.ch, a Swiss platform on data law. He is a certified information privacy professional and manager (CIPP/E, CIPM), fellow of information privacy (FIP) and AI governance professional (AIGP).

Jürg Schneider is a partner in the regulated markets, competition, tech and IP team at Walder Wyss. His practice areas include information technology, data protection and outsourcing. Jürg has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international contexts. His competencies regarding data protection include drawing up data protection concepts and strategies for companies, leading and assisting compliance projects regarding implementation of privacy legislation for Swiss and international companies, and advising clients in regulated sectors (banking, insurance, healthcare, etc) on data protection requirements as well as cybersecurity.

Hugh Reeves is a partner in the regulated markets, competition, tech and IP team at Walder Wyss. He advises clients on technology transactions, commercial contracts, telecommunications, intellectual property and digitalisation. Hugh is active in the areas of data protection and e-commerce and assists clients with their entry or expansion into the Swiss market.

Yannick Caballero Cuevas is an associate in the regulated markets, competition, tech and IP team at Walder Wyss, working in both the Lausanne and Geneva offices. He advises clients on data protection law, IT contracts, and regulatory issues relating to technology, including artificial intelligence.

Contributed by: David Vasella, Jürg Schneider, Hugh Reeves and Yannick Caballero Cuevas, **Walder Wyss Ltd**

Walder Wyss Ltd

Seefeldstrasse 123
8008 Zurich
Switzerland

Tel: +41 586 585 858
Fax: +41 586 585 959
Email: reception@walderwyss.com
Web: www.walderwyss.com

Regulation in the Face of Risk: Switzerland's Approach to Cybersecurity and AI Governance

Cyber threats are rapidly evolving, becoming ever more sophisticated and harder to detect. One ongoing but no less concerning trend is the increase of ransomware attacks, which have affected numerous companies and other organisations in Switzerland. Moreover, the National Cyber Security Centre (NCSC), the English designation for the *Bundesamt für Cybersicherheit* integrated within the Federal Department of Defence, Civil Protection and Sport (DDPS), reported a significant increase in phishing cases (eg, phishing attempts impersonating the Federal Tax Administration or Switzerland's popular payment app TWINT). This highlights the ongoing threat of phishing attacks, which often target individuals to gain access to sensitive information or systems.

Recent attacks include an attempt to infiltrate the IT systems of SBB, Switzerland's national railway, via email malware. This attack was partially successful, but no customer data was stolen. Another notable incident was a ransom attack on media companies, when a ransomware group breached the IT infrastructure of Neue Zürcher Zeitung and CH Media, two leading media outlets, stealing confidential data and encrypted files and extorting the companies. No ransom was paid, apparently, but sensitive employee and customer data later surfaced on the dark web. A hacker attack on a guardianship authority in the town of Saxon was successful, with sensitive client information stolen and published, affecting some 6,000 residents. Other notable incidents include an attack on the sewing machine manufacturer Bernina, which, according to media reports, paid a ransom; an attack on an education network used by the city of Basel-Stadt, leading to the theft of personal data of more than 750 persons; and a distributed denial-of-service (DDoS) attack during Ukrainian President Zelenskyy's video address to the Swiss Parliament. Other attacks targeted the city of Baden and the Canton of Schwyz.

The most widely publicised attack, however, was when a ransomware group attacked security software provider Xplain, which supplies numerous Swiss government agencies. The attackers claimed to have stolen over 900 GB of sensitive data, including information linked to the Swiss Army, customs, and police. An investigation report commissioned by the Confederation was issued on 28 March 2024. Noting the joint responsibility of Xplain and the Confederation in connection with this cyber-attack, the report pointed to the Confederation's failure in its duties to select, instruct and supervise the personal data subcontractor, in this case the company Xplain. In particular, the investigation report showed that no data processing contract had been concluded between the relevant federal administration units and Xplain. In an Xplain repeat, hackers hit Concevis, another major software vendor for the federal and cantonal governments.

These attacks illustrate that a key threat is the rise of sophisticated, hard-to-detect ransomware attacks, including on critical infrastructure providers, and that even advanced countries like Switzerland are vulnerable to potentially crippling cyber-attacks.

Recent regulatory updates

While the increase in reported attacks highlights the urgency of robust cybersecurity, the issue is hardly new. Switzerland has responded to these challenges

in recent months and years by adapting its cybersecurity framework on a number of levels.

The FADP and Data Protection Ordinance

The revised Federal Data Protection Act (FADP), which entered into force on 1 September 2023, introduced improved enforcement powers for the Swiss data protection authority, the Federal Data Protection and Information Commissioner (FDPIC). The FADP also introduced new requirements around data breach reporting, requiring controllers to inform the FDPIC as soon as possible about data security breaches that lead to a high risk and, where necessary, to communicate the breach to the affected data subjects. The reporting obligation is similar to that under the GDPR, but the threshold is higher (high risk under the FADP, and any relevant risk under the GDPR).

In addition, the FADP and the Federal Data Protection Ordinance (DPO) provide for a general requirement to ensure an appropriate level of data security in relation to personal data. The FADP calls for state-of-the-art data security measures, without specifying specific technical standards. This is a deliberate approach from the legislator, who chose to maintain a future-proof, technologically neutral philosophy. However, a specific security requirement is the obligation to ensure that data operations are logged by federal authorities, and by private actors that process sensitive personal data on a large scale or carry out "high-risk profiling", a form of profiling that leads to personality profiles. The FDPIC has provided guidance for implementing these logging obligations. As Switzerland is not a member of the European Economic Area (EEA), incident notifications in the EEA under the GDPR do not exempt companies from notification obligations towards the FDPIC under the FADP, if applicable, and vice versa.

The FADP provides that individuals (not legal entities, in contrast to the GDPR) who breached data security provisions and thereby failed to comply with the minimum requirements in that respect, will face criminal fines of up to CHF250,000. It remains unclear at this time if a general failure to implement a sufficiently robust level of data security can lead to a fine, but given the potential risks for business managers who may have a personal exposure, these fines are expected to work as an incentive for businesses to ensure state-of-the-art cybersecurity practices.

The Information Security Act

While the FADP applies to personal data only and, as noted, is fairly high-level, the Swiss Federal Council enacted the Information Security Act (ISA) and four implementing ordinances on 8 November 2023, effective as of 1 January 2024. The ISA is a response to the increasing number of cyber-attacks on public authorities and private individuals, and places high demands on information security. For example, it requires authorities to maintain an information security management system and to ensure that the third parties and providers they work with take necessary security measures. The ISA has also centralised cybersecurity activities under the NCSC; as discussed hereunder.

A significant feature of the ISA is the introduction of a reporting obligation for cyber-attacks for public authorities such as universities and federal, cantonal and municipal agencies; inter-cantonal, cantonal and intercommunal organisations; and providers of critical infrastructures, for example, in the energy, finance, healthcare, insurance, transport and communication and IT sectors. In-scope organisations must report cyber-attacks to the NCSC within 24 hours, where the relevant thresholds and definitions are met. This reporting obligation entered into force on 1 April 2025, and is in addition to other incident notifications, such as the obligation to report personal data security breaches to the FDPIC.

Updated government organisation at a federal level

The ISA and ensuing legislation have also reworked the government's security organisation. The NCSC, which is a federal office within the DDPS, now serves as the centre of competence for cybersecurity, acting as the primary point of contact for the economy, administration, educational institutions and the public on cyber-related issues. Its tasks include raising public awareness, receiving reports on cyber-incidents and supporting operators of critical infrastructures in managing these incidents. Protection of the federal administration against cyber-attacks is now a key task of a new specialist unit within the new State Secretariat for Security Policy (SEPOS), also within the DDPS.

Other regulatory activity

Other authorities have an increased focus on cybersecurity as well, within the scope of their supervisory activities. A key example is the Swiss Financial Markets Supervisory Authority (FINMA), which oversees compliance with, inter alia, data security regulations in the financial sector. It publishes an annual risk monitor as an overview of risks that FINMA sees as particularly significant. The 2025 version highlights that cyber-risks remain one of the biggest operational risks and observes a trend towards malware attacks targeting external service providers and a need for financial institutions to improve their responsibilities and control activities with regard to service providers. Outsourcing contributes to cyber-risks and remains a supervisory focus for FINMA, particularly because the concentration of outsourced services among a small number of providers means that an attack on any one of them can disrupt or impair multiple banks and financial institutions simultaneously. As of 1 January 2026, supervised institutions in categories 1 to 3 (namely extremely large, important and highly complex institutions with very high risk profiles (category 1), very large and complex institutions with high risk profiles (category 2), and large, complex institutions presenting significant risks (category 3)) will be required to co-ordinate their operational-resilience framework with other key components of their activities, in particular ICT and cyber-risk management, in order to ensure coherent and integrated operational-resilience arrangements.

One of FINMA's main supervisory tools is issuing guidance and circulars, which set out its expectations for regulated institutions. These include FINMA Circular 2023/1 Operational Risks and Resilience, which entered into force on 1 January 2024. It applies to banks and investment firms, requiring them to report certain cyber-attacks within 24 hours of becoming aware of them and to submit a full report within 72 hours. Again, this obligation is in addition to any other incident notification obligations. There is ongoing discussion in the market in relation to ensuring that the 24-hour requirement is met even where an institution has outsourced IT operations to a provider, such as a cloud services provider. On 7 June 2024, FINMA published FINMA Guidance 03/2024 – findings from FINMA's cyber risk supervision, clarification of FINMA Guidance 05/2020 and scenario-based cyber-risk exercises (see **3.3 Key Operational Resilience Obligations** in the Swiss Law and Practice chapter in this Guide).

Initiatives at a cantonal level

The cantons have also recently increased their efforts to prevent cyber threats. For example, Switzerland's largest canton by population, the Canton of Zurich, operates a Cantonal Cyber Security Centre (CCSC) as a knowledge hub for the canton, acting as a point of contact for cyber-issues for the cantonal administration, public authorities, critical infrastructure providers, cities, municipalities, cantonal organisations, business and industry, as well as the population. The CCSC is also responsible for implementing the cantonal cybersecurity strategy.

In addition, cantonal data protection legislation – applicable to public entities acting under cantonal laws, which may include private actors carrying out public tasks – requires notification of personal data security breaches to the cantonal data protection authorities.

The Artificial Intelligence Regulation (AI Regulation) and AI Act (AIA)

Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (the Artificial Intelligence Regulation, AI Regulation, AI Act or AIA) came into force on 1 August 2024. Its provisions will take effect in stages until August 2027 (Article 113 of the AI Act).

The AI Act is the comprehensive regulatory framework by which the EU (for the EEA, the AIA is of relevance) regulates the use of AI systems (AIS). Despite its name, the AI Act is not a comprehensive regulation of AI or market behaviour law, but rather a product safety law. It is based on the established principles of product regulation in the European single market, and it adopts a risk-based approach distinguishing between unacceptable-risk AI systems, high-risk AI systems, and limited-risk AI systems. In addition, it seeks to regulate general-purpose AI models, which must be distinguished from AI systems.

The AI Act is initially applicable in the EU. However, it will be incorporated into EEA law and will then also apply to Norway, Iceland and Liechtenstein. The AI Act is currently at the EEA review stage; it will only be formally incorporated into EEA law after a decision by the Draft Joint Committee. Moreover, a Swiss company may therefore be subject to the AI Act if it sells an AIS to or in the EU (as a provider, importer or distributor); sells another product in the EU that uses an AIS as a component; or generates output that is used in the EU.

Unlike the GDPR, the AI Act itself does not contain any provisions for fines, but in Article 99 it requires member states to introduce provisions for fines, as well as other enforcement measures. Fines can be imposed on all actors – ie, on all entities involved in the value chain. Depending on the type of violation, the fines can reach up to EUR35 million or 7% of the turnover.

In Switzerland, however, there is currently no overarching regulation on the use of AI (see **6.2 Cybersecurity and AI** in the Swiss Law and Practice chapter in this Guide). At the end of 2023, the Swiss Federal Council commissioned the Federal Department of the Environment, Transport, Energy and Communications (DETEC) to explore possible approaches for regulation within the framework of the Interdepartmental Coordination Group on EU Digital Policy, by the end of 2024, and a report was published on 11 February 2025.

As a result, AI is currently governed in Switzerland by general laws, depending on the legal object affected by the use of AI, such as:

- the data protection law (if personal data is processed during training or use);
- the secrecy protection law (if secret information is used for training or as an input);
- the employment contract law (if the personal data of applicants and employees is processed and if AI affects the employer's duty of care);
- public labour law (eg, when duties to co-operate take effect or when monitoring behaviour is discussed);
- personal rights (eg, when conversations or team calls are recorded);
- unfair competition law (when AI-generated content can be misleading);
- copyright law (eg, when AI is trained with works or uses works as input, and when the protection of output is under discussion);
- criminal law (when recording non-public conversations or when using AI for punishable behaviour in general);
- product liability and other liability laws; and
- other areas of law.

Private actors have also issued rules for themselves in the meantime. On 18 December 2024, FINMA published its Guidance 08/2024 – Governance and risk management when using AI, and numerous private companies have also issued or are in the process of issuing guidelines, codes and instructions, some of which are public and some of which are not.

At the end of 2023, the Swiss Federal Council commissioned DETEC to explore possible approaches for regulation within the framework of the Interdepartmental Coordination Group on EU Digital Policy, by the end of 2024. Based on this mandate, on 12 February 2025, DETEC and the Federal Department of Foreign Affairs (FDFA) presented an overview to the Swiss Federal Council of possible regulatory approaches to AI. On the basis of this overview, the Swiss Federal Council has decided on a Swiss regulatory approach for AI based on three objectives: strengthening Switzerland's location for innovation; safeguarding the protection of fundamental rights, including economic freedom; and increasing public trust in AI. To achieve these objectives, the Swiss Federal Council has set the following key steps for the future: incorporation of the Council of Europe's AI Convention (which Switzerland signed on 27 March 2025) into Swiss law; sector-specific legislation as far as required (cross-sector regulation, to be limited to central areas relevant to fundamental rights); and non-binding measures. Finally, the Swiss Confederation has developed a strategy for the use of AI within the federal administration. This strategy is structured around three pillars: strengthening AI-related competencies within the federal administration; enhancing trust in AI by establishing the conditions under which AI systems may be used in accordance with shared values and rules; and improving administrative efficiency.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com