Chambers

GLOBAL PRACTICE GUIDE

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

Cybersecurity

Switzerland
Jürg Schneider, David Vasella and Hugh Reeves
Walder Wyss Ltd

chambers.com

2020

SWITZERLAND

Law and Practice

Contributed by:
Jürg Schneider, David Vasella and Hugh Reeves
Walder Wyss Ltd see p.12

Contents

1. Basic National Regime

1.1 Laws

Switzerland is a federation comprising 26 federated states (cantons) as well as a centralised 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 offshoot – 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 of 19 June 1992 (the FDPA) and its ordinances, including the Ordinance to the Federal Act on Data Protection (the FDPO).

Data processing by public bodies is governed by the FDPA for federal bodies 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 is currently under revision in order to implement the revised Council of Europe's Convention 108 and to align with the EU General Data Protection Regulation (GDPR). The Federal Council published a proposal for the revised FDPA on 15 September 2017 and initiated a consultation process.

At the issue of this consultation process, the Federal Council decided to split the revision process into two separate phases. A first phase targeted the necessary amendments to bring Swiss legislation in line with changes to the Schengen/Dublin framework (EU Directive EC 2016/680 of 27 April 2016). These changes were made and implemented in a Federal Council decision of 30 January 2019 and entered into force on 1 March 2019. During a second and still ongoing phase, Parliament has been discussing the draft of the revised FDPA. Given these latest developments, no final wording of the revised FDPA is available as yet. There is a general expectation that the revised FDPA will not enter into force before January 2022.

There is no dedicated cybersecurity legislation in Switzerland to date. Cybersecurity is 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 (FTA); and
- the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading of 19 June 2015 (FinfrAct). The banking and financial markets legislation also leads to the financial markets regulator's (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 ad hoc law on cybersecurity may therefore appear misleading given the importance and national relevance of this topic. This conclusion nonetheless is unlikely to lead the Swiss legislator (Parliament) to issue any topical legislation on cybersecurity in the near future. On the contrary, the federal government published in 2012, with a revision in April 2018, a report concerning the national strategy on the protection of Switzerland from cyber-risks. The 2012 report identified 16 measures aimed at mitigating cyber-risks. Interestingly, the 2018 report contained 29 measures. This shows the growing 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 in another governmental output, the Digital Switzerland strategy. The first take on this was published in 2016 and its replacement arrived in autumn 2018; a further update is expected in the course of 2020, as this is a biennial process. This Digital Switzerland strategy comes with an action plan, several points of which address cybersecurity against the backdrop of the country's digitalisation processes.

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 if their data processing is capable of affecting a large number of persons. 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).

1.3 Administration and Enforcement Process

The FDPA sets out basic rules applicable to investigations carried out by the FDPIC.

The FDPIC has no direct enforcement powers against private bodies processing personal data. However, on its own initiative or at the request of a third party, it can carry out investigations if a suspected breach of data protection law is capable of affecting a large number of persons (ie, a system error) and in limited additional cases. 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. However, under the current FDPA, the FDPIC cannot issue binding instructions to the controller, though this is due to change under the revised FDPA. The FDPIC's only instrument at this stage is issuing a non-binding recommendation to change or terminate a processing activity. If the recommendation is not followed, the FDPIC may refer the matter to the Federal Administrative Court for a decision on the subject matter of the recommendation. This Federal Administrative Court's decision is binding but can be appealed before the Federal Supreme Court. Neither these courts nor the FDPIC can impose monetary sanctions, but they can refer the matter for criminal prosecution, which may lead to a fine of up to CHF10,000 in very limited scenarios.

Under the revised FDPA, the FDPIC is expected to have direct enforcement powers, including the right to direct the controller to change, suspend or cease processing activities. Failure to comply with a binding instruction will be liable to a fine against the responsible individuals of up to CHF250,000.

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 FDPA has been inadequate in the past. This is one of the drivers of the ongoing revision of the FDPA. This perceived lack of enforcement is due to several factors, including:

- the FDPIC has no direct enforcement powers against private bodies processing personal data and, with limited resources, typically concentrates on data processing by federal bodies and, in the private sector, on significant or high-profile cases;
- there is no risk of criminal sanctions for a breach of data protection laws, except in very limited scenarios; and
- in the event of a breach of data protection law, there is a risk of civil liability towards the concerned data subjects and, depending on the circumstances, a risk of negative publicity. However, there is normally no financial risk as claims for compensation with the required data are subject to establish financial losses. There is no claim for compensation of non-material damage, in contrast to the GDPR.

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. In case of a breach of the sectoral rules, FINMA has a varied toolbox of enforcement means. These include the revocation of licences to practice, fines or even custodial sentences. FINMA also occasionally and for preventive purposes relies on a "name and shame" strategy, meaning that the author of any offense 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, and is currently in the process of revising the FDPA to follow the revision of Convention 108.

In addition, Switzerland is not a member of the EU or of the EEA and 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 current revision of the FDPA therefore largely aligns with the GDPR and, while there is no final draft to date, it is expected that the revised FDPA will be compatible with the GDPR such that a company that complies with the GDPR should generally be in compliance with the revised FPDA. Moreover, it is expected that the European Commission will not revoke its finding that Switzerland's data protection legislation provides an adequate level of data protection under the GDPR.

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 revision of 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

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 organisations, 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 key official actors in the cyber-security area are as follows.

- MELANI, the Federal Reporting and Analysis Centre for Information Assurance. MELANI focuses on the protection of Swiss critical infrastructures through early detection and threat management. It also functions as a hub for the dissemination of information to private computer and internet users, as well as local SMEs.
- The Federal Cybersecurity Competence Centre, under the leadership of the Federal Cybersecurity Delegate. In an effort to centralise the administrative activities in this area, MELANI is set to become an integral part of this Cybersecurity Competence Centre. Moreover, though this remains an ongoing process, the government will step up its cyberdefence workforce by launching a Cyber Defense Campus.
- GovCERT.ch, which MELANI set up and 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.
- The Federal Intelligence Services (FIS), through their Prophylax programme, seek to raise awareness around economic espionage and cyber-attacks. The Prophylax programme is first of all addressed to local companies, international organisations based in Switzerland as well as local universities and higher education schools. It aims to protect the industrial and education sectors against involuntary leaks.
- The Federal cybercrime agency, the Swiss Coordination Unit for Cybercrime Control (CYCO), which is primarily a forwarding and co-ordinating authority for criminal cases.
- The FDPIC, which retains strong prerogatives given the absence of stand-alone cybersecurity legislation.

Other cantonal or inter-cantonal bodies also serve a purpose of information sharing. This is notably the case of the inter-cantonal Swiss Criminality Prevention Service (or SKP PSC, under its German or French and Italian-language moniker). This service seeks to facilitate inter-cantonal police co-ordination as well as crime prevention measures.

As mentioned above, the FDPIC retains a central role in the area of cybersecurity. It can investigate cases brought to its attention and can also do so on its own initiative, within its limited powers noted above. The revised FDPA should bring about stronger enforcement powers for the FDPIC (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

In contrast to the relevant laws of most European countries, the FDPA protects information pertaining to legal entities much in the same way it protects information pertaining to individuals. The FDPIC therefore considers that a disclosure of information pertaining to legal entities to countries without such protection requires adequate safeguards. Also, because data security is seen as a subset of data protection, the scope of data security provisions encompasses any legal entity personal data as well, thus heightening cybersecurity considerations accordingly. More generally, this is a striking difference between the Swiss data protection and data security system by comparison to its EU counterparts.

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 development remains the abovementioned revision process of the FDPA.

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** concerning the Federal Cybersecurity Competence Centre).

In addition, in December 2019, the government announced that it was considering introducing a general duty on operators of critical infrastructures to notify cybersecurity breaches.

Public attention remains high. This is because of the stream of data breaches internationally, the increased awareness around data protection worldwide, but also because of some cybersecurity considerations affecting national security.

In this latter category, the global debate about Chinese hardware provider Huawei's participation in the 5G network technology deployment in many countries and the risk (real or perceived) of Chinese governmental access to confidential information has made the headlines locally. In this respect, we note that Huawei's participation in the Swiss 5G landscape is a reality and the governmental authorities have not (at the time of writing) publicly issued any ban or restriction in that respect.

The participation of a Swiss company, formerly named Crypto AG, in a decades-long international espionage scheme made the headlines in early February 2020. This case so far appears to show that a provider of encryption technology would have been co-operating with US and German services and included a backdoor into its technology, which technology it provided to an important number of foreign states. It is too early to foresee any consequences of this matter on the Swiss legal and regulatory landscape, though it will likely lead to questioning Switzerland's international policy as regards cybersecurity, cyberespionage 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. Because the Swiss legislator relies on a technologically-neutral approach, these rules on data security remain rather abstract and do not refer to any specific technology, or any specific standard or technical requirement.

So far, and in the foreseeable future, Parliament will not be removing data security from the data protection legislation and will not draft any stand-alone 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 will be upheld and bolstered upon entry into force of the revised FDPA; see **1.3 Administration and Enforcement Process**). Moreover, it is expected that an intentional failure to implement technical and organisational measures determined as a minimum standard by the Swiss Federal Council in the revised FDPO will be liable to 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 the OFCOM in case of security incidents and, more generally, contains requirements governing the security and the availability of telecommunications services and networks.

The FinfrAct is a modern law, coming into force on 1 January 2016, 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 FinfrAct.

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 inter alia 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, which both 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 as regard to the national railway industry.

2.3 Overarching Cybersecurity Agency

See **1.5 Information Sharing Organisations**.

MELANI has played a helpful role as an information-sharing platform and demonstrated the need for an increased governmental support to the area of cybersecurity. It 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). The Cyber Security Delegate (appointed in June 2019) and the Cyber Security Competence Centre are the result of the implementation plan of the 2018-2022 national strategy for the protection of Switzerland against cyber-risks. Going forward, personnel and financial resources are set to further increase and MELANI will become a part of the Cybersecurity Competence Centre.

As a consequence of the above, 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. At this time, the FDPIC cannot open an investigation unless a suspected privacy breach is capable of affecting a large number of persons and in limited additional cases, including if a mandatory notification to the FDPIC has not been made. Nonetheless, the FDPIC is a valuable contact point for all matters relating to data security and is slated to receive further enforcement powers under the revised FDPA.

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 on the Operational Risks at 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. Both these FINMA documents were recently lightly revised (taking into account the needs and limitations of small banks), the latest versions having entered into force on 1 January 2020.

2.6 Other Relevant Regulators and Agencies

See above **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 extremely 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.

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

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.

The FDPO sets out 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);
- a processing policy in certain cases of automated data files.

In the financial sector, FINMA Circular 2018/3 on Outsourcing as well as FINMA Circular 2008/3 on Operational Risks at Banks call for the targeted undertakings to ensure proper resilience and business continuity, as well as adequate incident management plans.

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 outsourcings 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 2018-2022 national strategy for the protection of Switzerland against cyber-risks, the government stressed 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), as well as 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

Under the FDPA and FDPO, there is no general reporting obligation, nor is there an affirmative security requirement. In addition, there is no obligation to notify the data subjects themselves, though arguably controllers would have to do this based on the principles of good faith and transparency, if not under any contractual obligation to do so. There may nonetheless be a public reporting duty, also arising from such principles of good faith and transparency, if it appears unfeasible or unreasonable to reach out to each data subject individually.

In any case, reporting of cyber-incidents to MELANI is well-advised and helps disseminate information about potential cyber-risks across the industry.

Going forward, the revised FDPA should contain a reporting requirement binding upon controllers. The latter will have to report to the FDPIC any data breaches resulting for high risks for the rights and freedoms of the data subjects. In addition, the Federal Council (the executive arm) announced in December 2019 that it is considering introducing a breach notification obligation in cases of cybersecurity incidents affecting critical infrastructures.

4.2 Material Business Data and Material Non-public Information

At the time of writing, there are no specific affirmative security requirements for material business data and material non-public information.

In any case, reporting of cyber-incidents to MELANI is well-advised and helps disseminate information about potential cyber-risks across the industry.

4.3 Critical Infrastructure, Networks, Systems

As mentioned in **4.1 Personal Data**, the government announced in December 2019 that it is considering introducing a breach notification obligation in cases of cybersecurity incidents affecting critical infrastructures.

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.

MELANI has issued guidelines on recommended preventive measures and countermeasures to address DDoS attacks. MELANI remains a good first contact point in case of DoS attacks.

4.5 Other Data or Systems
In the financial and banking sector, Annex 3 of FINMA Circular 2008/21 Operational Risks at Banks, there is 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.

5. Data Breach Reporting and Notification

5.1 Definition of Data Security Incident or Breach
There is no general duty to report data security incidents or breaches. As mentioned above (see in particular **4.1 Personal Data**), the situation might change in the future under, on the one hand, the revised FDPA and, on the other hand, as a result of governmental motions to introduce a reporting obligation in case of data security incidents affecting critical infrastructures.

Sectoral rules and regulations may still come into play. This is notably the case in the banking sector, where FINMA Circular 2008/21 contains wording on reporting and external communication of data security incidents.

5.2 Data Elements Covered
See above **5.1 Definition of Data Security Incident or Breach**.

In the banking sector, the data covered is CID (client-identifying data).

5.3 Systems Covered
There is no specific systems covered given the fact that, firstly, there is currently no overarching reporting obligation and, secondly, that the Swiss legislator typically opts for a technologically-neutral approach thereby eschewing any discussion around a specific technology (though exceptions exist).

5.4 Security Requirements for Medical Devices
There is no specific cybersecurity and data breach notification rules pertaining to medical devices. However, 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 is no specific cybersecurity and data breach notification rules pertaining to industrial control systems and SCADA.

5.6 Security Requirements for IoT
There is no specific cybersecurity and data breach notification rules pertaining to IoT. However, various authorities serve as valuable contact points. In particular, the FDPIC and MELANI 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 Reporting Triggers
See **5.1 Definition of Data Security Incident or Breach**.

5.8 "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, therefore, a logical 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 cyber-risks (in both its 2012 and 2018 versions) 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 Organisations**) or their sectoral regulators, if any.

7.2 Voluntary Information Sharing Opportunities

See above **1.5 Information Sharing Organisations**.

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 cyber-attacks, but they did lead to a reinforcement of the regulatory landscape and FINMA revised at that time 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 discussion to provide for class actions in civil proceedings, though proponents of this approach received a recent set-back with the Swiss government deciding against including class actions in the ongoing revision of the Swiss Civil Procedure Code. Class actions are a hotly debated topic and it is uncertain whether, or in what form, they will make it into the law.

9. Due Diligence

9.1 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.

Because of the eminently technical nature of cybersecurity measures, a technical due diligence, performed by IT cyberse-

curity auditors, is recommended. In any case, the contractual documentation around corporate transactions tend to be qualified regarding any cyber-risks.

9.2 Public Disclosure

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

9.3 Other Significant Issues

All significant issues have been addressed above.

Walder Wyss Ltd has a data protection team of about 15 members. In addition, attorneys from other teams provide advice on data protection issues related to their practice areas. Data protection advice has traditionally been a very strong practice area at Walder Wyss, reaching back more than 25 years. The firm advises major Swiss and international clients in all data protection matters, including the GDPR, and regularly represents clients before the Swiss Data Protection and Information Commissioner as well as before courts. All six office locations are fully integrated, allowing the firm to provide high-quality data protection advice throughout Switzerland and in all national languages. The firm has a strong international network when it comes to matters that require advice on foreign data protection laws.

Authors

Jürg Schneider is a doctor iuris, attorney at law, and a partner, co-head of the data protection team 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. He 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. In addition, Jürg regularly publishes and lectures on ICT topics, is a member of several professional organisations and co-editor of a website providing comprehensive information on Swiss data protection law. He is a member of the board of directors of the International Technology Law Association and was a recent co-chair of its data protection committee. Jürg's special competencies regarding data protection include drawing up data protection concepts and strategies for companies, leading and assisting compliance projects regarding implementation of GDPR (and the future revised Swiss DPA) for Swiss and international companies, advising clients in regulated sectors (banking, insurance, healthcare, etc) on data protection requirements, among others.

David Vasella is a doctor iuris, attorney at law, CIPP/E, partner and co-head of the data protection team. David advises on technology, data privacy and IP matters, with a focus on the transition of businesses into the digital space. He 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. David also regularly advises in relation to commercial IP matters, regulated products and market practices. In addition, David frequently speaks and publishes in his area of expertise. He is an editor of the Swiss journal for data law and information security and a member of the professional bodies IAPP and DGRI.

Hugh Reeves is an attorney at law and a senior associate in the information technology, intellectual property and competition team. He pursued a further education degree (LLM) at the University of California at Berkeley, where he specialised in the intersection of law and technology, before gaining additional professional experience within a leading Silicon Valley law firm. Hugh's preferred areas of practice include technology transfers, information technology law, data protection, as well as copyright, patent, trade mark and trade secret law. He is registered with the Vaud Bar Registry and admitted to practise throughout Switzerland. Hugh has contributed to many publications relating to data protection law.

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