Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2024

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

Switzerland: Law & Practice and Trends & Developments

Jürg Schneider, David Vasella and Hugh Reeves
Walder Wyss Ltd

SWITZERLAND

Law and Practice

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

Contents

Walder Wyss Ltd was established in Zurich in 1972 and has since grown at record speed. Today the firm has more than 250 legal experts and approximately 100 support staff in six offices in Switzerland's economic centres. Walder Wyss is an agile firm that is approachable, adapts to clients quickly, and does not hide behind formalism. Because it is fully integrated, the partners bring in those people who have the greatest expertise and are best suited for a particular task – this helps it avoid silos and ensures that work is carried out with optimal efficiency. Walder Wyss is the first large Swiss firm with a strong focus on tech, including data protection.

Authors

Jürg Schneider is a partner and head of the Lausanne office. His practice areas include information technology, data protection and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration and global outsourcing projects. Jürg has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international contexts. His special competencies regarding data protection include drawing up data protection concepts and strategies for companies, leading and assisting compliance projects regarding implementation of the GDPR (and the revised Swiss DPA) for Swiss and international companies, and advising clients in regulated sectors (banking, insurance, healthcare, etc) on data protection requirements.

David Vasella is a partner and co-head of Walder Wyss' regulated markets, competition, tech and IP team. He advises on technology, data privacy and IP matters, with a focus on the transition of businesses into the digital space. David deals with cross-jurisdictional data protection projects, including GDPR implementation, data retention, e-discovery, cloud projects, digital marketing, online regulation, information technology and e-business matters. He also regularly advises in relation to commercial IP matters, regulated products and market practices. In addition, he frequently speaks and publishes in his areas of expertise. David is an editor of the Swiss journal for data law and information security, CIPP/E certified, and a member of the professional bodies IAPP and DGRI.

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

Walder Wyss Ltd

Seefeldstrasse 123
P.O. Box
8034 Zurich
Switzerland

Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
Email: reception@walderwyss.com
Web: www.walderwyss.com

walderwyss

1. Basic National Regime

1.1 Laws

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

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

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

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

While the FDPA and the GDPR are similar in their approach and purpose, there are notable differences. For example, there is a data breach notification obligation under the FDPA, similar to that under the GDPR, but the trigger for notifying a personal data breach to the Swiss data protection authority, the Federal Data Protection and Information Commissioner (FDPIC), is "high risk", whereas, under the GDPR, any relevant risk requires notification. Another key difference is the level of activity by the relevant authorities: while many supervisory authorities within the EEA are more active, by providing guidance and/or by enforcing the GPDR, the Swiss Data Protection Authority is generally reluctant to take a decisive stance and rarely provides guidance for private actors. However, the FDPIC has initiated several investigations under the revised FDPA.

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

maintain processing regulations, have also been introduced.

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

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

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

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

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

- self-empowerment (Switzerland to expand its position as one of the world's leading knowledge, education and innovation locations in cybersecurity);

- securing digital services and infrastructures (Switzerland to implement measures to strengthen cyber-resilience);
- ensuring effective detection, prevention, management and defence against cyber-incidents (Switzerland to ensure the capacities and organisational organisation to be able to quickly identify cyberthreats and incidents and minimise damage);
- combating and prosecuting cybercrime effectively (Switzerland to expand its ability to identify threat actors, and prosecute them); and
- keeping a leading role in international co-operation (Switzerland to foster an open, free and secure cyberspace and compliance with international law in the digital space).

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

A further manifestation of the government's interest in cybersecurity is another governmental venture, the Digital Switzerland Strategy. The Digital Switzerland Strategy sets guidelines for Switzerland's digital transformation, and is updated annually by the Federal Council, each time with three focus topics. It is binding on the Federal Administration, and provides guidance for other stakeholders involved in digitalisation. The first take on this was published in 2016, and replacements arrived in 2018 and 2020. On 8 December 2023, the Federal Council adopted the updated Digital Switzerland Strategy for 2024, with cybersecurity, the Swiss approach to the regulation of AI systems, and electronic interfaces (API) as its focus topics.

At the same time, the Federal Council has approved the new Digital Administration Switzerland Strategy 2024–2027, which defines the fields of action to be prioritised in order for the Confederation, the cantons, and cities and municipalities to jointly determine how the digital transformation of administrations is to be driven forward. A second strategy approved by the Federal Council is the Digital Federal Administration strategy, which creates a framework for digital transformation projects in the Federal Administration.

1.2 Regulators

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

It is also worth mentioning here that the key official actor in the cybersecurity area is the National Cyber Security Centre (NCSC), which is now integrated in the new Federal Office for Cybersecurity (BACS), within the Federal Department of Defence, Civil Protection and Sports (DDPS). Indeed, in an effort to centralise the administrative activities in this area, other actors (such as MELANI, GovCert and CYCO) became an integral part of the NCSC and now the BACS. Its tasks include raising public awareness, receiving reports on cyber-incidents, and supporting oper-

ators of critical infrastructures in managing these incidents. Protection of the Federal Administration against cyber-attacks is now a key task of a new specialist unit within a new State Secretariat for Security Policy (Sepos), also within the DDPS.

1.3 Administration and Enforcement Process

The FDPA sets out basic rules applicable to investigations carried out by the FDPIC. The FDPIC had no direct enforcement powers against private bodies processing personal data under the former version of the FDPA, but could, on its own initiative or at the request of a third party, carry out investigations if a suspected breach of data protection law was capable of affecting a large number of persons and, in limited additional cases, issue a non-binding recommendation to change or terminate a processing activity. If the recommendation is not followed, the FDPIC could refer the matter to the Federal Administrative Court for a decision on the subject matter of the recommendation.

Under the revised FDPA, however, the FDPIC now has the right to carry out investigations more broadly as well as direct enforcement powers, including the right to direct the controller to change, suspend or cease processing activities. In the course of an investigation, the FDPIC has the right to demand the production of documents, make inquiries and ask for a demonstration of a particular processing of personal data. Failure to comply with a binding instruction may, if referred to criminal prosecution, incur liability to a fine against the responsible individuals of up to CHF250,000. Such fines can also be levied by the criminal courts against the responsible individual(s) in cases of non-compliance with minimum legal data security requirements, though it is doubtful whether the legislator has indeed provided for such minimum requirements. Most data security regulations under the FDPA and FDPO are very general in nature or focus on accountability, rather than security, except maybe for the obligation to ensure that certain higher-risk data operations are logged, as noted above.

The FDPIC's increased (compared to the prior version of the FDPA) powers and the more dissuasive criminal sanctions are seen as one of the most significant novelties in Swiss data protection legislation. Indeed, it could be argued that the former FDPA did not confer sufficient enforcement abilities upon the FDPIC and that this, combined with the largely symbolic fines, has somewhat marginalised the impact of the (current) FDPA across the board.

The investigation by the FDPIC is subject to the Federal Act on Administrative Procedure (APA), which provides for due process rights for the investigated party and third parties – for example, rights to refuse to testify. The procedure before the Federal Supreme Court is regulated by the Federal Act on the Supreme Court.

There is a general view that enforcement of the former FDPA was insufficient. This was one of the drivers of the revision of the FDPA. This perceived lack of enforcement was due to several factors, including the following.

- The FDPIC had no direct enforcement powers against private bodies processing personal data and, with limited resources, typically concentrated on data processing by federal bodies and, in the private sector, on significant or high-profile cases.
- There was no risk of criminal sanctions for a breach of data protection laws, except in very limited scenarios.

- In the event of a breach of data protection law, there was a risk of civil liability claims from the concerned data subjects and, depending on the circumstances, a risk of negative publicity. However, there was normally no financial risk as claims for compensation necessitated establishing a financial loss. There was no claim for compensation of non-material damage, in contrast to the GDPR, or any form of statutory damages.

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

FINMA has also revised its circular, with the updated version Circular 2023/1 Operational Risks and Resilience – Banks coming into force on 1 January 2024. It requires banks and investment firms to report certain cyber-attacks within 24 hours of becoming aware and to submit a full report within 72 hours.

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

1.4 Multilateral and Subnational Issues

Switzerland has implemented the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) through the FDPA.

In addition, Switzerland is not a member of the EU or of the EEA and is under no obligation to implement the EU General Data Protection Regulation (GDPR), but the EU is Switzerland's most important partner, and ensuring a level playing field for Swiss and EU-based companies is an important policy objective. The (revised) FDPA largely aligns with the GDPR, such that a company that complies with the GDPR should generally be in compliance with the FDPA. Moreover, revising the FDPA has been a key factor in the European Commission's confirmation of its finding that Switzerland's data protection legislation provides an adequate level of data protection under the GDPR, on 15 January 2024.

For data processing in relation to criminal prosecution, and in the framework of police and judicial co-operation, Switzerland transposed, on 30 January 2019, EU Directive 2016/680 into domestic Swiss legislation through the FDPA. It expedited the adoption of this piece of legislation, with the relevant changes having entered into force on 1 March 2019.

1.5 Information Sharing Organisations and Government Cybersecurity Assistance

Firstly, the FDPA does not provide an official role for NGOs and SROs. Such organisations would not, for example, have a right to bring a civil claim against a company perceived to be in breach of privacy laws. However, there are a number of organisations that promote privacy, including several consumer protection organisa-

tions, though they do not perform these tasks on the basis of a legal mandate. Furthermore, NGOs and SROs may request the FDPIC to open investigations if a suspected privacy breach is capable of affecting a large number of persons (ie, a system error) and in limited additional cases.

The NCSC – now part of the BACS – is the key official actor in the cybersecurity area (see **1.2 Regulators**). GovCERT.ch, whose parent organisation is the NCSC, is the Computer Emergency Response Team (CERT) for Switzerland. Its tasks comprise the support of the critical IT infrastructure in Switzerland in dealing with cyberthreats. It maintains close relationships with other CERT organisations, thereby seeking to promote the exchange of cyberthreat-related information. Furthermore, the FDPIC retains strong prerogatives given the absence of standalone cybersecurity legislation.

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

As mentioned above, the FDPIC retains a central role in the area of cybersecurity. The revised FDPA now grants the FDPIC certain enforcement powers (see **1.3 Administration and Enforcement Process**).

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

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

1.6 System Characteristics

The prior version of the FDPA qualified legal and natural persons as data subjects, thereby protecting the personal data of legal entities. This specificity was at odds with the GDPR and numerous other foreign laws, and has been removed with the revision of the FDPA.

Moreover, Switzerland has avoided any ad hoc cybersecurity legislation, rather following sector-specific legislating efforts, and cybersecurity remains fundamentally closely tied to the area of data protection. Lastly, the Swiss legislator has historically defended a so-called technologically neutral approach. This means that Swiss laws only seldom address a specific technology. This avoids any lag between technological evolution and the legal landscape and makes Swiss legislation more resilient over time. However, it does come with the drawback that the legislation is not always sufficiently precise, thus resulting in enforcement uncertainty.

1.7 Key Developments

The most important developments are the entry into force of the FDPA on 1 September 2023 and the new ISA (see **1.1 Laws**).

The Swiss government's efforts to bolster and centralise cybersecurity and cyberdefence activities are also a promising and ongoing development (see **1.5 Information Sharing Organisations and Government Cybersecurity Assistance**). In that respect, many commentators have been sounding the alarm as it appears that Swiss companies as well as public bodies (often on the municipal level) have not been taking cyberthreats seriously enough – a concern only exacerbated by the "Xplain" and Concevis attacks (see Trends & Developments).

Public attention remains high. This stems from the stream of data breaches locally and internationally, the increased awareness around data protection worldwide, but also results from some cybersecurity considerations affecting national security. In this latter category, the war in Ukraine and the international geo-political situation, combined with the roll-out of next generation technologies, especially 5G networks, have led to a heightened awareness of cyberthreats.

It is still too early to foresee any long-term consequences of this for the Swiss legal and regulatory landscape, though it will likely lead to questioning Switzerland's international policy in regard to cybersecurity, cyber-espionage and international co-operation.

1.8 Significant Pending Changes, Hot Topics and Issues

See **1.7 Key Developments**.

2. Key Laws and Regulators at National and Subnational Levels

2.1 Key Laws

See **1.1 Laws**. The only truly overarching body of laws is the federal legislation on data protection, namely the FDPA and its implementing ordinances, in particular the FDPO. The FDPA and the FDPO contain provisions on data security, but the Swiss legislator relies on a technologically neutral approach, with the result that these rules on data security remain rather abstract and do not refer to any specific technology, or any specific standard or technical requirement, except for the obligation to keep logs of certain higher-risk processing activities.

So far, and in the foreseeable future, Parliament will not be removing data security from the data protection legislation and will not draft any standalone cybersecurity act. Consequently, data protection legislation should remain at the centre of everyone's cybersecurity considerations and the FDPIC will play an important role going forward (which role is upheld and bolstered with the revised FDPA discussed herein – see **1.3 Administration and Enforcement Process**). Moreover, under the FDPA, an intentional failure to implement certain minimum technical and organisational measures may incur liability for a fine against the responsible individuals of up to CHF250,000.

The TCA, and its surrounding ordinances and technical guidelines, includes a notification duty to OFCOM in case of security incidents and, more generally, contains requirements governing the security and the availability of telecommunications services and networks.

The FinMia is a modern law regulating the operation of the financial market infrastructures. It is notable as it takes into account the dependency of said infrastructures on information technology and the ensuing cyber-risks. It seeks to ensure that all relevant actors have robust and resilient systems that permit business continuity and data integrity. As mentioned above, FINMA is

essential to the proper implementation of the FinMia.

2.2 Regulators

For the data protection regulator, the FDPIC, see **2.4 Data Protection Authorities or Privacy Regulators**. In addition, the Federal Office of Communications (OFCOM), acting under the supervisory oversight of the Federal Communications Commission (ComCom), is the regulator in charge of the telecommunications and information society sectors. OFCOM plays a role in the area of cybersecurity as telecommunications legislation contains rules on telecommunications network security and availability and telecommunications secrecy, both of which may be a concern from a cyber-risk standpoint. OFCOM issues intermittent technical regulations relating to the security and availability of telecommunications services and infrastructures.

Moreover, there is a duty to notify OFCOM regarding issues with telecommunications networks that affect a significant number of users.

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

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

2.3 Over-Arching Cybersecurity Agency

See **1.5 Information Sharing Organisations and Government Cybersecurity Assistance**.

The National Cyber Security Centre's (NCSC) predecessor, MELANI, played a helpful role as an information sharing platform and demonstrated the need for an increased governmental support to the area of cybersecurity. The NCSC – now BACS – is also competent to request the blocking of ".ch" and ".swiss" top-level domains if these are suspected of being used for cybercrime purposes (such as malware distribution and phishing activities).

Given the ongoing focus surrounding digitalisation, the protection of privacy and cybersecurity concerns, Switzerland is currently at a promising turning point in its cybersecurity practice on a federal level. This strengthening of the federal government's cybersecurity activities also meets a growing public need for more potent cyber-risk mitigation measures.

2.4 Data Protection Authorities or Privacy Regulators

The FDPIC, as mentioned in **1.2 Regulators**, plays a key role in the area of cybersecurity. Since 1 September 2023, the FDPIC is able to investigate virtually any breach of data protection regulations, including if a mandatory notification to the FDPIC has not been made. However, and somewhat surprisingly, a breach of the notification obligation is not liable to criminal fines.

2.5 Financial or Other Sectoral Regulators

FINMA, as the financial markets supervisory authority, frequently adopts and adapts various circulars and notices. In particular, FINMA Circular 2008/21 and its recent replacement (entry into effect on 1 January 2024) Circular 2023/01 Operational Risks and Resilience – Banks is central to all banks' cybersecurity practices as it lays out principles and guidelines on proper risk management surrounding client-identifying data (CID). FINMA Circular 2018/3 on Outsourcing by Banks and Insurers is another essential text as it contains rules on the security of data in an outsourcing context.

2.6 Other Relevant Regulators and Agencies

See **2.2 Regulators**.

3. Key Frameworks

3.1 De Jure or De Facto Standards

De jure, there is no obligation to abide by any particular technical standards. This is in no small part the result of Switzerland's technologically neutral approach. In practice, however, companies regularly look to the international standards as a benchmark or as a best practice requirement. This is common in the financial sector, for instance, and is also in line with the requirements of the FDPA as one can presume – as a rule of thumb – that compliance with the international standards, such as the ISO 27001 standards, would provide shelter from data security concerns under the FDPA. Moreover, the revised FDPO will likely introduce minimum standards for technical and organisational measures.

In addition, the FDPA allows the certification of data processing systems or programs as well as private persons or federal bodies that process personal data. This certification, though extremely rare in practice, in effect requires compliance with ISO 27001 as a prerequisite. The reliance on certification mechanisms is expected to gain more traction with the revised FDPA, which promotes such approaches.

3.2 Consensus or Commonly Applied Framework

There is no "reasonable security" test in Switzerland, nor any framework applied in that respect.

3.3 Legal Requirements and Specific Required Security Practices

The FDPA contain a reference to "adequate technical and organisational measures" to protect personal data, though this is generally understood as a reference to the use of state-of-the-art technologies, as further detailed in the FDPO. These measures must moreover "enable the avoidance of data security breaches".

The FDPO sets out base technical and organisational measures as follows:

- general measures imposed on anyone processing personal data – these measures include protection against accidental or unauthorised destruction, accidental loss, technical faults, forgery, unlawful copying or alteration;
- special measures such as entrance control (to premises containing personal data), personal data carrier control, control of transport, disclosure, storage, usage, access and input;
- the maintenance of records of any automated processing of sensitive personal data or personality profiles (with a one-year retention period, as noted above); and
- a processing policy in certain cases of automated data files, namely when the processing concerns sensitive personal data or high-risk personality profiles.

In the financial sector, FINMA Circular 2018/3 on Outsourcing and FINMA Circular 2023/01 Operational Risks and Resilience – Banks, call for the targeted undertakings to ensure proper resilience and business continuity, as well as adequate incident management plans, and potentially an obligation to notify cyber-attacks to FINMA, in addition to any other notification obligations (where applicable).

Outsourcing, as well as the use of cloud services, is broadly permitted, though the provider must ensure adequate data security. To that effect, many cloud service providers have sought data security and cybersecurity certifications, though whether they in practice implement proper cybersecurity practices is often difficult for the clients of such services to ascertain. In addition, the parties involved in outsourcing or cloud services may have to implement additional safeguards in case of cross-border disclosures of personal data.

3.4 Key Multinational Relationships

In its national strategy for the protection of Switzerland against cyber-risks, the government stresses the value of effective international co-operation and networking. This strengthening of the international co-operation remains a work in progress and a strategic priority for the government.

That said, Switzerland has been involved with or appears to closely follow the standardisation work internationally, among others with the UN World Summit on the Information Society (WSIS), the International Telecommunications Union (ITU), plus the OECD's and the WEF's work on improving digital security.

As a side note, Geneva has been emerging as a hub for internet governance. For instance, the Geneva Internet Platform, which is an initiative of the Swiss authorities, positions itself as a centre for digital policy debates around many ICT topics, including cybersecurity. It serves permanent missions based in Geneva and supports Geneva-based institutions in their digital policy activities.

4. Key Affirmative Security Requirements

4.1 Personal Data

The FDPA imposes reporting requirements on controllers and processors. Controllers have to report to the FDPIC any data breaches resulting in high risks for the rights and freedoms of the data subjects. Controllers must also inform the data subject if this is necessary for the protection of the data subject or if the FDPIC so requests (some limitations do, however, apply). A processor shall notify the controller as soon as possible of any data security breach. In addition, a breach notification obligation in cases of cybersecurity incidents affecting critical infrastructures is expected to enter into force in 2025 (see **1.7 Key Developments**).

4.2 Material Business Data and Material Non-public Information

At the time of publication of this guide (March 2024), there are no specific affirmative security requirements for material business data and material non-public information. In any case, as noted in **4.1 Personal Data**, reporting of cyber-incidents to BACS is well-advised and helps disseminate information about potential cyber-risks across the industry.

4.3 Critical Infrastructure, Networks, Systems and Software

As mentioned in **4.1 Personal Data**, a breach notification obligation in cases of cybersecurity incidents affecting critical infrastructures is in the works and is expected to apply from 1 January 2025. Moreover, the Federal Office for National Economic Supply (FONES) published a minimum ICT standard document as well as an ICT self-assessment tool directed at operators of critical infrastructures. This document rests, in part, on the requirements of the quite ubiquitous NIST Framework to which it refers.

4.4 Denial of Service Attacks

Denial of service (or DoS) attacks remain an ongoing threat, often leading – especially in the form of so-called "distributed DoS, DDoS" – to the total incapacitation of the victim's IT systems and network. The NCSC issued guidelines on recommended preventative measures and countermeasures to address DDoS attacks. The NCSC is a good first contact point in case of DoS attacks.

4.5 Internet of Things (IoT), Software, Supply Chain, Other Data or Systems

In the financial and banking sector, FINMA Circular 2008/21 Operational Risks at Banks and its replacement Circular 2023/01 contain a notification duty in certain cases of data breach. This Circular provides that the banks must have a clear communication strategy in case of serious incidents pertaining to client-identifying data (CID); this communication strategy must specify when it is necessary to notify FINMA, criminal prosecution authorities, the clients concerned and the media.

There has been little specific legislative effort directed at IoT and supply chain actors. This mostly relates to Switzerland's technologically neutral approach to legislative action. Therefore, the general requirements under the FDPA in terms of data security play a predominant role, though sector-specific rules may come into play as well. That said, 1 January 2023 updates to telecommunications legislation brought about, in particular, increased network security requirements, especially in the form of reinforced anti-piracy and anti-tampering mechanisms to handle malicious activities; in addition, operators of 5G networks and services that operate on these networks have to implement an information security management system.

4.6 Ransomware/Extortion

According to the BACS's semi-annual report 2023/1, all industries are affected by ransomware, which continues to be the greatest cyberthreat in Switzerland. See Trends & Developments for information about some recent, notable cyber-incidents.

Currently, there are no payment prohibitions, though victims of ransomware are as a general practical rule well-advised not to pay out any ransom money. Moreover, the FDPA provides an obligation to report data security breaches to the FDPIC, which can be relevant in the ransomware field.

Reporting and liaising with the BACS, as well as the filing of a criminal complaint, are highly recommended but not mandatory (so long as the notification obligation for providers of critical infrastructure is not in force).

5. Data Breach or Cybersecurity Event Reporting and Notification

5.1 Definition of Data Security Incident, Breach or Cybersecurity Event

The FDPA imposes breach notification duties, when the breach is likely to result in a high risk to

the personality or fundamental rights of the data subject. The communication must be addressed to the FDPIC as soon as feasible. The communication must contain an indication of the nature of the breach, the consequences and the measures taken or envisaged.

As previously mentioned, a reporting obligation in case of data security incidents affecting critical infrastructures is also expected for 2025.

Sectoral rules and regulations may still come into play. This is notably the case in the banking sector, where FINMA Circular 2023/01 contains wording on reporting and external communication of data security incidents.

5.2 Data Elements Covered

See **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**. In the banking sector, the data covered is CID (client-identifying data).

5.3 Systems Covered

There are no specific systems covered given the fact that the Swiss legislator typically opts for a technologically neutral approach thereby eschewing any discussion around a specific technology (although exceptions exist).

5.4 Security Requirements for Medical Devices

There are no specific cybersecurity and data breach notification rules pertaining to medical devices. However, where software qualifies as a medical device, a reporting obligation of serious incidents may apply, and Swissmedic, the competent sectorial authority, ensures that it makes the general public aware of health risks arising from medical devices.

5.5 Security Requirements for Industrial Control Systems (and SCADA)

There are no specific cybersecurity and data breach notification rules pertaining to industrial control systems and SCADA.

5.6 Security Requirements for IoT

There are no specific cybersecurity and data breach notification rules pertaining to IoT. However, various authorities serve as valuable contact points. In particular, the FDPIC and the BACS play an important role – the former for matters pertaining to data protection and data security, the latter for any voluntary notification of a cyber-incident.

Security requirements around IoT are also a priority for the government, which mentioned in its Digital Switzerland Strategy (see **1.1 Laws**) the need for the industry to implement state-of-the-art cybersecurity measures to accompany the growth of IoT on the Swiss market.

5.7 Requirements for Secure Software Development

There are no specific mandatory requirements pertaining to security software life cycle, certifications, patching or the disclosure of vulnerabilities. This is mainly due to the technologically neutral approach of Swiss legislation. However, duties to patch faulty security software or disclosure vulnerabilities may arise from the general principles of data protection legislation and such topics could therefore call for a case-specific assessment. In addition, certifications may start to play a bigger role under the revised FDPA.

5.8 Reporting Triggers

See **5.1 Definition of Data Security Incident, Breach or Cybersecurity Event**.

5.9 "Risk of Harm" Thresholds or Standards

There is currently no "risk of harm" or similar threshold applicable in Switzerland.

6. Ability to Monitor Networks for Cybersecurity

6.1 Cybersecurity Defensive Measures

Swiss law offers the competent authorities certain means to monitor telecommunications, including emails and other information. From a cybersecurity standpoint, the Federal Act on the Intelligence Services (IntelSA) of 25 September 2015 gives the Swiss Federal Intelligence Services (FIS) broad powers to intercept and monitor communications and networks on grounds of national interests, including safeguarding democratic and constitutional principles as well as national and international security.

The IntelSA gives broad powers to the FIS, such as:

- covert surveillance of telecommunications, including telecommunications monitoring, recording and localisation of the targeted person;
- covert intrusion into computer systems and computer networks, even when located abroad; and
- recording of cross-border cable-based networks.

6.2 Intersection of Cybersecurity and Privacy or Data Protection

Unlike the USA, Switzerland protects personal information not (predominantly) as a privacy right, but rather as a matter of data protection. In other words, it is the (personal) data and not the individual that is the subject matter of Swiss data protection legislation.

It is a logical next step to treat cybersecurity as a subset of data protection. Indeed, as things currently stand, Swiss law assimilates cybersecurity and data security, which is a core principle of data protection (see above **1.1 Laws** and **2.1 Key Laws**). There is, therefore, a clear intersection between cybersecurity and data protection.

Going forward, despite the low likelihood of any ad hoc cybersecurity legislation, it is probable that the legislator and the authorities will progressively dissociate the notion of cybersecurity from the area of data protection. Indeed, the protection of personal data is only one among many concerns that cybersecurity must address. For instance, the need, for national security reasons, to protect critical infrastructures may be properly addressed through cybersecurity, though there is arguably little relevance of data protection legislation in that respect (ie, only to the extent that personal data comes into play).

Moreover, the report of the Swiss national strategy on the protection of Switzerland from cyberrisks considers that cybersecurity concerns the protection of information and communication infrastructures against attacks and disruptions, thereby showing a move away from a data protection environment to a more transversal understanding of the notion of cybersecurity.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information

There is no general obligation to disclose cybersecurity information with the government. However, sharing of information is generally encouraged and the companies wishing to share the information can approach the bodies mentioned above (see **1.5 Information Sharing Organisa-**

tions and Government Cybersecurity Assistance) or their sectoral regulators, if any.

7.2 Voluntary Information Sharing Opportunities

See **1.5 Information Sharing Organisations and Government Cybersecurity Assistance**.

8. Significant Cybersecurity and Data Breach Regulatory Enforcement and Litigation

8.1 Regulatory Enforcement or Litigation

To date, there have been no leading or seminal decisions on the specific matter of cybersecurity.

8.2 Significant Audits, Investigations or Penalties

The most significant regulatory intervention came after several leaks in the banking sector during the post-2008 financial crisis. These data leaks were typically not the result of cyberattacks, but they did lead to a reinforcement of the regulatory landscape; at that time, FINMA revised its Circular 2008/21 to bring increased attention to matters of data security and risk management.

8.3 Applicable Legal Standards

See **8.1 Regulatory Enforcement or Litigation**.

8.4 Significant Private Litigation

The matter is not relevant in this jurisdiction.

8.5 Class Actions

Though some basic collective action schemes do exist (with no immediate possibility for the claimants to move for damages), class actions are not permitted in Switzerland. There is some ongoing discussion to provide for class actions in civil proceedings. Proponents of such class actions received a setback in 2020, with the Swiss government deciding against including class actions in the revision of the Swiss Civil Procedure Code. However, in December 2021, the Federal Council launched a new process towards the introduction of collective redress into the Swiss Civil Procedure Code, to allow for the assertion of claims for compensation and a possibility of collective settlements in a new representative action procedure. However, the National Council's Committee for Legal Affairs came to the conclusion, in July 2023, that measures to prevent misuse of class action instruments should be examined further. It is expected that the Commission will resume deliberations in the first quarter of 2024. This goes to show that class actions remain a hotly debated topic, both as a matter of principle and regarding the specificities of such legal instrument, and it is uncertain whether, or in what form, they will make it into the law.

9. Cybersecurity Governance, Assessment and Resiliency

9.1 Corporate Governance Requirements

As already discussed, the Swiss legislator has a "technologically neutral" approach. This approach has several consequences: first, the FDPA does not provide for a specific obligation for the board of directors or any required certifications. Nonetheless, legal entities and their board of directors are responsible for compliance with the FDPA (eg, mandatory reporting) and the requirements of their specific sector if regulated, such as banking, insurance, and healthcare, to name a few.

10. Due Diligence

10.1 Processes and Issues

The legal due diligence exercise from a cybersecurity perspective should firstly address any general data protection law considerations, being specified that data security forms an integral part thereof. As a second step, it is necessary to ascertain whether the target of the due diligence process performed any IT systems resilience testing, such as penetration testing. The results of such testing should be disclosed and analysed. In addition, the target of the due diligence should properly document any data breach, and this should include any remedial steps taken and their outcome.

Given the eminently technical nature of cybersecurity measures, a technical due diligence, performed by IT cybersecurity auditors, is recommended. In any case, the contractual documentation around corporate transactions tends to be qualified regarding any cyber-risks.

10.2 Public Disclosure

There is no public disclosure obligation upon organisations to publish their cybersecurity risk profile or experience.

11. Insurance, Artificial Intelligence and Other Cybersecurity Issues

11.1 Further Considerations Regarding Cybersecurity Regulation

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

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

Trends and Developments

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

Walder Wyss Ltd was established in Zurich in 1972 and has since grown at record speed. Today the firm has more than 250 legal experts and approximately 100 support staff in six offices in Switzerland's economic centres. Walder Wyss is an agile firm that is approachable, adapts to clients quickly, and does not hide behind formalism. Because it is fully integrated, the partners bring in those people who have the greatest expertise and are best suited for a particular task – this helps it avoid silos and ensures that work is carried out with optimal efficiency. Walder Wyss is the first large Swiss firm with a strong focus on tech, including data protection.

Authors

Jürg Schneider is a partner and head of the Lausanne office. His practice areas include information technology, data protection and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration and global outsourcing projects. Jürg has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international contexts. His special competencies regarding data protection include drawing up data protection concepts and strategies for companies, leading and assisting compliance projects regarding implementation of the GDPR (and the revised Swiss DPA) for Swiss and international companies, and advising clients in regulated sectors (banking, insurance, healthcare, etc) on data protection requirements.

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

David Vasella is a partner and co-head of Walder Wyss' regulated markets, competition, tech and IP team. He advises on technology, data privacy and IP matters, with a focus on the transition of businesses into the digital space. David deals with cross-jurisdictional data protection projects, including GDPR implementation, data retention, e-discovery, cloud projects, digital marketing, online regulation, information technology and e-business matters. He also regularly advises in relation to commercial IP matters, regulated products and market practices. In addition, he frequently speaks and publishes in his areas of expertise. David is an editor of the Swiss journal for data law and information security, CIPP/E certified, and a member of the professional bodies IAPP and DGRI.

Walder Wyss Ltd

Seefeldstrasse 123
P.O. Box
8034 Zurich
Switzerland

Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
Email: reception@walderwyss.com
Web: www.walderwyss.com

walderwyss

Current Trends and Challenges

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

The most widely publicised attack, however, was when a ransomware group attacked security software provider Xplain, which supplies numerous Swiss government agencies. The attackers claimed to have stolen over 900GB of sensitive data, including information linked to the Swiss Army, customs, and police. An investigation is ongoing.

In an Xplain repeat, hackers hit Concevis, another major software vendor to the federal and cantonal governments. While some data has appeared online, ransomware groups have not claimed responsibility for the attack. In both cases, the federal government apparently did not audit the providers' security standards.

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

Recent Regulatory Updates

While the increase in reported attacks highlights the urgency of robust cybersecurity, the issue is all but new. Switzerland has responded to these challenges in recent months and years by adapting its cybersecurity framework on a number of levels.

The revised FDPA and FDPO

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

In addition, the FDPA and the Federal Data Protection Ordinance (FDPO) provide for a general

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

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

The new Information Security Act

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

A significant feature of the ISA is the introduction of a reporting obligation for cyber-attacks for public authorities such as universities, federal, cantonal and municipal agencies, as well as intercantonal, cantonal and intercommunal organisations, and for providers of critical infrastructures, for example in the energy, finance, healthcare, insurance, transport and communication and IT sectors. In-scope organisations must report cyber-attacks to the National Cybersecurity Centre within 24 hours, where the relevant thresholds and definitions are met. It is currently expected that this obligation will come into force on 1 January 2025. This notification obligation is in addition to other incident notifications, such as the obligation to report personal data security breaches to the FDPIC.

Updated government organisation at a federal level

The ISA and ensuing legislation have also reworked the government's security organisation. The Federal Office for Cybersecurity (BACS), within the Federal Department of Defence, Civil Protection and Sport (DDPS), now serves as the centre of competence for cybersecurity, acting as the primary contact for the economy, administration, educational institutions, and the public on cyber-related issues. Its tasks include raising public awareness, receiving reports on cyber-

incidents, and supporting operators of critical infrastructures in managing these incidents. The BACS has absorbed the former National Cyber Security Centre, and protection of the Federal Administration against cyber-attacks is now a key task of a new specialist unit within a new State Secretariat for Security Policy (Sepos), also within the DDPS.

Other regulatory activity

Other authorities have an increased focus on cybersecurity as well, within their supervisory activities. A key example is FINMA, the Swiss financial market supervisory authority, which oversees compliance with – inter alia – data security regulations in the financial sector. It publishes an annual risk monitor as an overview of risks that FINMA sees as particularly significant. The 2023 version highlights that cyber-risks remain one of the biggest operational risks and observes a trend towards malware attacks targeting external service providers. Outsourcing contributes to cyber-risk and is a focus for FINMA.

One of FINMA's main supervisory tools is issuing guidance and circulars, which set out its expectations for regulated institutions. These include the FINMA Circular 2023/1 Operational Risks and Resilience – Banks, which entered into force on 1 January 2024. It applies for banks and investment firms and requires them to report certain cyber-attacks within 24 hours of becoming aware and to submit a full report within 72 hours. Again, this obligation is in addition to any other incident notification obligations. There is ongoing discussion in the market in relation to ensuring that the 24-hour requirement is met even where an institution has outsourced IT operations to a provider, such as a cloud services provider.

Initiatives at a Cantonal level

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

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

CHAMBERS GLOBAL PRACTICE GUIDES

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

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