Legal 500
Country Comparative Guides 2025

Switzerland

Data Protection & Cybersecurity

Contributor

Bär & Karrer Ltd.

Christian Kunz

Partner | christian.kunz@baerkarrer.ch

Ferdinand Rombach

Associate | ferdinand.rombach@baerkarrer.ch

Katharina Schreiber

Associate | katharina.schreiber@baerkarrer.ch

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Switzerland.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Switzerland: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered; what sectors, activities or data do they regulate; and who enforces the relevant laws).

In Switzerland, data protection, privacy and cybersecurity are primarily governed by the Swiss Federal Act on Data Protection of 25 September 2020 (Data Protection Act, FADP), together with the Swiss Federal Ordinance on Data Protection of 31 August 2022 (Data Protection Ordinance, FODP), both effective since 1 September 2023. Although the FADP is aligned with the EU GDPR in many respects, it has not just simply adopted its provisions on a one-to-one basis. Therefore, organizations operating in both the EU and Switzerland must keep in mind the specificities of Swiss data protection regulations.

The FADP applies to the processing of personal data of natural persons by private persons and federal bodies. Cantonal or communal authorities follow their own cantonal data protection laws, which also extend to private companies only if they perform a public service mandate. The FADP may have extraterritorial effect on controllers and processors established outside Switzerland when their processing activities have an effect in Switzerland (e.g., if they process personal data of a larger number of individuals located in Switzerland).

Additional sectoral rules apply to areas such as banking, insurance, and telecommunications. Financial institutions regulated by the Swiss Financial Market Supervisory Authority (FINMA) must meet stringent confidentiality and cyber- and information-security obligations.

The Federal Data Protection and Information Commissioner (FDPIC) is responsible for enforcing the FADP, conducting investigations, and issuing recommendations. In serious cases, administrative or criminal sanctions may be imposed by the competent criminal prosecution authorities on individuals (particularly against individuals who, for example, intentionally obstruct investigations or unlawfully disclose personal data). At the cantonal level, cantonal data protection authorities may hold competence over public bodies in their respective cantons.

Switzerland does not have a single comprehensive cybersecurity act but instead relies on various laws and regulations. Criminal offences involving unauthorised access to IT systems, hacking and malware are primarily addressed by the Swiss Federal Criminal Code (SCC), which criminalises computer misuse, data theft and related offences. The Swiss National Cyber Strategy, first adopted in 2012 and updated periodically, sets strategic objectives and encourages public-private cooperation to enhance cybersecurity. The National Cyber Security Centre (NCSC) monitors cyberthreats and works closely with industry to improve cyber resilience. Operators of critical infrastructure — including those in the energy, telecommunications, defence, and related sectors — are subject to additional obligations regarding risk assessments and the reporting of information security incidents to the NCSC. In finance, FINMA Circulars impose duties to maintain adequate IT security systems and to notify FINMA of cyber incidents.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

Switzerland's revised FADP only recently took effect in September 2023. Further, since January 2024, the new Information Security Act (ISA) is in force, which consolidates the key legal foundations for the security of the federal government's information and IT resources into a single law. A key provision, which came into effect on 1 April 2025, is the mandatory reporting of cyberattacks on critical infrastructure. Operators of critical infrastructure are required to report cyberattacks to the National Cyber Security Centre (NCSC) within 24 hours of discovery. See Q40 for additional information.

At present, no overarching new legislation in the area of data protection, privacy or cybersecurity has been announced for 2025 – 2026. However, there may be further refinements or regulatory guidance within this timeframe, partly in response to ongoing developments at both EU and international levels (for instance, in connection with changes in cross-border data transfer frameworks).

3. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

In Switzerland, there is no general registration or licensing requirement under the FADP. In other words, private companies that process personal data are not required to formally register with, or obtain a licence from, the Federal Data Protection and Information Commissioner (FDPIC) simply on account of processing personal data.

Unlike under the EU GDPR, only federal bodies must appoint a data protection officer (DPO). For private companies, appointing a DPO is voluntary. However, if a private company wishes to avoid the obligation to notify the FDPIC of its data protection impact assessment outcomes, it must appoint and register a DPO with the FDPIC. In addition, the revised FADP requires data controllers, with the exception of SMEs with fewer than 250 full-time employees, to maintain internal records of their data processing activities.

4. How do the data protection laws in your jurisdiction define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data")? Do such laws include a specific definition for special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction (e.g., "controller", "processor", "data subject", etc.)?

Similar to the definition set out in the EU GDPR, the FADP defines "personal data" as any information relating to an identified or identifiable natural person. "Sensitive personal data" is defined slightly more broadly than under the EU GDPR, encompassing information relating to religious, philosophical, political, or trade union-related views or activities, health, the intimate sphere or affiliation to a race or ethnicity, genetic data, biometric data that uniquely identifies a natural person, details about administrative or criminal proceedings or sanctions, and data relating to social assistance measures.

Furthermore, the FADP defines a "data subject" as a natural person whose personal data is processed.

"Processing" refers to any operation with personal data, regardless of the means or procedures used, and includes in particular the collection, recording, storage, use, modification, disclosure, archiving, deletion, or destruction of such data. The term "disclosure" denotes transmitting or making personal data accessible, while the "controller" is any private person or federal body that alone or jointly with others decides on the purpose and means of the processing, and the "processor" is any private person or federal body that processes personal data on behalf of the controller.

The FADP also defines "profiling", "high-risk profiling", "data security breach", and "federal body".

5. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

The FADP encompasses several core principles relating to the processing of personal data. First, the law requires that personal data be processed lawfully (principle of legality), in good faith (principle of good faith), and in accordance with the principle of proportionality, meaning that data may only be processed in a manner that is suitable, required, and necessary to achieve the intended purpose. The processing must therefore be limited to the minimal amount of data and the shortest duration necessary to achieve the specific purpose. While not explicitly mentioned, the principle of good faith is understood to encompass transparency. Data controllers must thus ensure that data subjects know how, why, and by whom their personal data is processed, including any disclosures to third parties. Under the FADP, contrary to the EU GDPR, data subjects must also be informed about the recipient countries to which their data is transferred, together with any safeguards or statutory exceptions relied upon.

Additionally, personal data may only be collected for a specific purpose that is evident to the data subject (principle of purpose limitation), and the data must not be processed in a way that is incompatible with that purpose. Further, every appropriate measure must be taken to ensure personal data is accurate (principle of data accuracy). In keeping with that principle, any data found to be inaccurate or incomplete in light of its processing purpose must be corrected, deleted, or destroyed.

In conceptual contrast to the EU GDPR, which requires a specific legal basis for any processing of personal data, the FADP allows data processing without such basis, provided that the controller observes these core principles of data processing. A legal justification becomes necessary only where a breach of these principles occurs. In such cases, the controller must be able to demonstrate an appropriate justification, such as valid consent from the data subject, an overriding private or public interest, or a statutory basis. Notably, Swiss law does not enumerate these justifications as exhaustively as the EU GDPR does in Article 6.

Although the FADP does not impose a strict maximum data retention period, personal data must be deleted or rendered anonymous once it is no longer needed for the purpose for which it was originally collected. Retaining data beyond what is necessary risks infringing the principle of proportionality. Consequently, controllers should adopt clear internal data retention policies detailing how long data is kept and establishing procedures for the secure deletion or anonymization of personal data.

Finally, although not expressly framed as a data processing principle under the FADP, controllers and processors must at all times preserve data security (that is, the confidentiality, integrity, and availability of the data) by implementing appropriate technical and organisational measures (TOMs).

6. Are there any circumstances for which consent is required or typically obtained in connection with the processing of personal data? What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

Under the FADP, consent is generally not required for processing personal data. However, if a controller breaches any of the data processing principles (*i.e.*, lawfulness, proportionality, good faith, purpose limitation, or data accuracy; see question 5 above), the controller must be able to justify its processing activity – for example, by the affected data subject's consent, an overriding private or public interest, or a statutory basis. If a controller elects to rely on consent as the legal basis for processing, the following applies:

- **Freely given, specific, informed**: Consent must be given voluntarily and based on clear, comprehensible information regarding the nature, scope and purpose of processing: Data subjects should know what data is processed, why it is processed, how it is used, and whether any transfers occur (including relevant safeguards or exceptions).
- **Form requirements**: No strict rule mandates written or signed consent, though verifiable consent is advisable. If a controller relies on consent to process sensitive personal data or conducts high-risk profiling, or if a federal body conducts profiling, such consent must be explicitly given. The same applies where a controller intends to rely on consent as a statutory exception to transfer personal data to a third country or international body that does not guarantee an adequate level of protection.
- **Implied Consent**: Permissible if the data subject's intent is clear and the privacy intrusion minimal. The controller must demonstrate that consent was informed.
- **Bundled Consent**: Incorporating consent into broader documents (e.g., terms of service) is permissible, provided that data subjects are clearly informed of the specific processing activities to which they are consenting. Multiple separate processing activities should be clearly distinguished.

7. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

Because the FADP follows a "risk-based" approach, the processing of sensitive personal data must meet higher standards than the processing of personal data involving lower risks. Article 5 lit. c FADP defines "sensitive personal data" (see also Q4).

Under the FADP, the disclosure of sensitive personal data to third parties is *per se* considered a violation of personality rights unless justified by the data subject's *explicit* consent, by law, or by an overriding private or public interest. In practice, such overriding private or public interests rarely exist; thus, explicit consent is the primary legal basis for disclosure in the absence of a specific statutory provision.

Notably, Article 6 para. 7 FADP does not introduce a general obligation to obtain consent for processing sensitive personal data. Instead, it specifies that, if

controllers rely on consent as their justification for processing sensitive personal data, the consent must be given *explicitly*.

Additionally, under the FADP, controllers must conduct a data protection impact assessment (DPIA) where the intended data processing is likely to result in a high risk to the personality or fundamental rights of the data subject. The FADP explicitly recognizes the large-scale processing of sensitive personal data as a high-risk activity that triggers the obligation to conduct a DPIA.

Furthermore, federal authorities must generally only process sensitive personal date where there is a statutory basis in a formal law. A statutory basis in a substantive law is only sufficient as the basis for processing sensitive personal data if the processing is essential for a task required by a formal law and the purpose of processing poses no particular risks to the data subject's fundamental rights.

Although the FADP does not specifically categorize *children*'s data as sensitive, the Federal Data Protection and Information Commissioner (FDPIC) acknowledges the heightened level of protection that must be afforded to children's data. Enhanced protective measures typically include (i) ensuring informed consent is provided by a legal guardian and (ii) presenting privacy information in clear, age-appropriate language and supplemented by visual aids — such as pictograms or symbols — to facilitate understanding by children.

8. Do the data protection laws in your jurisdiction include any derogations, exemptions, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

The FADP does not apply to in the following situations:

- **Household exemption**: When personal data is processed by a natural person exclusively for personal use.
- **Parliamentary activities**: When personal data is processed by the Federal Assembly and parliamentary committees as part of their deliberations.
- **Entities with immunity**: When personal data is processed by institutional beneficiaries under Article 2 para. 1 of the Host State Act of 22 June 2007, which enjoy immunity from jurisdiction in Switzerland.

Additionally, data processing and data subject rights in court proceedings and other proceedings governed by federal procedural law are subject to the applicable procedural laws. However, in administrative proceedings of first instance, the FADP applies.

Finally, the FADP does not apply to public registers concerning private law transactions, in particular with respect to access to these registers and data subject rights, where such matters are regulated by specific provisions under applicable federal law. In the absence of such special provisions, the FADP remains applicable.

9. Does your jurisdiction require or recommend risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

The FADP requires data controllers to carry out a data protection impact assessment (DPIA) when the intended processing of personal data is likely to result in a high risk to the personality or fundamental rights of the data subjects.

A DPIA is mandatory particularly in situations where sensitive personal data is processed on a large scale, where systematic monitoring of publicly accessible areas takes place, or where new technologies are used in ways that significantly increase risks to individuals. The assessment must evaluate whether the data processing is necessary and proportionate in light of its intended purpose and identify any risks that may arise for the data subjects.

If high risks are identified, the controller must also outline the measures planned to mitigate those risks. In cases where the identified risks cannot be adequately mitigated, the controller is required to consult with the Federal Data Protection and Information Commissioner (FDPIC) before commencing processing, unless the controller previously consulted with its data protection officer (DPO).

Although the FADP does not prescribe a specific format for DPIAs, best practice involves documenting the nature and purpose of the processing, evaluating the necessity and proportionality of the data collection, assessing potential risks, and defining appropriate measures to mitigate those risks. DPIAs should be conducted at an early stage – ideally during the planning and design phase of the processing activity – and must be reviewed and updated where there is a substantial change in the nature, scope, or context of the processing.

The FDPIC has issued a factsheet to assist controllers in complying with Articles 22 and 23 FADP including a flowchart for the preliminary assessment of whether a

DPIA must be carried out as well as a template for structuring a DPIA.

Further, the FDPIC provides detailed information on the DPIA (in German, French and Italian) on its website. While the information is primarily aimed at federal bodies, the guidelines are also helpful for private companies.

10. Are there any specific codes of practice applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

At present, Switzerland does not have binding sector-specific codes of practice (codes of conduct) formally issued or approved by the Federal Data Protection and Information Commissioner (FDPIC) under the law.

11. Are organisations required to maintain any records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Yes, under the FADP, organisations are required to maintain records of their data processing activities and establish internal documentation and processes to ensure compliance with data protection obligations.

Specifically, Article 12 FADP mandates both controllers and processors to maintain a register of their processing activities (ROPA) and, if requested, make it available to the Federal Data Protection and Information Commissioner (FDPIC).

Controllers, as a minimum, are obliged to record (i) the identity of the controller, (ii) the purpose of processing, (iii) a description of the categories of data subjects and the categories of processed personal data, (iv) the categories of recipients, (v) if possible, the retention period for the personal data or the criteria for determining this period, (vi) if possible, a general description of the measures taken to guarantee data security, (vii) if data is disclosed abroad, details of the recipient state and the guarantees applied.

The processor's record shall contain (i) information on the identity of the processor and of the controller, (ii) the categories of processing carried out on behalf of the controller, (iii) if possible, a general description of the measures taken to guarantee data security, and (iv) if data is disclosed abroad, details of the recipient state and the guarantees applied.

There is an exemption from the obligation to maintain such records for companies with fewer than 250 employees, provided they are not processing sensitive personal data on a large scale, conducting high-risk profiling, or engaging in processing activities that present a high risk to the data subjects' rights.

While the FADP does not specify a particular format, Swiss organisations typically meet these requirements in practice by adopting templates (e.g., an excel spreadsheet or word document) or specialized IT tools – often aligned with the EU GDPR – to maintain their ROPAs.

In addition to maintaining a ROPA, organisations are also expected to document other key compliance processes. These include conducting and retaining records of data protection impact assessments (DPIAs) where required, documenting consent when it is used as a legal basis for processing, establishing written contracts with processors, and implementing internal policies and procedures for handling data subject requests and ensuring data security.

12. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

Under the FADP, there is no explicit obligation to adopt formal data retention or data disposal policies. However, the principles embedded in the FADP – in particular, the principles of proportionality (data minimization), purpose limitation and storage limitation – effectively require organisations to implement appropriate practices for retaining and deleting personal data.

The FADP mandates that personal data must only be processed for as long as it is necessary to achieve the purpose for which it was originally collected. Once that purpose has been fulfilled, the data must be either anonymised or deleted, unless a valid legal basis (such as a statutory retention obligation) justifies continued storage. In practice, this implies that organisations must implement internal mechanisms to monitor applicable retention periods and ensure timely and secure disposal of data.

Although the law does not require written data retention or deletion policies, organisations are strongly recommended to implement documented policies and

procedures to support compliance with these principles. This includes defining specific retention periods for various categories of personal data, regularly reviewing stored data to assess its necessity, and securely deleting or anonymising data that is no longer required.

In practice, Swiss businesses often integrate these policies into broader data lifecycle or information governance frameworks, supported by technical controls.

13. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

Similar to the EU GDPR, Swiss data protection laws oblige controllers to seek the Federal Data Protection and Information Commissioner's (FDPIC's) opinion if the data protection impact assessment (see Q19 for further information about data protection impact assessment requirements) carried out before the planned processing indicates that such processing will pose a high risk to the personality or the data subject's fundamental rights, despite any planned measures taken by the controller (Article 23 FADP).

The FDPIC will then take a position on the planned data processing. For instance, the FDPIC may raise objections to the planned processing and communicate them to the data controller. In this case, the FDPIC proposes suitable measures. If the FDPIC has general objections to the data protection impact assessment (e.g., if it finds the assessment too general, or if risks or measures are not described with sufficient detail), it advises the data controller to specify or supplement it.

While only obtaining an opinion and, ultimately, no "approval" or "authorization" from the FDPIC is required, there is a significant risk in ignoring the FDPIC's objections and proposed measures. Failure to address objections or proposed measures may likely result in an investigation opened by the FDPIC, and, moreover, in a violation of data protection law (e.g., data protection principles or data security), which could have corresponding civil and, if applicable, criminal consequences.

However, there are two exceptions to the obligation to consult with the FDPIC under Swiss data protection laws. First, if a data protection impact assessment was not required for a processing operation due to an exception according to Article 22 para. 4 or para. 5 FADP, consultation with the FDPIC is also not required. Further, a private controller may dispense with consulting the FDPIC if it has consulted with the data protection officer appointed by such controller.

In practice, businesses may also opt for voluntary consultation with the FDPIC to clarify the interpretation of the FADP, e.g., in contexts involving new technologies or cross-border data processing.

14. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

Contrary to the EU GDPR, there is no mandatory requirement for private organizations under the FADP to appoint a data protection officer (DPO), Chief Information Security Officer (CISO), or any other specifically named person responsible for data. It is only mandatory for federal bodies. Instead, the FADP provides for a voluntary appointment mechanism that allows data controllers to designate a *data protection officer* (referred to in the official versions of the FADP in German and French as *Datenschutzberater* or *conseiller à la protection des données*).

While optional, this designation can bring tangible benefits. If a data controller chooses to appoint a data protection officer in accordance with Article 10 FADP, that person must be both qualified and independent in their function. Their role includes advising the organisation on its data protection obligations, monitoring internal compliance with data protection policies, and supporting the execution of data protection impact assessments (DPIAs). Importantly, where a data protection officer has been duly appointed and is involved in the execution of DPIAs, the organisation may be exempt from the requirement to consult the Federal Data Protection and Information Commissioner (FDPIC) prior to initiating high-risk data processing. While the data protection officer advises the company on data protection, the responsibility for ensuring that personal data is processed in compliance with data protection requirements remains with the data controller.

The FADP does also not require the appointment of a CISO, nor does it set out specific responsibilities for such a role. However, Article 8 of the FADP mandates that data controllers implement appropriate technical and organisational measures (TOMs) to ensure data security. In practice, especially for larger organisations or those processing sensitive or high volumes of personal data, appointing a CISO or similar role is considered a best

practice for meeting these obligations, even though it is not a legal requirement.

15. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s) or recommendation(s).

Under the FADP, there is no explicit legal obligation to conduct employee training. However, such training is strongly recommended as part of the duty to implement appropriate technical and organisational measures (Article 8 FADP).

While the law does not prescribe specific content or frequency, the Federal Data Protection and Information Commissioner (FDPIC) encourages regular training, particularly for staff handling personal or sensitive data. Training typically covers lawful processing, data security, breach reporting, and handling data subject rights. In practice, providing data protection training is a key component of ensuring compliance and reducing the risk of human error.

16. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

Under the FADP, data controllers are **legally required** to inform data subjects about their data processing activities. This duty is grounded in the principle of **transparency** and enshrined in **Article 19 FADP**.

Controllers must inform data subjects ***at the time of collection*** – whether the data is collected directly from the individual or obtained from third-party sources. The notice must include key information that enables individuals to understand how their personal data will be used and to exercise their rights. Specifically, the law requires disclosure of at least (i) the controller's identity and contact details; (ii) the purpose of processing; (iii) if applicable, the recipients or the categories of recipients to which personal data is disclosed (e.g. sub-processors), and (iv) if data is transferred abroad, the destination country and any safeguards in place or exceptions relied upon (which goes beyond the requirements under the EU GDPR).

If the data is **not collected directly** from the data subject, the controller must also inform the individual of the **categories of personal data** processed.

While the FADP does not prescribe a specific form for providing notice, it specifies controllers must provide information in a precise, transparent, comprehensible, and easily accessible manner (Article 13 FODP).

In practice, many organisations fulfill this obligation by publishing a **privacy notice online,** typically on their website, and supplementing it with additional disclosures in contracts, forms or apps. For employees, many organisations provide the information in separate employee privacy notices or the employee handbook.

17. Do the data protection laws in your jurisdiction draw any distinction between the responsibility of controllers and the processors of personal data? If so, what are the implications?

Under the FADP, the law makes a clear distinction between the roles of data controllers and data processors, each carrying distinct responsibilities. A controller is the party that, alone or jointly with others, determines the purpose and means of processing personal data (Article 5 lit. j FADP), while a processor handles personal data on behalf of the controller (Article 5 lit. k FADP).

The FADP places the primary legal responsibility for compliance on the controller. Controllers are obligated to ensure that all data processing activities adhere to the data processing principles (lawfulness, proportionality, good faith, purpose limitation, and data accuracy). They must establish appropriate technical and organisational measures to ensure data security, maintain records of processing activities, inform data subjects of the processing and assess data protection risks through data protection impact assessments (DPIAs) where necessary. In the event of a data breach, it is the controller who must notify, where applicable, the Federal Data Protection and Information Commissioner (FDPIC) and the affected individuals. And private controllers with their domicile or residence abroad must designate a representative in Switzerland, where necessary.

Processors, by contrast, have a more limited role. They must process personal data only in accordance with the controller's instructions. They must seek approval before engaging sub-processors, establish appropriate technical and organisational measures to ensure data security and maintain records of processing activities.

To formalise this relationship, the FADP requires that controllers enter into a *data processing agreement* (DPA) with their processors (Article 9 para. 1 FADP). The DPA outlines the scope of the processing, the processor's duties, including the obligation to act solely on the controller's instructions, to establish appropriate technical and organisational measures to ensure data security and to notify the controller of data breaches. It typically also addresses other key aspects such as sub-processing arrangements, the return or deletion of personal data, the handling of data subject rights, and the controller's audit rights.

The practical implication of this division of roles is that controllers remain primarily responsible for ensuring compliance with applicable data protection obligations, irrespective of any delegation of processing activities to processors. Accordingly, controllers are required to exercise **appropriate due diligence** in the **selection, instruction, and ongoing supervision** of their processors. Conversely, while processors act on behalf of the controller, they are nonetheless obliged to **adhere strictly to the controller's instructions** and fulfil their contractual and statutory duties with care, as failure to do so may result in **liability exposure**, particularly where the processor acts beyond or contrary to its authorised mandate.

18. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these or any similar terms defined?

Monitoring

Swiss data protection laws do not explicitly address monitoring and therefore do not define the term “monitoring". However, the FADP, along with its Ordinance, nevertheless applies if a monitoring system processes personal data. In particular, the data processing principles of good faith, transparency and proportionality (Article 6 paras. 2 and 3 FADP) must be complied with.

In practice, monitoring becomes most relevant within the context of employment relationships. According to Article 328 lit. b of the Swiss Code of Obligations, processing employee personal data is permitted only to assess the employee's suitability for the job or if it is necessary for the performance of the employment contract. Article 26 of the Ordinance 3 to the Swiss Employment Act prohibits the use of monitoring systems to monitor the behaviour of employees in the workplace.

Profiling / High-Risk Profiling

Under the FADP (as under the EU GDPR), *profiling* is defined as any form of automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements (Article 5 lit. f). Profiling may serve various purposes, including risk assessment, behavioural analysis, or targeted marketing, is very common in practice and has no specific legal consequences for private controllers under the FADP. Profiling must be made sufficiently transparent and data subjects must be informed about the categories of data created through profiling (e.g., preference data).

A qualified form of profiling and specialty under the FADP is *high-risk profiling*, which is defined as profiling that poses a high risk to the personality or fundamental rights of the data subject by linking data that allows for an assessment of essential aspects of a natural person's personality (Article 5 lit. g). In this respect, the FADP deviates from the EU GDPR, which only recognizes qualified profiling in connection with automated individual decisions. The classification as high-risk profiling depends heavily on the individual case and triggers the controller's obligation to carry out a data protection impact assessment (DPIA) but does not lead to a general consent requirement. However, if the controller relies on consent to justify a high-risk profiling if a processing principle has been violated and there is no other justification, such consent must be given explicitly (Article 6 para. 7 lit. b FADP). Further, the overriding interest in creditworthiness checks is irrelevant if the check is based on high-risk profiling (Article 31 para. 2 lit. c no. 1 FADP).

Automated Decision-Making

If a decision is taken exclusively on the basis of an automated processing and has legal effects on the data subject or affects him significantly, the FADP obliges the controller to specifically inform the data subject of such *automated individual decision* and to give the data subject upon request the opportunity to state his position. Contrary to the EU GDPR, controllers are not required to proactively provide meaningful information about the underlying logic. The data subject can request that the decision be reviewed by a human, which reinforces that no one should be subject to an autonomous decision by a machine if they do not want to

be. No information is required, and no right to state the position needs to be granted or human review can be requested, if either the automated decision is directly related to the conclusion or performance of a contract and fulfills the data subject's request, or the data subject has explicitly consented to the automated decision-making.

Unlike the EU GDPR (Article 22 para. 1), profiling is not necessarily considered automated individual decision-making under the FADP. For instance, if a retail company employee uses a computer to analyse customer behaviour (such as purchase history, browsing patterns, and demographic data) and the system suggests segmenting customers into marketing groups like "frequent buyers", "discount seekers", or "luxury shoppers" for targeted promotional emails, this constitutes profiling. However, if the employee reviews and approves the segmentation before any emails are sent, the decision is not made solely by automated means. In this scenario, there is profiling, but no automated individual decision-making within the meaning of the FADP.

Tracking Technologies and Cookies

Although the FADP does not specifically name cookies or browser tracking technologies, their use falls within the scope of personal data processing if they collect identifiable user information. In such cases, the FADP applies.

The Federal Data Protection and Information Commissioner (FDPIC) has clarified that the use of tracking technologies requires *user notification* and, depending on the nature and intrusiveness of the technology, potentially *prior consent*. This is especially relevant if particularly sensitive personal data is processed through cookies or if high-risk profiling is conducted (Article 6 para. 7 FADP), or for third-party cookies used for behavioural advertising or cross-site tracking. For purely functional cookies necessary to operate a website, consent is not required ("opt-out"), though disclosure is still advisable. Switzerland also aligns with European standards in practice. Websites accessible from the EU commonly implement cookie banners or consent management platforms that comply with both Swiss and EU rules. In addition to the FADP, the Swiss Federal Telecommunications Act (TCA) obliges website operators to inform website users about their use of cookies (or similar techniques such as web-beacons) and the purpose of such use (Article 45c lit. b TCA). Swiss companies typically comply with this obligation by publishing a privacy and cookies policy on their website.

19. Please describe any restrictions on targeted advertising and/or behavioral advertising. How are these terms or any similar terms defined?

Under the FADP, targeted advertising and behavioral advertising are not explicitly defined as legal terms. However, these practices are regulated to the extent that they involve the processing of personal data, particularly through profiling and tracking technologies. The key restrictions arise from the FADP's general principles, especially lawfulness, transparency, purpose limitation, and proportionality as well as from the controller's duty to inform users about such practices (typically via privacy notices or cookie banners) and grant users an "opt-out" option or obtain their consent ("opt-in"), as required.

20. Please describe any data protection laws in your jurisdiction restricting the sale of personal data. How is the term "sale" or such related terms defined?

Under the FADP, there is no explicit prohibition or definition of the "sale" of personal data. Instead, it treats any disclosure of personal data to a third party – whether for payment, benefit, or free of charge – as a form of data processing, subject to the general requirements of the FADP.

21. Please describe any data protection laws in your jurisdiction restricting telephone calls, text messaging, email communication, or direct marketing. How are these terms defined?

While the FADP and its general data protection principles apply to the processing of personal data within electronic advertising practices, the Swiss Federal Act on Unfair Competition (UCA) sets forth specific regulations that must be observed.

Direct Email or Text Messaging (SMS) Marketing

Mass mailing of advertising messages via telecommunications is primarily regulated by Article 3 para. 1 lit. o UCA. In principle, mass advertising by email or text messaging (SMS) is only permissible with the recipients' prior voluntary and express consent (i.e., opt-in). For consent to be valid, recipients must have been adequately informed, in particular about the use of their email address for marketing purposes as well as their right to withdraw their consent at any time. Additionally, each mass marketing email must contain the correct name, address, and email contact of the sender, and

provide an option to easily opt-out of future emails at no cost (e.g. by providing a link to unsubscribe).

As an exception, a recipient's consent is not required (i.e., opt-out) if (i) the recipient is a customer of the sender, (ii) the advertising concerns similar products or services of the sender, and (iii) upon the first collection of the recipient's contact information, the recipient was given the opportunity to object to its use of it for marketing purposes.

Violation of the UCA's requirements constitutes unfair competition, which may lead to civil and criminal penalties. Affected recipients may also file a complaint with the Swiss State Secretariat for Economic Affairs (SECO).

Direct Marketing by Telephone

Under Swiss law, direct telephone marketing is generally permitted as long as the person whose data is being used has made their address and telephone number publicly accessible and unless it is not done in an aggressive way (e.g. by repeatedly calling the same person).

Article 3 para. 1 lit u UCA prohibits the use of addresses and telephone numbers for advertising purposes if the recipients are not listed in the Swiss telephone directory or if their information is marked with an asterisk (*) in the telephone directory (i.e., opt-out). Furthermore, making advertising calls without displaying a telephone number that is listed in the directory and for which there is a right of use constitutes an act of unfair competition (Article 3 para. 1 lit. v UCA).

22. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined?

The FADP classifies “biometric data that uniquely identifies a natural person" – facial recognition systems that extract and analyse facial features for identification or authentication falls into this category – as *sensitive personal data* (Article 5 lit. c FADP). This classification imposes additional restrictions, which are explained in more detail in the section regarding sensitive personal data under Q4.

23. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning (“AI”).

While artificial intelligence and machine leaning are not explicitly addressed, the FADP follows a technology-neutral approach, rendering it directly applicable to all AI-supported data processing, which the Federal Data Protection and Information Commissioner (FDPIC) emphasized in a statement issued in November 2023. One of the most direct legal mechanisms impacting AI is Article 21 FADP, which grants data subjects the right not to be subject to decisions based solely on automated processing that has legal effects on the data subject or affects him significantly (see Q19 hereto). This encompasses many AI-driven decisions, such as credit scoring, automated hiring systems, or pricing algorithms.

In February 2025, the Swiss Federal Council decided not to introduce a Swiss equivalent of the EU AI Act, but to ratify the Council of Europe's Convention on AI and to amend Swiss law where necessary and as sector-specific as possible. Cross-sector rules will be limited to critical areas like data protection.

24. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

Swiss data protection law places specific restrictions on cross-border transfers of personal data. Under the FADP, a cross-border transfer occurs when personal data is either transmitted to, or made accessible by, a recipient located outside of Switzerland.

According to the FADP, private entities and federal bodies may transfer personal data abroad only if the destination country ensures an *adequate level of data protection* based on its legislation (Article 16 para. 1 FADP). The Swiss Federal Council maintains a list of such countries, territories, specific sectors, and international bodies in Annex 1 of the Data Protection Ordinance (FODP). This list largely aligns with the European Commission's adequacy decisions; however, notable exceptions exist: Japan and South Korea have been granted adequacy status by the EU, but not by Switzerland.

If the destination does not offer an adequate level of protection, transfers are only permitted if *appropriate safeguards* are in place pursuant to Article 16 para. 2 FADP, or if a *statutory exception* applies under Article 17 FADP. Appropriate safeguards include standard contractual clauses (SCCs) approved by the Federal Data Protection and Information Commissioner (FDPIC), such

as the post-*Schrems II* EU SCCs with Swiss-specific adaptations, and binding corporate rules (BCRs). In practice, Swiss companies frequently rely on SCCs as the primary mechanism for securing such transfers.

In line with the CJEU's *Schrems II* decision (Case C-311/18, July 2020), Swiss data exporters are also expected to conduct a *data transfer impact assessment (DTIA)* to evaluate whether the legal framework of the recipient country undermines the protections provided by the SCCs. Where risks are identified, *supplementary measures* may be required to ensure an equivalent level of data protection.

Specifically with respect to data transfers to the *United States*, the Swiss Federal Council has recognized the U.S. Data Privacy Framework (DPF) as providing an adequate level of protection for Swiss personal data, but only for U.S. organizations that are self-certified under the Swiss–U.S. DPF. This adequacy determination facilitates transfers to certified U.S. entities without the need for additional safeguards. However, for transfers to U.S. entities that are not certified under the Swiss-U.S. DPF, organisations must rely on alternative safeguards (such as SCCs) and conduct a DTIA.

25. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

Under the FADP, data controllers and processors are required to implement appropriate personal data security measures. Article 8 FADP establishes a general obligation to ensure the confidentiality, availability and integrity of personal data by adopting suitable technical and organisational measures (TOMs). These measures must be proportionate to the risks associated with the data processing activities. *Minimum* security requirements are further specified in Article 3 of the Data Protection Ordinance (FODP).

While the FADP does not prescribe specific technologies or controls, it adopts a principles-based, risk-oriented approach. In practice, organisations are expected to implement access controls, encryption, secure data storage and transmission protocols, regular data integrity checks, backup and recovery procedures, and other industry-standard practices.

In the event of a data breach, Article 24 FADP requires data controllers to notify the Federal Data Protection and Information Commissioner (FDPIC) as soon as possible – though the FADP does not impose a fixed 72-hour deadline as under the EU GDPR. Notification is mandatory where the breach is likely to result in a high risk to the personality or fundamental rights of affected individuals. Where necessary for their protection, or upon request by the FDPIC, the controller must also inform the affected data subjects.

When a data controller engages a data processor, the data processing agreement (DPA) must obligate the processor to implement appropriate TOMs and to promptly notify the controller in the event of a personal data breach (see Q18).

In January 2024, the FDPIC published an updated "Guide to Technical and Organisational Data Protection Measures (TOM)", aimed at supporting companies in assessing and implementing appropriate TOMs under the FADP.

26. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

In the FADP, the term "data security breach" is defined as any breach of security resulting in the accidental or unlawful loss, deletion, destruction or alteration of personal data or the disclosure of or access to personal data by unauthorised persons (Article 5 lit. h FADP).

In the event of a data breach, Article 24 FADP requires data controllers to notify the Federal Data Protection and Information Commissioner (FDPIC) as soon as possible – though the FADP does not impose a fixed 72-hour deadline as under the EU GDPR. Notification is mandatory where the breach is likely to result in a high risk to the personality or fundamental rights of affected individuals. Where necessary for their protection, or upon request by the FDPIC, the controller must also inform the affected data subjects. See Q25 for more information on security breach notification requirements.

27. Do the data protection laws in your jurisdiction establish specific rights for individuals, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are

exercised, and any exceptions.

The FADP establishes several specific rights for individuals regarding their personal data (while largely aligned with the EU GDPR in substance, the FADP tends to be less prescriptive and more flexible in its implementation), such as:

- **Right to access**: Under Article 25 para. 1 FADP, data subjects may request confirmation from a controller as to whether their personal data is being processed. If so, the controller must provide, at minimum: (i) the identity and contact details of the controller, (ii) the personal data being processed, (iii) the purposes of the processing, (iv) the retention period or, if not available, the criteria used to determine it, (v) the source of the data if not obtained directly from the data subject, (vi) the existence of any automated individual decision-making and the logic involved, and (vii) the recipients or categories of recipients to whom personal data is disclosed, if applicable, including, if abroad, their countries of residence or domicile and safeguards applied or exceptions relied upon. Requests must be made in writing, and controllers are generally required to respond within 30 days, although this may be extended. Controllers may refuse, restrict, or delay access under Article 26 FADP in cases where disclosure is restricted by Swiss law (e.g., professional secrecy), would affect overriding third-party interests, or the request is clearly unjustified (e.g., abusive or frivolous). Private controllers may also limit access based on their own overriding interests, provided the data is not intended to be disclosed to third parties.
- **Right to rectification**: Data subjects may request the correction of inaccurate personal data under Article 32 para. 1 FADP, unless such rectification is prohibited by law or the data is processed solely for archiving purposes in the public interest.
- **Right to erasure / "to be forgotten"**: The right to erasure is incorporated into the right to object under Article 30 para. 2 lit. b FADP (in conjunction with Article 32 para. 4 FADP). A controller may refuse deletion of data where legal retention obligations or overriding public or private interests apply, in accordance with Article 31 FADP.
- **Right to object**: Data subjects have the right to object to the processing of their personal data (*opt-out right*) under Article 30 para. 2 lit. b FADP. Controllers may however continue processing where necessary to fulfil legal obligations, contractual duties, or to protect overriding public or private interests as defined in Article 31 FADP.
- **Right to data portability**: According to Article 28 FADP, data subjects may request a copy of their personal data in a commonly used format (*e.*, a conventional electronic format that allows the personal data to be transmitted and reused by the data subject or another controller at a proportionate cost) or request its transfer to another controller, provided the data is processed automatically and based either on consent or on a contract with the data subject. As set out in the FODP, the copy must generally be provided within 30 days of receipt of the request, although this may be extended.

28. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

Yes, Swiss data protection law provides individuals with a private right of action to seek judicial redress through a combination of injunctive, corrective, and compensatory remedies in cases where their rights under the FADP have been infringed.

Under Article 32 para. 2 FADP, data subjects may bring civil claims before the competent courts if their personality rights have been violated due to unlawful processing of their personal data. The relevant provisions of the Swiss Civil Code (specifically Articles 28, 28a, and 28g to 28l) establish the general legal framework for protecting personality rights, which includes the right to data protection.

The remedies available through civil action are broad. Affected individuals may request that a court prohibit or suspend certain data processing activities, require the deletion or destruction of unlawfully processed personal data, or order the correction of inaccurate data. In addition, claimants may seek compensatory damages for financial loss, compensation for pain and suffering such as emotional distress or reputational damage, although Swiss courts grant such compensation only with considerable restraint, and, in some cases, the disgorgement of profits unlawfully obtained through misuse of personal data.

Legal proceedings must be initiated before the competent cantonal civil court, and the burden of proof generally lies with the claimant. Swiss law does not currently provide for class actions in data protection cases, so each individual must bring their own claim, though coordinated proceedings are possible when multiple individuals are affected by the same issue.

While the Federal Data Protection and Information Commissioner (FDPIC) can investigate data protection

violations and issue corrective orders, it does not have the authority to award damages. Therefore, the private right of action serves as the principal legal avenue for individuals seeking financial or injunctive relief for harm caused by violations of their data protection rights.

29. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been sustained, or is non-material injury to feelings, emotional distress or similar sufficient for such purposes?

The FADP allows affected individuals to pursue claims through the civil courts for both material and non-material harm resulting from unlawful processing of their personal data, as well as disgorgement of profits obtained through such processing.

The legal basis for such claims is found in Article 32 para. 2 FADP, which refers to the general protection of personality rights under the Swiss Civil Code, specifically Articles 28, 28a, and 28g–28l. These provisions allow individuals to seek redress when a violation of their personality rights (as manifested in the right to privacy and data protection) has caused them harm.

Swiss law recognizes two types of compensation:

- *Compensatory damages* for material (economic) loss: Individuals may claim compensation for financial loss resulting from a breach of data protection obligations.
- *Compensation for pain and suffering*: Swiss courts may also award compensation for non-economic harm, including emotional distress, reputational damage, anxiety, or infringement of personal dignity.

In practice, however, Swiss courts take a restrictive approach to awarding compensation for pain and suffering. Such compensation is typically granted only in cases where the non-material harm is serious, specific, and clearly substantiated. This cautious application reflects broader trends in Swiss tort law, which sets a relatively high threshold for awarding compensation for emotional or reputational injury.

30. How are data protection laws in your jurisdiction typically enforced?

The principal body responsible for overseeing compliance is the Federal Data Protection and Information Commissioner (FDPIC). Specifically, the FDPIC is authorized to:

- **Conduct investigations** and **audits**: The FDPIC may initiate inspections or inquiries, either proactively or in response to complaints from data subjects or data breach notifications. Investigations involve assessing whether entities or federal bodies comply with their obligations related to processing personal data.
- **Issue binding decisions** and **administrative measures**: Following an investigation, the FDPIC can issue binding rulings, prohibitions, or instructions to stop specific data-processing activities that violate the law, to delete data in whole or in part or to notify individuals about data breaches reported to the FDPIC (Article 49 para. 1 and Article 51 paras. 1 and 3 FADP). Such measures are enforceable, and entities and federal bodies are required to comply.
- **Recommend corrective actions**: In addition to enforcement actions, the FDPIC often provides guidance to organizations on how to rectify identified violations and comply with data protection standards.

However, unlike under the EU GDPR, where the data protection authorities have the authority to impose fines, the FDPIC does not have this authority. If an investigation reveals serious breaches of data protection obligations, the FDPIC may refer the case to the criminal prosecution authorities (see Q32).

The supervision of personal data processing by municipal and cantonal bodies falls within the responsibility of the cantonal data protection supervisory authorities.

Furthermore, data subjects who suffer harm due to breaches of their data protection rights have the option to enforce their rights directly through civil courts (see Q29, Q30 and Q32). Such civil remedies can run parallel to enforcement actions taken by the FDPIC.

31. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

The most serious violations – such as failure to provide adequate information to data subjects, breaches of access rights, non-compliance with cross-border data transfer rules or failing to comply with minimum data security standards can result in criminal fines of up to CHF 250'000 for the individual responsible (Articles 60 et seqq. FADP). These sanctions apply only in cases of intentional misconduct. Negligent acts are not punishable.

In contrast to the EU GDPR, where administrative fines

are imposed on the organization itself, the FADP places criminal liability primarily on natural persons who intentionally breach specific data protection obligations. Only in cases where the identity of the responsible individual cannot be determined without disproportionate investigative effort, the law allows for a fine of up to CHF 50'000 to be levied against the company (Article 64 para. 1 FADP).

Civil courts may award damages to affected data subjects and grant injunctive relief to stop unlawful processing. Additionally, individuals can seek restitution of profits derived from breaches and request the publication of judgments.

32. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

At present, Switzerland does not have an equivalent to the GDPR's fine guidance from the European Data Protection Board (EDPB) or any other rules or guidelines specific to the FADP regarding how fines or thresholds for sanctions are to be determined. Enforcement relies on general criminal law principles and case-by-case judicial discretion.

33. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Binding decisions of the FDPIC can be appealed to the Federal Administrative Court. The appeal must generally be filed within 30 days of notification of the decision. The Federal Administrative Court will assess whether the decision complies with federal law and can either uphold, amend, or annul the decision. Appeals against decisions of the Federal Administrative Court may be lodged with the Federal Supreme Court by the appellant and the FDPIC (Article 52 para. 3 FADP).

Binding decisions of cantonal data protection supervisory authorities can typically be appealed to the cantonal administrative courts in accordance with local cantonal laws.

Criminal convictions and fines imposed by cantonal criminal courts can be appealed to a higher cantonal court. Further appeals may be brought within a deadline of usually 30 (and in exceptional cases only 10) days of notification of the decision to the higher cantonal court to the Federal Supreme Court, but only on matters of federal law or constitutional rights.

Judgments from cantonal civil courts can generally be appealed to a higher cantonal court. If the amount in dispute exceeds CHF 30'000, or the case involves legal questions of fundamental importance, further appeals may be submitted to the Federal Supreme Court.

34. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

In Switzerland, enforcement around data protection has slightly intensified under the revised FADP which entered into force in September 2023. The Federal Data Protection Commissioner (FDPIC) is actively conducting proactive investigations, notably into the 2023 ransomware attack on Xplain, Digitec Galaxus' advertisement personalization strategies, and media companies' tracking practices. Reporting thresholds for data breaches in Switzerland are lower compared to the GDPR, necessitating heightened vigilance by businesses.

In the field of artificial intelligence and data protection, the FDPIC has emphasized transparency and user control concerning AI models trained on publicly available personal data. A preliminary review into the AI model “Grok”, which used personal data from X (formerly Twitter), has led to an opt-out mechanism for users.

In the healthcare sector, the FDPIC has prioritized oversight of initiatives involving sensitive patient data processing due to inherent privacy risks.

Given limited resources, legal enforcement by the FDPIC follows the principle of expediency, focusing primarily on severe violations, such as high-risk data leaks.

35. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide details.

Switzerland mandates specific risk management measures, particularly in regulated sectors and for operators of critical infrastructure. The Swiss Financial Market Supervisory Authority (FINMA) imposes detailed cybersecurity requirements on financial institutions, including obligations to implement ICT risk management systems, conduct vulnerability testing, use multi-factor authentication, maintain incident response capabilities, and report serious incidents. These are laid out in

circulars such as FINMA 2023/1 and 2018/3.

Importantly, since 1 April 2025, critical infrastructure operators – spanning sectors like finance, energy, healthcare, and telecoms – are legally required to report cyber incidents to the NCSC under the revised Information Security Act (ISA). More broadly, any authorities and organizations subject to the ISA, not only critical infrastructure operators, must create and implement an Information Security Management System (ISMS) that meets the requirements of the ISA. This includes assessing the protection needs of information (Article 6 ISA) and, where needed, their classification (Art. 11-15 ISG), identifying and continuously assessing risks (Article 8 ISA), defining security procedures and measures related to information technology (Articles 16-19 ISA), and ensuring personnel and physical protection (Article 20-23 ISA).

Under the ISA, authorities and organizations must also ensure that appropriate protective measures are taken to safeguard this information against unauthorized access, loss, disruption, or misuse (Art. 6-10 ISG).

Further, under the FADP, any private organization and federal body processing personal data is obliged to take appropriate data security measures (see Q26). These include safeguards against unauthorized access and data loss, and typically involve access controls, encryption, system updates, staff training, and contingency planning.

36. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding supply chain management? If so, please provide details of these requirements.

In Switzerland, cybersecurity-related supply chain requirements primarily arise from sector-specific regulations and strategic policies that emphasize risk-based governance and third-party oversight. For financial institutions, the Swiss Financial Market Supervisory Authority (FINMA) imposes binding obligations to manage risks associated with outsourcing and third-party providers. FINMA Circular 2018/3, which governs outsourcing arrangements, mandates that regulated entities must ensure full control over outsourced functions and maintain comprehensive oversight of third-party service providers. This includes obligations to assess the cybersecurity posture of vendors, define clear responsibilities in contracts, ensure access and audit rights, and implement contingency planning to mitigate service interruptions. Moreover, FINMA Circular 2023/1 on operational risks further stresses the need to monitor third-party risk as an integral component of ICT governance. It requires institutions to integrate suppliers into their risk assessments, ensure their participation in incident response planning, and assess their adherence to security standards throughout the lifecycle of the relationship.

Further, under the FADP, organizations that delegate data processing to third-party data processors must ensure that the processor provides sufficient guarantees of data security (see Q18 and Q26). This means that processors must be selected and monitored based on their ability to guarantee appropriate security standards. While the law does not spell out exact cybersecurity requirements for suppliers, it effectively imposes a duty of diligence in supply chain management.

More broadly, the National Cyberstrategy emphasizes the resilience of national infrastructure, including the dependency on secure and reliable supply chains. Although this strategy is non-binding for private companies outside regulated sectors, it sets the tone for expected best practices. For operators of critical infrastructure – who, since 1 April 2025, are legally required to report cyber incidents to the National Cyber Security Centre (NCSC) – this implies a growing emphasis on managing supplier-related risks as part of national security interests. Further, when cooperating with third parties not subject to the ISG, authorities and organizations subject to the ISA must ensure that legal requirements are met during both the commissioning and execution of tasks. Security measures must be specified contractually (Article 9 ISA).

37. Do the cybersecurity laws in your jurisdiction impose information sharing requirements on organisations?

Yes, Swiss cybersecurity laws do impose information sharing requirements, particularly for regulated sectors and critical infrastructure operators. Since 1 April 2025, operators of critical infrastructure are legally required to report significant cyber incidents to the National Cyber Security Centre (NCSC) under the Information Security Act (ISA). This ensures national coordination and timely response to threats affecting public services or national security. This reporting obligation includes incidents that significantly impact the availability, confidentiality, or integrity of information systems essential to national security or public welfare. Organizations falling within the definition of critical infrastructure must notify the NCSC within 24 hours, enabling the government to monitor threat trends, provide technical support, and coordinate with relevant stakeholders.

In the financial sector, institutions supervised by the Swiss Financial Market Supervisory Authority (FINMA) must notify FINMA of cyber attacks that are of substantial supervisory importance within 24 hours of detection and conduct an initial assessment of its critically, in accordance with Article 29 para. 2 of the Financial Market Supervision Act (FINMASA) and FINMA's circulars, notably FINMA Guidance 03/2024, 05/2020 and 01/2023. The actual report must then be submitted within 72 hours via the FINMA web-based survey and application platform (EHP). These reports help supervisors assess sector-wide risks and can trigger audits or additional oversight.

Outside of these formal obligations, the NCSC encourages voluntary reporting and participation in public-private information exchange platforms. For instance, the NCSC maintains threat intelligence forums and issues cyber threat bulletins, which companies can both contribute to and benefit from. While not mandatory for all organizations, contributing to and receiving cyber threat information is considered best practice.

Additionally, under the FADP, companies must notify the Federal Data Protection and Information Commissioner (FDPIC) of personal data breaches. While this pertains specifically to personal data breaches rather than broader cybersecurity threats, it reinforces the overall expectation of transparency and accountability following security incidents.

38. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, what are their legal responsibilities?

While Switzerland's legal framework does not universally require companies to formally appoint a Chief Information Security Officer (CISO), certain regulated sectors are expected to designate a person or function responsible for cybersecurity governance and oversight. In the financial sector, the Swiss Financial Market Supervisory Authority (FINMA) mandates that supervised entities implement a structured ICT risk management framework. Under FINMA Circular 2023/1, this includes clearly assigning responsibilities for information security, typically fulfilled by a CISO or equivalent role. Responsibilities include overseeing the development of security policies, coordinating incident response, managing ICT risks, and reporting significant security issues to executive management and FINMA.

Similarly, operators of critical infrastructure under the Information Security Act (ISA) must have internal structures and competencies in place to detect, manage, and communicate cyber incidents. While the law does not explicitly require appointing a CISO or point of contact, compliance with these obligations typically necessitates assigning such responsibilities to a designated individual or team capable of interacting with the NCSC and ensuring internal readiness.

More specifically, Article 81 ISA requires certain public authorities and organizations – such as the Federal Council and the Swiss National Bank – to appoint a Chief Information Security Officer (CISO). Their responsibilities include advising and supporting the responsible entities within their area in fulfilling their duties and obligations under the ISA. They are also tasked with managing the information security function and the associated risk management on behalf of their authority or organization. Additionally, they monitor compliance with information security requirements, report their findings, propose necessary measures, and may report security-related incidents to the NCSC.

For companies outside these sectors, there is no statutory requirement to appoint a specific individual responsible for cybersecurity. However, in practice, many Swiss companies – especially medium to large enterprises – appoint a CISO or equivalent to meet both compliance and operational expectations. This individual is often responsible for developing internal security policies, ensuring staff training, conducting risk assessments, and serving as a liaison with regulators or authorities in the event of a cyber incident.

39. Are there specific cybersecurity laws / regulations for different industries (e.g., finance, healthcare, government)? If so, please provide an overview.

The Information Security Act (ISA) imposes cybersecurity obligations on public and private organizations operating critical infrastructures such as energy suppliers, financial institutions, insurance companies, healthcare facilities, and medical laboratories. Under the ISA, which latest revision came into force in April 2025, operators of critical infrastructures are required to report significant cyberattacks to the National Cyber Security Centre (NCSC) within 24 hours, irrespective of whether personal data is involved (see Q35 and Q41).

In the financial and insurance services sector, the Swiss Financial Market Supervisory Authority (FINMA) oversees cybersecurity compliance through various instruments,

notably FINMA's Circulars. For example, banks must manage cyber risks in accordance with FINMA Circular 2023/1. Supervised Institutions must report cyberattacks of substantial importance to FINMA within 24 hours, following the requirements laid out in FINMA Guidances 2024/3 and 2020/5 (see Q37 and Q41).

The healthcare sector is another focus area. The NCSC has issued cybersecurity standards that healthcare providers are recommended to implement, such as patch management, monitoring of log data, and restrictions on risky email attachments. Specific regulatory requirements also apply, including mandatory certification for electronic patient record (EPR) providers under the Federal Act on the Electronic Patient Record (EPRA), cybersecurity obligations for medical devices under the Medical Devices Ordinance (MedDO), and technical safeguards for health-related data under the Human Research Act (HRA) and Human Research Ordinance (HRO). Healthcare entities must report certain incidents to the Federal Office of Public Health (FOPH) or, in the case of medical devices, to Swissmedic (see Q41).

In the telecommunications sector, providers are subject to cybersecurity obligations under the Telecommunications Act (TCA). They must take measures to mitigate risks and prevent damage to infrastructures and services. The Ordinance on Telecommunications Installations (TIO) and the Ordinance on Internet Domains (OID) impose additional cybersecurity requirements, including the obligation for registries to block malicious domains. Telecommunications service providers must immediately report faults or incidents affecting at least 10,000 customers to the National Emergency Operations Centre (NEOC) (see Q41).

40. What impact do international cybersecurity standards have on local laws and regulations?

International cybersecurity standards have a highly influential role, even though they are not legally binding within the Swiss jurisdiction. While standards such as ISO/IEC 27001 (information security management), NIST frameworks, and the EU's NIS2 Directive are not incorporated directly into national law, these standards serve as reference models for evaluating the adequacy of security measures, especially in regulated sectors. For example, the Swiss Financial Market Supervisory Authority (FINMA) references international frameworks in its circulars, particularly when defining expectations for ICT risk management and operational resilience. Supervised entities – such as banks and insurers – are not legally required to adopt ISO/IEC 27001, but they are expected to implement equivalent controls. In regulatory audits or incident reviews, the absence of such controls may be viewed as a deficiency.

Similarly, the National Cyberstrategy aligns with international principles on national cyber resilience, incident response coordination, and critical infrastructure protection. Although tailored to Switzerland's federal structure and risk landscape, the strategy is informed by OECD recommendations, EU cybersecurity norms, and global public-private cooperation models.

41. Do the cybersecurity laws in your jurisdiction impose obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and under what circumstances must a cybersecurity incident be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

Under the new Information Security Act (ISA), which latest revision came into force in April 2025, operators of critical infrastructure are required to report a cyberattack on its information systems to the National Cyber Security Centre (NCSC) within 24 hours of discovery, provided such cyberattack has serious consequences (Article 74d-e ISA).

The ISA defines a cyberattack as a cyber incident which was intentionally triggered. A cyber incident, in turn, is an event in the use of information systems that compromises the confidentiality, availability, or integrity of information, or the traceability of its processing. However, a cyberattack only must be reported if it:

a. jeopardizes the functionality of critical infrastructure involved (employees or third parties affected by system disruptions or the affected organization or authority can only maintain its operations with the help of emergency plans);
b. has led to manipulation or leakage of information (business-relevant information viewed, altered, or disclosed by unauthorized parties; or reports of data security breaches under the FADP);
c. remained undetected over an extended period of time (more than 90 days), especially if there are indications it was executed to prepare for further cyberattacks; or
d. is associated with extortion, threat, or coercion.

The report must include the type and execution of the cyberattack, the Impact of the cyberattack, the measures taken, and the planned further actions, if known (Art. 74e ISA).

Further, under Article 29 para. 2 of the Federal Act on the Swiss Financial Market Supervisory Authority (FINMASA), institutions supervised by the Swiss Financial Market Supervisory Authority (FINMA) must report cyber attacks to FINMA. FINMA Guidance 05/2020 and the updated clarification in Guidance 03/2024 outline the scope and deadlines for such notifications. FINMA expects an initial report within 24 hours of the incident, followed by a detailed report. If a report is also required to the NCSC, it may be submitted there first with a request to forward it to FINMA.

Additionally, under Article 96 of the Ordinance on Telecommunications Services (OTS), telecommunications service providers must immediately report any faults – including cybersecurity incidents – in telecommunications infrastructure or services that could impact at least 10'000 customers to the National Emergency Operations Centre (NEOC). Providers are also required to publish information about such faults on a publicly accessible website. The NEOC, in turn, informs the Federal Office of Communications (OFCOM). Non-compliance may result in penalties under Article 53 of the Telecommunications Act (TCA).

In the healthcare sector, specific reporting obligations apply to providers of electronic patient records (EPR), which must report incidents classified as security-relevant in their data protection and data security management system to the Federal Office of Public Health (FOPH) (Article 12 para. 3 of the Ordinance to the Federal Act on the Electronic Patient Record). Similarly, manufacturers of medical devices must report any serious incidents involving a medical device made available in Switzerland to Swissmedic, if the incident in question occurred in Switzerland (Article 66 of the Medical Devices Ordinance).

42. How are cybersecurity laws in your jurisdiction typically enforced?

In the area of national cyber resilience, the National Cyber Security Centre (NCSC) coordinates responses to cyber threats, especially those involving critical infrastructure operators. Since 1 April 2025, these operators are legally required to report serious cyber incidents to the NCSC within 24 hours of discovery (see Q41). Failure to report or cooperate can result in administrative consequences and increased regulatory scrutiny. Although the NCSC itself is not an enforcement body in the traditional sense, it plays a crucial role in informing, escalating, and coordinating cross-agency responses.

For regulated sectors such as banking and insurance, the Swiss Financial Market Supervisory Authority (FINMA) plays a central enforcement role. It monitors compliance with cybersecurity obligations through regular audits, supervisory reviews, and incident reporting requirements. When a financial institution suffers a major cyber incident or demonstrates deficiencies in ICT risk management, FINMA may conduct a formal investigation, require remedial action plans, impose restrictions on operations, or, in serious cases, initiate enforcement proceedings. These proceedings can result in public reprimands, orders to replace management, or – as *ultima ratio* – licence withdrawal.

For personal data breaches, the Federal Data Protection and Information Commissioner (FDPIC) is responsible for enforcement under the FADP (see Q31).

43. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

Swiss regulators possess significant oversight and inspection authority in relation to cybersecurity compliance, particularly within regulated sectors such as finance and critical infrastructure. The Swiss Financial Market Supervisory Authority (FINMA) holds extensive audit and investigative powers over banks, insurers, and other supervised entities. Under its supervisory framework, FINMA can conduct on-site inspections, review internal documentation and ICT risk management processes, and demand access to security policies, audit reports, penetration test results, and records of cyber incidents. FINMA may also mandate external audits through licensed audit firms, issue formal orders for remediation, and require institutions to demonstrate compliance with its circulars on cybersecurity and outsourcing. In more serious cases, it can initiate enforcement proceedings, impose operational restrictions, or require changes in management.

Similarly, the Federal Data Protection and Information Commissioner (FDPIC) has oversight powers under the FADP. The FDPIC can launch investigations *ex officio* or in response to complaints, inspect organizational measures taken to protect personal data, and access documents and IT systems necessary to assess compliance (see Q31). In certain cases, the FDPIC can refer violations to criminal authorities for prosecution.

For critical infrastructure operators, the National Cyber Security Centre (NCSC) plays a central role in monitoring and coordinating responses to cyber threats. While the NCSC does not carry enforcement authority in the traditional sense, it does oversee the mandatory cyber

incident reporting regime introduced in April 2025. The NCSC may conduct follow-up assessments, request technical details and logs related to reported incidents, and advise on improvements to security posture. Failure to cooperate may trigger involvement from other authorities or lead to reputational and compliance consequences.

44. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction?

Sanctions for cybersecurity law violations in Switzerland stem primarily from the FADP, sector-specific regulations such as those imposed by FINMA, and the Information Security Act (ISA).

Under the FADP, individuals may face criminal sanctions for wilful violations of certain data protection-related obligations (see Q32).

In the financial sector, the Swiss Financial Market Supervisory Authority (FINMA) has the power to take administrative enforcement measures rather than impose fines. These can include the issuance of binding orders, formal reprimands, the appointment of an independent monitor, or the removal of individuals from management positions. In serious cases, FINMA may restrict or revoke a company's license to operate. While FINMA does not levy monetary penalties, its actions can significantly disrupt business operations and lead to loss of client trust.

For critical infrastructure operators, who have been subject to mandatory cyber incident reporting under the ISA since 1 April 2025, failure to report or cooperate with the National Cyber Security Centre (NCSC) may initially result in increased scrutiny, regulatory escalation, and potential liability under sector-specific legislation. However, as of 1 October 2025, persistent failure to report – following expiry of two deadlines set by the NCSC – can result in fines of up to CHF 100'000 (Article 74g-74h ISA).

Failure by telecommunications service providers to comply with their reporting obligations under Article 96 of the Ordinance on Telecommunications Services (OTS) – including the duty to report faults, such as cybersecurity incidents, that could affect at least 10'000 customers to the National Emergency Operations Centre (NEOC), or to publish related information on a publicly accessible website – may result in fines of up to CHF 5'000 pursuant to Article 53 of the Telecommunications Act (TCA).

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

At present, Swiss law does not currently provide specific or formulaic rules for calculating fines or establishing clear thresholds for sanctions related to cybersecurity violations.

46. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Yes, enforcement decisions in Switzerland are open to appeal, depending on the authority involved and the legal basis of the decision.

With regard to the Information Security Act (ISA) and obligations to report cyber incidents to the National Cyber Security Centre (NCSC), the NCSC may issue a binding decision. Such decision is subject to appeal first through administrative objection proceedings, and then – if unresolved – via the Federal Administrative Court, with final recourse to the Federal Supreme Court if legal issues are at stake.

In the context of data protection, decisions made by the Federal Data Protection and Information Commissioner (FDPIC) can be challenged before the Federal Administrative Court, and further appeal may be made to the Federal Supreme Court on limited legal grounds. (see Q34).

For entities supervised by the Swiss Financial Market Supervisory Authority (FINMA), enforcement actions can also be appealed to the Federal Administrative Court. The appeal must generally be filed within 30 days of notification. The Court reviews the legality, legally relevant facts of the case, and adequacy of FINMA's actions. Further appeal to the Federal Supreme Court, which power of review is limited to legal issues, is possible.

47. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

With cybersecurity regulatory developments under the Information Security Act (ISA), effective since January 2024, critical infrastructure sectors must comply with mandatory 24-hour breach reporting requirements as of April 2025. The National Cyber Strategy emphasizes resilience against hybrid threats and NATO

interoperability, with particular attention to encryption implementation, regular security audits, and enforcement of two-factor authentication. The National Cyber Security Centre (NCSC) coordinates incident response efforts and enforces security standards.

Contributors

Christian Kunz
Partner
christian.kunz@baerkarrer.ch

Ferdinand Rombach
Associate
ferdinand.rombach@baerkarrer.ch

Katharina Schreiber
Associate
katharina.schreiber@baerkarrer.ch