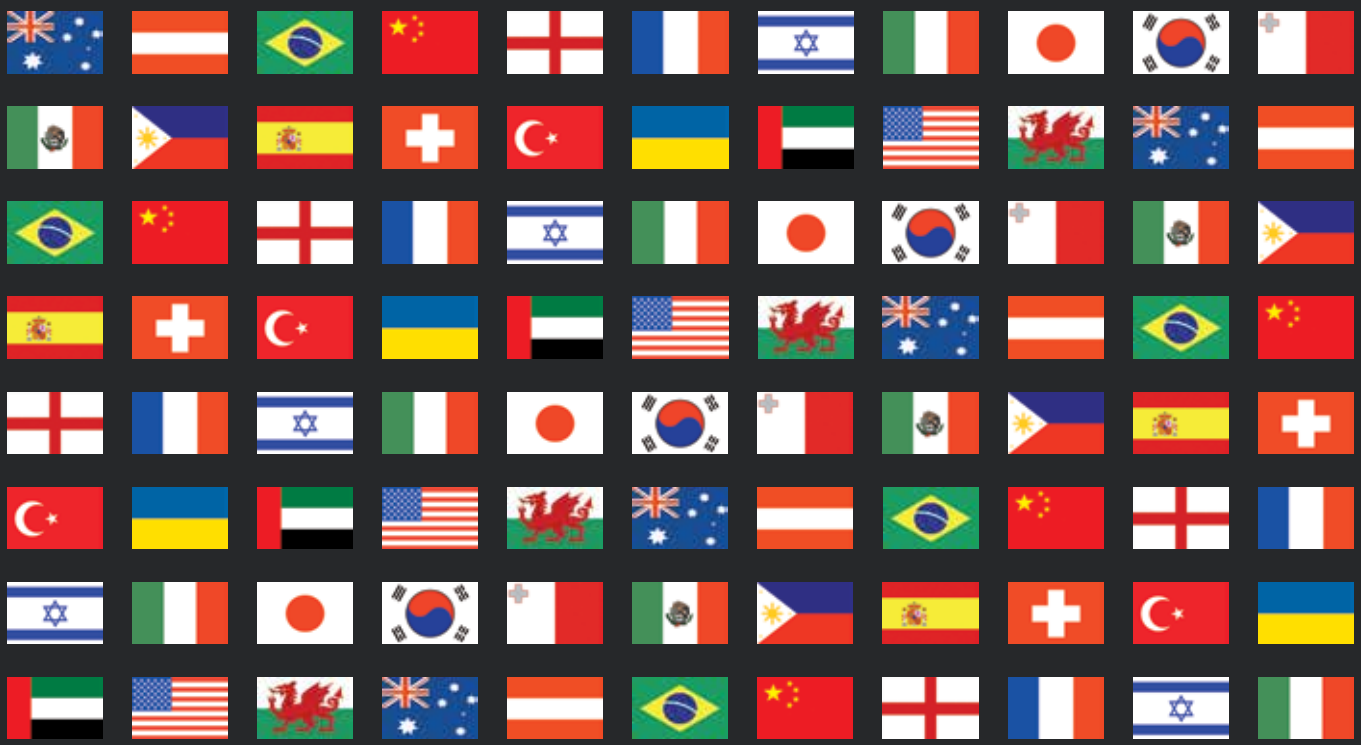
Cybersecurity

Contributing editors
Benjamin A Powell and Jason C Chipman



2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cybersecurity 2018

Contributing editors

Benjamin A Powell and Jason C Chipman

Wilmer Cutler Pickering Hale and Dorr LLP

Reproduced with permission from Law Business Research Ltd
This article was first published in January 2018
For further information please contact editorial@gettingthedealthrough.com

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
James Spearing
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2015
Fourth edition
ISBN 978-1-912377-38-1

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Preface

Cybersecurity 2018

Fourth edition

Getting the Deal Through is delighted to publish the fourth edition of *Cybersecurity*, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique **Getting the Deal Through** format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Australia, Italy, Philippines, Spain, Turkey and Ukraine.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.gettingthedealthrough.com.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Benjamin A Powell and Jason C Chipman of Wilmer Cutler Pickering Hale and Dorr LLP, for their continued assistance with this volume.

GETTING THE DEAL THROUGH

London
January 2018

Switzerland

Michael Isler, Hugh Reeves and Jürg Schneider
Walder Wyss Ltd

Legal framework

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

No dedicated cybersecurity legislation has been adopted in Switzerland to date, and there are also no plans to comprehensively address the issue in a bespoke legal instrument. Rather, cybersecurity is and will remain regulated by a patchwork of various acts and regulatory guidance.

In fact, the pertinent legislative landscape has been analysed in a report concerning the national strategy on the protection of Switzerland from cyber risks, which was approved by the federal government in 2012. In a nutshell, the report outlines the existing cybercrime defence scheme and defines the main goals for enhancing protection against cyber risks. After identifying the risks that originate from cyberthreats, the report identifies major weaknesses and resolves how the various stakeholders should proceed. The strategy emphasises three main objectives:

- early identification of threats and dangers;
- improvement of the resilience of critical infrastructure; and
- reduction of cyber risks, especially cybercrime, cyberespionage and sabotage.

The report ultimately proclaims 16 measures aimed at minimising cyber risks and enhancing cybersecurity, one of which is dedicated to the validation of the existing legal and regulatory instruments. 15 out of 16 of these measures were deemed fulfilled by the end of 2016. The report acknowledges that the existing scattered legal framework is inconsistent and incomplete, but also opines that the adoption of a comprehensive cybersecurity regime would be inappropriate for addressing cyber risks. Rather, the existing legislative framework will be subject to continuous adjustment by taking into account the specific exposure to cyber risks within the relevant scope of application of each statute. A corresponding legislative agenda has been devised, but is not publicly accessible.

In April 2017, the Federal Council, based on the success of the 'National strategy for Switzerland's protection against cyber risks', initiated a process to update this strategy for the years 2018 to 2023. Although no specifics have yet been disclosed at the time of writing, the release of a new national strategy for the years 2018–2023 is expected by April 2018.

The aforementioned national cybersecurity strategy partially overlaps with another governmental initiative, the 'Digital Switzerland' strategy, which was adopted in spring 2016. The associated action plan features, inter alia, an 'effect analysis' of the cybersecurity strategy, including an examination of aspects of international cooperation, particularly with the EU in relation to network and information security.

The following list sets out the most relevant legislative instruments dealing explicitly or implicitly with cybersecurity in the private sector.

The Budapest Convention on Cybercrime (CCC)

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

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

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

The Federal Data Protection Act (FDPA)

The FDPA governs the protection of personal data, which encompasses information pertaining to identified or identifiable natural persons and legal entities. Pursuant to article 7 FDPA, personal data must be protected against unauthorised processing through adequate technical and organisational measures. Enforcement of the data security principles is largely left to self-control by the concerned organisations and, eventually, civil courts; regulatory oversight by the Federal Data Protection and Information Commissioner (FDPIC) in the area of data security, therefore, only exists in isolated cases, but is non-existent on a large scale. In the wake of the adoption of the General Data Protection Regulation within the EU, a fundamental revision of the FDPA is ongoing.

A preliminary draft of a revised FDPA was issued in late December 2016 and, subsequently, a draft of a new FDPA was issued on 15 September 2017 for a public consultation process. The revised FDPA is tentatively scheduled to enter into force on 1 August 2018 and will bring about wide-ranging changes, not only to the FDPA itself, but to various other laws insofar as they touch upon data protection issues. In particular, legal entities will no longer benefit from dedicated data protection, transparency will be strengthened, data breaches will have to be notified in most cases and the criminal sanctions for offences against the FDPA will be bolstered. As far as data security is concerned, however, the matter has not been specifically or exhaustively addressed as a stand-alone subject and, rather, will remain part of the subject matter of the revised FDPA and its ordinance (as is presently the case under current law).

Federal Telecommunications Act (TCA)

Pursuant to article 48a TCA and article 96 of the corresponding Ordinance on Telecommunications Services (OTS), the Federal Office of Communications (OFCOM) is responsible for implementing the administrative and technical requirements pertaining to the security and availability of telecommunications services, which includes notification of the regulator in the event of security incidents. This body of laws is undergoing a revision process in order to render it more compliant with the current technological landscape; in particular, rules against unsolicited messaging and spamming will be reinforced. Moreover, the Federal Act on the Surveillance of Postal and Telecommunications Traffic of 6 October 2010 governs real-time and retroactive monitoring of postal and telecommunications traffic and has been revised, with the new law set to enter into force on 1 March 2018.

In addition, the Federal Act on the Intelligence Service has also been revised, the new law having entered into force on 1 September 2017; this Act governs the monitoring of data streams to and from Switzerland in order to fulfil antiterrorism and national security objectives.

Further, pursuant to article 15 of the Ordinance on Internet Domains, the registry for the '.ch' top-level domain (currently the SWITCH foundation) is required, if requested to do so by an OFCOM accredited body, to combat cybercrime, to block domain names if there are reasonable grounds to suspect that they are being used to access sensitive data using illegal methods (phishing) or to distribute harmful

software (malware). The only organisation entitled to accomplish this task is the Reporting and Analysis Centre for Information Assurance (MELANI).

The Federal Act on Financial Market Infrastructure (FinfrAct)

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

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

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

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

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

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

Another important instrument of financial sector oversight relevant to cybersecurity is FINMA Circular 2008/7 regarding the outsourcing by banks. It is currently undergoing a significant amendment aiming at aligning the prerequisites applicable to banks and insurers, increasing transparency of the outsourced tasks by introducing an inventory, and imposing specific obligations on systematically important banks. In contrast to prevailing trends in regulatory activity, the Circular's former provisions on data protection are proposed to be repealed to avoid duplication with the FDPA.

Another emphasis lies on the protection of critical infrastructure from cyberthreats, such as in the electricity, transportation and telecommunications sector. The healthcare sector has also received increasing attention recently, in particular, regarding the vulnerability of medical devices connected to the internet. However, it is fair to state that in small and medium enterprises, cybersecurity has not made it to the agenda of many board meetings as an item of strategic importance, but continues being treated as a mere technicality.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

Adherence to international standards related to cybersecurity (such as ISO 27001:2013) is not mandatory in Switzerland. However, many undertakings are undergoing certification voluntarily, and such standards also serve as a benchmark when it comes to compliance with best practices, as, for example, imposed by the regulator in the financial sector or by customers outsourcing their ICT operations to third parties.

Further, pursuant to article 11 FDPA, the manufacturers of data processing systems or programs, as well as private undertakings that process personal data, may submit their systems, procedures and organisations to be evaluated by an accredited independent certification body on a voluntary basis. If they do so (which is very rare), abidance by the standards of ISO 27001:2013 is a prerequisite for such certification.

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

As a matter of principle, the responsibility for cybersecurity lies with the data processing organisation and not with the individuals entrusted with the task. Failure to comply with the data security requirements enshrined in article 7 FDPA does not constitute a criminal offence and, therefore, solely provides civil (tort) remedies to the persons (including legal entities) affected by a breach. It must, however, be noted that this situation is likely to change after the entry into force of the revised FDPA. Indeed, the draft of the revised FDPA criminalises intentional violations of basic data security requirements

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

5 How does your jurisdiction define cybersecurity and cybercrime?

Neither cybersecurity nor cybercrime are defined terms under Swiss statutory laws. There is also no judicial precedence that would help clarify these terms. The neighbouring concept of data security enshrined in data protection legislation has not gained contours either, because it remains vague on the actual degree of security that is necessitated.

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

In line with the scope of application of the CCC, it can be argued that, outside heavily regulated sectors, cybersecurity in the legislative reality equates defence against cybercrime, namely repressive sanctions and procedures in relation to the crimes committed via the internet, while preventive security measures are dealt with as a sub-concern of data privacy.

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

Pursuant to article 7 FDPA, personal data (see question 1 for a definition of personal data) must be protected against unauthorised processing through adequate technical and organisational measures commensurate to the type of personal data being processed. Given these vague requirements and even though the FDPA stipulates minimum protective measures, there is a large margin of discretion as to what such minimum requirements would precisely entail (see question 26 for more details). This picture will most likely remain fundamentally unchanged under the revised FDPA, as its draft remains vague in terms of technical and organisational requirements.

Even in heavily regulated sectors, such as critical infrastructures, the minimum protective measures are rarely defined. The organisations running the infrastructure are deemed best positioned to assess and implement the actual level of cybersecurity needed for their specific

operations and risk exposures. The government would only intervene where self-regulation fails. However, the national cyber risk strategy acknowledges a desire and need to devise more authoritative cybersecurity standards. An interesting observation is that the competitive landscape would not allow the adoption of more stringent (and costly) security requirements on a national level without simultaneous international harmonisation.

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

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

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

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

In its 2012 report on cyber risks, the federal government pointed out the fragmented and inconsistent regulation of cybersecurity in critical infrastructure. Although some legislative instruments deal with protection against cyber risks, they generally lack precise definition of the required security measures. The same conclusion was reached by a similar report dealing with the national strategy for the protection of critical infrastructure, which was endorsed by the federal government in the same year.

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

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

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

Given its limited resources, MELANI's activities are limited to the sharing of knowledge and tools that are proprietary to MELANI in its capacity as a governmental agency and cannot be accessed otherwise by the industry. Such knowledge and tools, for example, consist in intelligence gathered and pooled by MELANI through the network of the national computer emergency response teams.

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

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

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

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

The telecommunications secrecy does not provide for a clear exemption with respect to filtering of malicious content. However, according to article 321-ter paragraph 4 of the SPC, breach of the telecommunications secrecy for the sake of preventing damage is justified and, therefore, not subject to prosecution. On the other hand, pursuant to article 49 TCA, the falsification or suppression of information by a person involved in the provision of telecommunications services constitutes a criminal offence. In a synthesis of these two partially contradicting provisions, the following conditions will apply:

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

A suppression of the entire message is only permissible if:

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

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The following cybercrimes are sanctioned pursuant to the SPC:

- unauthorised obtaining of data (article 143 SPC);
- unauthorised access to a data processing system (article 143-bis SPC);
- damage to data (article 144-bis SPC);
- computer fraud (article 147 SPC);
- breach of secrecy or privacy through the use of an image-carrying device (article 179-quater SPC);
- obtaining personal data without authorisation (article 179-novies SPC);
- industrial espionage (article 273 SPC); and
- breach of the postal or telecommunications secrecy (article 321-ter SPC).

Further, the TCA stipulates criminal sanctions where private information received through means of a telecommunication device is used or disclosed to third parties without permission (article 50 TCA), or of the establishment or operation of a telecommunications installation with the intention to disturb telecommunications or broadcasting (article 51 TCA). In addition, the processing of data on external devices by means of transmission using telecommunications techniques without informing users thereof is prohibited (article 45c TCA) and constitutes a misdemeanour. Last but not least, transmission of mass advertising

through telecommunication channels (spam) constitutes an act of unfair competition and is criminalised as such.

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

Although cloud services have become increasingly popular in Switzerland, there are no specific provisions with regard to the security requirements of cloud computing. Accordingly, the general data protection provisions apply. If personal data are processed in the cloud by a provider, such processing regularly qualifies as data processing by a third party on behalf of the principal as per article 10a FDPA. Pursuant to this provision, the processing of personal data may be outsourced to a cloud provider by agreement or by law if the data are processed only in the manner permitted for the principal itself and the outsourcing is not prohibited by a statutory or contractual duty of confidentiality. Moreover, the principal must ensure that the provider guarantees appropriate data security. Depending on the sensitivity of data processed in the cloud, this may entail an obligation of the principal to conduct security audits, which will often be unrealistic in a cloud setting. In practice, principals will largely rely on the cloud providers' data security certifications, which, however, provide no guarantee that the respective security controls and procedures are actually heeded.

Additionally, cloud computing will frequently entail cross-border disclosure of personal data. According to article 6 FDPA, personal data must not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular, due to the absence of legislation in the country of import that guarantees an adequate level of data protection. However, even in the absence of such comparable privacy legislation, cross-border disclosure through cloud services is generally permissible if sufficient alternative safeguards (in particular, contractual clauses) substitute for an adequate level of data protection. Given that in Switzerland data pertaining to legal entities are, in contrast to the majority of European data protection laws, qualified as personal data, outsourcing to the cloud in a cross-border setting may often trigger the obligation to enter into contractual guarantees; it must, however, be noted that the draft revised FDPA does away with the qualification of legal entities as data subjects, and the divergence between Swiss and EU law is thus expected to be evened out in this respect with the entry into force of the revised FDPA.

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

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

Best practice

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

MELANI, which is sponsored by the federal government, has adopted recommendations for small and medium-sized enterprises with regard to best practices for removing malware, cleaning up websites, protecting industrial control systems and content management systems, secure e-banking and countering distributed denial-of-service attacks. They are partially based on recommendations issued by the US Industrial Control Systems Cyber Emergency Response Team.

14 How does the government incentivise organisations to improve their cybersecurity?

Apart from the services provided by MELANI, the federal government also has a stake in the public–private partnership Swiss Cyber Experts, which is an alliance of cybersecurity experts in the ICT industry, the private and public sector, and science. The Swiss Internet Security Alliance is a similar project, which aims to reduce the infection rate of devices within Switzerland. Further, cybersecurity projects occasionally receive a grant from the Commission for Technology and Innovation, which is a federal innovation promotion agency responsible for encouraging science-based innovation in Switzerland by providing financing, professional advice and networks. Apart from these examples, no other meaningful incentive schemes exist.

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

The pertinent industry norms, such as ISO 27001:2013, can be obtained from the Swiss Association for Standardization against payment (www.snv.ch). Further, MELANI provides some additional guidance (www.melani.admin.ch).

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

Victims of cyberattacks are encouraged to share information and to report incidents to the supporting units maintained by the federal government (see question 17).

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

Victims of cyberattacks are encouraged to notify incidents to MELANI. The report can be made by a simple message on MELANI's website and may be submitted anonymously. If the victim is also interested in a criminal investigation, a complaint may be filed with the Cybercrime Coordination Unit Switzerland (CYCO). CYCO is Switzerland's reporting channel for illegal subject matter on the internet. Complaint forms are available on its website. CYCO will forward the complaint to the competent prosecution authority in the country.

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

The national strategy for the protection of Switzerland against cyber risks, which was adopted by the federal government in 2012, has identified a desire within the industry for intensified cooperation between the public authorities, the private sector and operators of critical infrastructure in order to mitigate cyber risks. Stakeholders expect increased consistency in the elaboration of standards and procedures to be devised in a cooperative manner. The federal government also holds that the primary responsibility to fight cyberattacks lies with each responsible organisational unit individually, and the authorities are only supposed to interfere if public interests are at stake or if the relevant risks cannot be addressed at the competent subordinate level. In line with this strategy, the government is a stakeholder in private initiatives dedicated to the enhancement of cybersecurity awareness and defence schemes (see question 14).

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

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

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

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

- the FDPIC, who is responsible for the supervision of private undertakings with regard to their compliance with the FDPA; and
- CYCO, which forwards cases of incoming reports to the appropriate prosecution authorities in Switzerland and abroad (namely the police and public prosecutors in charge of prosecuting cybercrimes).

On a sectoral level, the authorities entrusted with regulatory oversight are also responsible for enforcing compliance of the regulated

Update and trends

In contrast to neighbouring jurisdictions, the Swiss government has so far rebutted plans to initiate bespoke cyber risk legislation. The official strategy still counts on self-education and self-regulation, seconded by a strengthening of data breach obligations under the revised data protection act and specific sectoral regulations for critical infrastructures. However, the multiple cyberattacks that have prominently hit Swiss undertakings and public institutions in the past year have eventually driven political initiatives to consider cyber legislation. Further, the cybercrime agency MELANI has been criticised for a lack of resources, skills and persuasiveness. In order to address these shortcomings, a parliamentary commission on security policies has recently called for the prompt setting up of a federal cybersecurity competence centre as well as an army-run cyber defence organisation comprising 'cyber troops' and tasked with defending Swiss interests in the cyber environment. Hence, cyber risk regulation is already on the legislative agenda.

As hinted at above, another area of cyber risk has emerged to public awareness in the past year: cyber warfare. There are first attempts on the international stage to launch a debate on an international treaty, and the Swiss government has repeatedly shown support for such an initiative.

undertakings with cybersecurity rules. In crisis situations affecting critical infrastructure, the special task force for information assurance would intervene. It is composed of decision-makers from the public and private sector dealing with critical infrastructures. Critical infrastructures are those involved in power supply, emergency and rescue services, banks and insurance companies, telecommunications, transport and traffic, public health (including water supply), as well as the government and public administrations.

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

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

On a general level, the FDPIC is endowed with powers to investigate cases on his or her own initiative or at the request of a third party if methods of data processing are capable of breaching the privacy of a larger number of persons (conceptual systemic failures). This could, for instance, be the case if a specific undertaking processing a large number of sensitive personal data is suspected of neglecting data security obligations. However, the investigative powers would not extend to the examination of data breaches. In the performance of his or her duties, the FDPIC is empowered to request files, obtain information and investigate data processing mechanisms. The FDPIC does not, however, have enforcement powers; he or she may only issue recommendations. If these recommendations are not complied with, the FDPIC may institute proceedings before the Swiss Federal Administrative Court (see question 23 for more details). By contrast, the draft of the revised FDPA gives the FDPIC the authority to issue binding decisions and take the administrative measures he or she deems necessary.

In regulated sectors, the authorities do have extended investigative powers within their field of competence. By way of example, FINMA may appoint independent experts to conduct audits of supervised persons and entities that must provide such experts with all information and documents required to carry out their tasks.

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

Switzerland has experienced an increased exposure to cyber incidents in the recent past, with ransomware and identity theft being among the top issues; more specifically, MELANI observed an increase of incidents concerning the WannaCry and NotPetya ransomware as well as usurpation of the names of various federal authorities or companies (such as the Swiss Post and Swisscom). In July 2017, the federal government managed to fend off a cyberattack using the Turla malware, which targeted the servers of the Department of Defence, Civil Protection and Sport.

The most notable event, however, surfaced in spring 2016, when it was revealed that the Swiss defence technology company RUAG had been the victim of cyberespionage since 2014, resulting in a loss of approximately 23Gb of data. The federal government decided to have the report of the technical analysis conducted by MELANI published to give organisations the chance to check their networks for similar infections, and to show the modus operandi of the attacker group.

On a judicial level, the expectations of expedited international cooperation in combatting cybercrime propagated by the CCC suffered a setback by a landmark decision handed down by the Swiss Federal Supreme Court in January 2015 – the judges ruled that cantonal prosecutors were not empowered to bypass judicial assistance and order Facebook to release the IP history of its users by virtue of article 32 of the convention. With respect to cybersecurity regulations, new rules on the treatment of electronic client data by banks adopted by FINMA entered into force at the beginning of 2015, with a further tightening having entered into force in July 2017. These amendments have boosted cybersecurity awareness in the financial sector.

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

If a recommendation made by the FDPIC in the course of an investigation (referred to in question 21) is not complied with or is rejected by the affected entity, the matter may be referred to the Swiss Federal Administrative Court for a decision. There is also the right to appeal against such decision before the Swiss Federal Supreme Court. However, there are no penalties associated with this. As mentioned above (see question 4), the draft revised FDPA contains provisions under which failure to follow the basic data security requirements may lead to a criminal fine.

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

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

In the absence of a general obligation to report cyberthreats and data breaches, there are no criminal or administrative penalties associated with such failure. In regulated sectors, failure to submit a required report to the regulatory authority may be prosecuted as a crime or entail administrative sanctions, depending on the applicable statute in question. It can, however, already be noted that the draft of the revised FDPA calls for data breaches to be notified to the FDPIC, unless an exception applies (see question 28 for further details on the notification of data breaches); this reporting obligation, if not heeded, may lead to criminal penalties. Moreover, failure to implement the minimal requirements for data security is criminally sanctioned by a fine.

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

Victims of cyberattacks may seek redress in a civil action against the tortfeasor. This may be the cybercriminal or the entity that has failed to comply with appropriate data security standards and procedures. Since class actions do not exist in Switzerland, private individuals whose data have been hacked will, in most cases, be incapable of asserting financial damages in an amount that merits a claim. As mentioned above (see question 24), the draft revised FDPA (not yet in force) provides that if the basic data security measures were not implemented, a criminal complaint may be filed by the injured party, which may lead to a criminal fine.

Threat detection and reporting

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

As mentioned in question 6, personal data must be protected against unauthorised processing through adequate technical and organisational measures. Such measures are set forth in more detail in articles 8 to 12 of the implementing Ordinance to the FDPA. Any systems in which personal data are processed must live up to appropriate state of the art technical standards in terms of protection against risk of unauthorised or accidental destruction or loss, technical flaws, forgery, theft or unlawful access, copying, use, alteration and other kinds of unauthorised processing. More specific requirements are imposed on systems

that feature automated processing of personal data. Such systems must, in particular, ensure appropriate access, disclosure, storage and usage controls. It is worth mentioning that, in the context of the revision of the FDPA, the implementing Ordinance to the FDPA is also slated for an overhaul; such a revised ordinance has, however, not yet been issued.

Sector-specific regulations do not contain more detailed requirements on the actual standards to be implemented.

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

To date, Swiss law does not expressly prescribe such recording obligations.

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

The current FDPA does not provide for an explicit obligation to notify data breaches. Should Switzerland ratify the revised Council of Europe Treaty 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), a notification obligation in the case of data breaches would have to be included in local law. Pursuant to article 7, paragraph 2, of the revised treaty, the data controller is obliged to notify, without delay, at least the competent supervisory authority of data breaches that may seriously interfere with the rights and fundamental freedoms of data subjects. Consequently, and in anticipation of the said ratification, the draft of the revised FDPA provides for a duty to notify data breaches to the FDPIC (see question 24). The draft rules call for data controllers to notify the FDPIC as soon as possible in case a data breach occurs and when such breach is likely to result in a high risk to the privacy or the fundamental rights of the data subject; conversely, the data processors have to notify all breaches of data security to the data controller as soon as possible. This breach notification mechanism will not systematically require informing the data subjects, as this step shall only be required when necessary for the protection of the data subject or if requested by the FDPIC.

Sector and critical infrastructure specific notification duties include:

- financial services sector: mandatory notification to FINMA without delay regarding events of material relevance for the supervision of the relevant supervised entity;
- telecommunications sector: notification to OFCOM in the case of faults in the operation of telecommunications networks that affect a significant number of customers;
- aviation sector: notification to the Federal Office of Civil Aviation in the case of safety-related data breaches;
- railway industry: notification to the Federal Department of the Environment, Transport, Energy and Communications in the case of severe incidents; and
- nuclear sector: notification to the Swiss Federal Nuclear Safety Inspectorate in the case of safety-related data breaches.

29 What is the timeline for reporting to the authorities?

The sector-specific provisions mentioned in question 28 require the affected entity to report any relevant cybersecurity incidents without delay.

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

Scholarly opinion holds that article 4, paragraph 2, FDPA, which stipulates the principle of good faith, entails the rule that data subjects must be informed of unauthorised access to their data. However, such notification duty depends on the gravity of the breach in question. Further, specific contractual obligations may impose on organisations a duty to report threats or breaches. As mentioned above (see questions 24 and 28), the draft of the revised FDPA contains rules on the notification of data breaches. Pursuant to these rules, the data controller may be required to inform the data subjects of the breach if such information should prove necessary for the protection of the data subject or if it is requested by the FDPIC.

walderwyss attorneys at law

Michael Isler **michael.isler@walderwyss.com**
Hugh Reeves **hugh.reeves@walderwyss.com**
Jürg Schneider **juerg.schneider@walderwyss.com**

Seefeldstrasse 123
8034 Zurich
Switzerland

Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
www.walderwyss.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

ISBN 978-1-912377-38-1