iclg

Cybersecurity 2025

Eighth Edition

Contributing Editor:
Edward R. McNicholas
Ropes & Gray LLP

glg Global Legal Group

Expert Analysis Chapters

Q&A Chapters

Switzerland


Daniela Fábián


Aranya di Francesco

FABIAN PRIVACY LEGAL GmbH

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Art. 143bis of the Swiss Criminal Code (SCC) (unauthorised access to a data processing system) is the "hacker paragraph" in Switzerland. According to Art. 143bis para. 1 SCC, anyone who obtains unauthorised access by means of data transmission equipment to a data-processing system that has been specially secured against access, shall be criminally liable. Any person who markets or makes available passwords, programs or other data that he/she knows or must assume are intended to be used to commit such an offence (hacking tools) shall also be criminally liable (Art. 143bis para. 2 SCC). The maximum penalty is a custodial sentence not exceeding three years or a monetary penalty for both cases. Criminally punishable hacking requires that a security mechanism is in place (encryption, ciphering or password protection). Where the attacker is knowingly and intentionally provided with the access information and is solely contractually or morally obliged to not use it, no criminal sanctions can be imposed.

Criminal liability due to violation of Art. 143bis para. 1 SCC has been ruled in the following case:

- Login to a password-protected e-mail account with a password that the offender found on a piece of paper, which the owner of the e-mail account has accidentally left behind in a former shared apartment, without the intention to share the password with the offender.[1]

In contrast, criminal liability was denied in the following cases:

- Access to an IT application as well as business e-mails of a company, since the accused was voluntarily provided with the (administrative) access rights.[2]
- Unauthorised access to a password-protected laptop. The accused was in possession of the utilised password with the knowledge and consent of the laptop owner, since the accused had set up the laptop. The laptop owner did not change the password after the set-up.[3]

In Switzerland, hacking may further constitute a criminal offence pursuant to Arts 143 or 179^{novies} SCC. According to Art. 143 SCC (data theft), any person who, for his/her own or for another's unlawful gain, obtains for him/herself or another data that is stored or transmitted electronically or in some similar manner and which is not intended for him/her and has been specially secured to prevent his/her access shall be criminally liable. The maximum penalty is a custodial sentence not exceeding five years or a monetary penalty. Art. 143 SCC requires that the offender in fact obtains data (in contrast to Art. 143bis SCC above) and overcomes safety measures for this reason. Where sensitive personal data is obtained, Art. 179^{novies} SCC (obtaining personal data without authorisation) states that any person who, without authorisation, obtains personal data that is particularly sensitive and that is not publicly accessible, shall be liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty.

Denial-of-service attacks

Denial-of-service attacks (DoS attacks) are punishable pursuant to Art. 144bis SCC (damage to data). According to Art. 144bis SCC, any person who without authority alters, deletes or renders unusable data that is stored or transmitted electronically or in some other similar way shall be criminally liable. The fine is a custodial sentence not exceeding three years or a monetary penalty. Where major damage is caused, the custodial sentence can reach up to five years. Damage to data is considered caused when the data cannot be accessed, even if this is only temporary, e.g. due to a DoS attack. Depending on the course of action of the attacker(s), a DoS attack can also be punishable under Art. 156 SCC (extortion) or Art. 181 SCC (coercion).

Phishing

Depending on the circumstances of the case, phishing may be punishable under different provisions of the SCC, such as Art. 143bis (unauthorised access to a data-processing system), Art. 144bis (damage to data), Art. 146 (fraud), Art. 147 (computer fraud), Art. 179^{novies} (obtaining personal data without authorisation) and Art. 251 (forgery of a document). The Swiss Federal Criminal Court (FCC) convicted an offender pursuant to Art. 147 SCC where victims were deceived to enter their account details into a phishing website and the corresponding passwords/pins were obtained by the means of *social engineering* as a form of deception.[4]

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

IT systems may be infected in the event of a DoS attack, which is punishable under Art. 144bis SCC, or to conduct phishing, which can constitute different criminal offences as outlined above. Where malware is used to execute hacking, theft of data or sensitive data, it is punishable pursuant to Art. 143, Art. 143bis or Art. 179^{novies} SCC (*cf.* above).

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime
The distribution of hacking tools is punishable under Art. 143bis para. 2 SCC with a custodial sentence not exceeding three years or a monetary penalty (*cf.* above). Further, the manufacturing, import, marketing, advertising, offering or otherwise making accessible of data-damaging programs (e.g. viruses) to commit damage to data is also punishable and can lead to a custodial sentence not exceeding three years or a monetary penalty. Where the offender acts for commercial gain, a custodial sentence of up to 10 years shall be imposed (Art. 144bis para. 2 SCC). Criminal liability due to violation of Art. 144bis para. 2 SCC has been ruled in the case of selling of CD-ROMs with instructions for the creation of a data-damaging program.[5]

Possession or use of hardware, software or other tools used to commit cybercrime
Depending on how the tools are used, the conduct may, for instance, be punishable as hacking or phishing (*cf.* above). The mere possession of hardware, software or other tools to commit cybercrime is not criminalised.

Identity theft or identity fraud (e.g. in connection with access devices)
On 1 September 2023, a new clause entered into force that criminally punishes identity theft. According to Art. 179^{decies} SCC, any person who uses the identity of another person without that person's consent in order to harm that person or in order to obtain an unlawful advantage for him/herself or another shall be criminally liable. The maximum sentence is a custodial sentence not exceeding one year or a monetary penalty. The offender must act with the intention of causing damage or gaining an advantage. The use of an identity out of exuberance or as a joke is not punishable. Where identity theft is committed for the purpose of damaging another person's reputation, it can be punished pursuant to Arts 173–178 SCC (offence against personal honour).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft is punishable under Art. 143 SCC or, where sensitive data is concerned, Art. 179^{novies} SCC (*cf.* above).

Breach of confidence by a current or former employee is punishable under:

- Art. 162 SCC: Any person who betrays a manufacturing or trade secret that he/she is under a statutory or contractual duty not to reveal, and any person who exploits for him/herself or another such a betrayal shall be criminally liable. The maximum penalty is a custodial sentence not exceeding three years or a monetary penalty.
- Where a person is subject to special secrecy, criminal liability may be triggered pursuant to Art. 320 SCC (breach of official secrecy), Art. 321 SCC (breach of professional confidentiality, e.g. for lawyers), Art. 321bis SCC (breach of professional confidentiality in research involving human beings) or Art. 321ter SCC (breach of postal or telecommunications secrecy). The sanction depends on the offence and amounts up to a custodial sentence not exceeding three years or to a monetary penalty.
- For all other professionals that are not subject to a special secrecy obligation as outlined above, Art. 62 of the Federal Act on Data Protection (FADP) applies and sanctions anyone who wilfully discloses secret personal data that they had obtained while practising their profession. The sanction is a fine not exceeding CHF 250,000.

Copyright infringements are punishable under Art. 67 *et seqq.* of the Copyright Act (CopA). According to Arts 67 and 69 CopA, infringement of copyrights or related rights can lead up to a custodial sentence not exceeding five years or a monetary penalty.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)
This behaviour is also known as "white-hat hacking". White-hat hacking is not *per se* legal in Switzerland, even if it is conducted with good intentions. It may lead to criminal liability under Art. 143bis SCC (*cf.* above), as hacking without the intention of enrichment is also a criminal offence. The Swiss data protection authority (Federal Data Protection and Information Commissioner (FDPIC)) has published a guideline for white-hat hackers explaining their legal position and the risks they take.[6]

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data
Such activities include disruption of public services (Art. 239 SCC), participation in a criminal or terrorist organisation (Art. 260ter SCC), political, industrial or military espionage (Arts 272–274 SCC) and money laundering (Art. 305bis SCC). Note that offences under the SCC are prosecuted either *ex officio* or on complaint (within three months).

If personal data is involved, cybersecurity Incidents may further constitute a breach of the data security requirements on the part of the addressee of the attack (*cf.* question 2.3 below). This either results in a criminal monetary penalty not exceeding CHF 250,000 (Art. 61 lit. c FADP) or administrative measures as outlined in Art. 51 FADP.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The FADP has an extraterritorial application (Art. 3 FADP). For the SCC, the principle of territoriality applies (Art. 3 SCC); however, in certain cases, the SCC also has extraterritorial application (Arts 4–7 SCC).

2 Cybersecurity Laws

2.1 *Applicable Laws*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, trade secret protection laws, data breach notification laws, confidentiality laws, and information security laws, among others.

In Switzerland, there is a vast number of applicable laws in the area of cybersecurity. At a higher level, the National Cyberstrategy (NCS) defines the national strategy and measures for the protection of Switzerland against cyber risks. The first NCS (NCS I) was implemented from 2012 to 2017, the second NCS (NCS II) from 2018 to 2022. The newest NCS (NCS III) was approved in April 2023. Further, Switzerland is bound by the Budapest Convention on Cybercrime (Budapest Convention), which came into effect on 1 January 2012 and requires Member States to harmonise their criminal law concerning cybersecurity.

Crucial laws that private companies from *all sectors* may consider in the area of cybersecurity are the following (non-exhaustive):

- SCC (*cf.* section 1 above);
- FADP and the Data Protection Ordinance (DPO) – applicable to the processing of personal data. In the context of cybersecurity, Art. 7 para. 1 FADP (privacy by design), Art. 8 FADP (data security) and Arts 1–6 DPO (technical and organisational measures to ensure data security) should be emphasised;
- Swiss Code of Obligations (CO) – in particular Art. 328 CO (duty of care of the employer to protect employees' personal data), Art. 321a CO (obligation of the employee to exercise due care to prevent cyber-attacks such as avoiding the download of malware or conducting risky behaviour such as login into unsecured Wi-Fi connections) and Art. 716/754 CO (liability in the area of cybersecurity);
- CopA (*cf.* section 1 above);
- international compliance regimes that claim extraterritorial application such as the EU General Data Protection Regulation (GDPR); and
- non-binding national and international cybersecurity standards and recommendations such as the information security checklist for small and medium-sized enterprises (SMEs) published by the Swiss National Cybersecurity Centre (NCSC),[7] the ISO Standards of the "2700" series, and the Cybersecurity Framework of the National Institute of Standards and Technology (NIST).

Sector-specific applicable laws are mentioned under questions 2.2 and 4.2 below.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes. Arts 74–80 of the Information Security Act (ISA) apply to public and private organisations that operate critical infrastructures (Art. 2 para. 5 ISA). These articles require operators of critical infrastructure to cooperate with the Swiss Federal Government to ensure that network and system disruptions as well as any misuse are rare, short-lived and manageable and that the extent of damage is low (Art. 74 para. 1 ISA). There is currently an ongoing revision of the ISA: as of 1 January 2025, operators of critical infrastructures shall be obliged to report cyber-attacks on their IT resources to the NCSC within 24 hours (Arts 74a and 74e para. 1 draft revised ISA). This reporting obligation is comprehensive and affects institutions operating in the areas of energy supply, financial institutions, insurances, health facilities and medical laboratories (a full list can be found in Art. 74b draft revised ISA). In contrast to the reporting obligation under the FADP (*cf.* question 2.4 below), all cybersecurity Incidents must be reported (even if they do not involve personal data). Exceptions are provided (Art. 74c draft revised ISA) and non-compliance may lead to a fine up to CHF 100,000 (Art. 74h draft revised ISA).

The Federal Office of National Economic Supply (FONES) has published ICT minimum standards and recommends that operators of critical infrastructures implement these.[8]

2.3 *Security measures*: Are organisations required under Applicable Laws to take specific security measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Across all sectors, the FADP and the DPO require organisations to implement adequate technical and organisational security measures (TOMs) for the processing of personal data and for preventing cybersecurity Incidents (Art. 8 FADP, Art. 1 *et seqq.* DPO). The measures follow a risk-based approach: considering the extent to which personal data requires to be protected, security measures must be in place that ensure confidentiality, availability, integrity and traceability of the data being processed. For the design of the specific TOMs, the FDPIC has published a guide on TOMs.[9] Further, the information security checklist for SMEs of the NCSC and sector-specific requirements may also be consulted (*cf.* questions 2.1 and 2.2 above and question 4.2 below).

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

For data security breaches involving personal data, the FADP introduced a general reporting obligation. Details on this duty of notification of data security breaches can be found in Art. 24 FADP and Art. 15 DPO and are outlined hereinafter:

(a) The controller, being the entity that determines the purpose and means of the data processing, shall notify the FDPIC of any breach of data security that is likely to lead to a high risk to the affected individual's (data subject's) personality or fundamental rights.

(b) The notification must be submitted to the FDPIC by the controller as "quickly as possible".

(c) The minimum information that must be reported is: (i) the form of the breach of data security (e.g. cyber-attack leading to unlawful disclosure); (ii) the consequences, including any risks, for the data subjects; (iii) the measures that have been taken or are planned in order to remedy the Incident and mitigate the consequences, including any risks; (iv) the name and the contact details of a contact person; (v) the time and duration of the breach, where possible; (vi) the categories and approximate amount of personal data concerned, where possible; and (vii) the categories and the approximate number of data subjects affected, where possible.

(d) No exemptions apply. The FDPIC is, however, entitled to further inform the public on such data breaches via press release, which it has done in the past (e.g. in the case of stolen data from booking platforms such as booking.com), and the public has the possibility to request access to official documents pursuant to the Federal Act on Freedom of Information in the Administration (FoIA).

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

(a) The controller shall inform the affected individuals if this is necessary for their protection, e.g. by changing access information or a password, or if the FDPIC requests it. However, the controller can restrict the information to the data subject, defer it or refrain from providing information if (a) there are specific grounds listed in the FADP or a statutory duty of secrecy prohibits, (b) information is impossible or requires disproportionate effort, or (c) the information of the data subject is ensured in an equivalent manner by a public announcement.

(b) The nature and scope of the information to be reported is set out in Art. 15 para. 3 DPO and includes: (i) the form of the breach of data security; (ii) the consequences, including any risks, for the affected individuals; (iii) the measures that have been taken or are planned in order to remedy the breach and mitigate the consequences, including any risks; and (iv) the name and contact details of a contact person. In contrast to the notification to the FDPIC, the report to the affected individuals must be provided in the simplest and most comprehensible language possible.

2.6 *Responsible authority(ies)*: Please provide contact details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

Notifications can be submitted online via the portal of the FDPIC.[10] The details of other competent authorities (the NCSC and the Swiss Financial Market Supervisory Authority (FINMA)) can be found under question 2.2 above and question 4.2 below.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

There is no *direct* sanction for non-notification of a data security breach to the FDPIC. However, failure to comply with the minimum requirements for data security can be sanctioned with a criminal fine not exceeding CHF 250,000. The consent of the notifying party is required for the notified information to be passed to the competent prosecution authorities, which is expected to be withheld in the vast majority of cases.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

Enforcement due to non-compliance with minimum data security requirements took place regarding a ransomware Incident involving the Federal Office of the Police (fedpol), the Federal Office for Customs and Border Security (FOCBS) and their processor, the IT company Xplain. After a ransomware attack against Xplain in May 2023, a large amount of personal data, including sensitive personal data of fedpol and the FOCBS, was published on the darknet. The FDPIC concluded that Xplain, fedpol and the FOCBS all had breached minimum standards of data security and issued recommendations.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
At the time of writing, there are no laws prohibiting the use of beacons to protect IT systems. It must be ensured that legal requirements such as transparency and purpose limitations are met.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
There is no law prohibiting the use of honeypots to protect IT systems in a manner compliant with applicable laws.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
The same considerations apply as mentioned above regarding beacons and honeypots.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber attacks?

Such measures shall comply with Art. 328b CO, Art. 26 of the Ordinance 3 of the Swiss Employment Act (EmpO 3) as well as the FADP. According to Art. 328b CO, the employer may handle data concerning the employee only to the extent that such data concerns the employee's suitability for his/her job or is necessary for the performance of the employment contract. Art. 26 EmpO 3 prohibits the use of surveillance or control systems to monitor the behaviour of employees in the workplace, and the FADP stipulates that processing of personal data must be proportionate, hence, where milder methods are possible, these shall be preferred (e.g. policies that ideally prohibit the use of business applications for private purposes and installation of newest updates and protection measures such as firewalls and anti-virus programs).

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber attacks?

Yes, since such technologies may also be used to carry out cyber-attacks. The importer must therefore be careful not to make him/herself liable to prosecution under Art. 143bis para. 2 or Art. 144bis para. 2 SCC (*cf.* section 1 above). Further, the Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods (Goods Control Act (GCA)), its

ordinance (Goods Control Ordinance (GCO)), the Embargo Act, and the Ordinance on the Export and Brokerage of Goods for Internet and Mobile Communication Surveillance contain restrictions regarding export, import, transit and brokerage.

4 Specific Sectors

4.1 Do legal requirements and/or market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes. Legal requirements and/or market practice vary across different business sectors in Switzerland (*cf.* question 4.2 below).

4.2 Excluding the requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services, health care, or telecommunications)?

Financial and insurance services

In Switzerland, the financial services market (e.g. banks, insurance companies) is supervised by the FINMA. Crucial legislation for the supervision activities of the FINMA are the Financial Market Supervision Act (FINMASA), the *ordinances* of the FINMA, *circulars* of the FINMA on the application of the financial market legislation (Art. 7 FINMASA) and FINMA *guidances*. The FINMA has consistently identified cyber risks as one of the main risks facing the Swiss financial centre, hence, the following sector-specific requirements must be considered:

- **Cybersecurity standards:** In addition to the requirements of the FADP and the DPO (*cf.* question 2.3 above), banks shall consider for the management of cyber risks the FINMA circulars "2017/1 corporate governance – banks"[11] and "2023/1 operational risks and resilience – banks".[12] Insurance companies are subject to FINMA circular "2017/2 corporate governance – insurers".[13] In 2022, the Swiss Financial Sector Cybersecurity Centre association was founded with the participation of the NCSC, which does not set any binding standards, but offers guidance to strengthen cybersecurity in the financial sector and is supported by the FINMA in this regard.
- **Special reporting obligations:** Institutions must report cyber-attacks to the FINMA pursuant to Art. 29 para. 2 FINMASA. The FINMA guidance 05/2020 on the duty to report cyber-attacks[14] and the recently published clarification to the 05/2020 guidance (FINMA guidance 03/2024)[15] contain details on the extent of the notification and the notification deadlines. The FINMA expects an initial report to be made to the FINMA within the first 24 hours following an Incident, and the detailed report can then be submitted subsequently via a web-based survey and application platform (EHP).[16] Where an institution must also report to the NCSC (e.g. banks, insurance companies; *cf.* question 2.2 above), the notification can be first addressed to the NCSC with the request to forward the notification to the FINMA. Failure to comply with the reporting obligation under Art. 29 para. 2 FINMASA may result in a sanction (e.g. a fine up to CHF 500,000 pursuant to Art. 49 para. 1 lit. b of the Swiss Banking Act) or supervisory measures such as a professional ban (Art. 33 FINMASA).

Healthcare

The healthcare sector is a major focus of cybersecurity and data protection authorities in Switzerland. The NCSC has issued recommendations on cybersecurity for the entire healthcare sector (hereinafter), and the FDPIC has conducted numerous proceedings in this area, e.g. data protection issues of the platform regarding electronic vaccination cards "meineimpfungen.ch".[17]

- **Cybersecurity standards:** Health data is typically personal data, and a higher standard must be applied to cybersecurity measures in accordance with the FADP and its risk-based approach as regards TOMs (*cf.* question 2.3 above). In this regard, the NCSC has defined minimum technical and organisational requirements for cybersecurity in the entire healthcare sector (e.g. patch and lifecycle management, timely monitoring of log data and blocking of risky email attachments) that it believes should be implemented as a priority across the board by all healthcare service providers.[18] With regard to specific areas, the following legislation must also be considered:
  - Electronic patient record (EPR): Providers of EPRs must obtain a certification that requires that technical and organisational certification criteria relating to data protection and data security are met (Arts 11 and 12 para. 1 lit. b Federal Act on the Electronic Patient Record (EPRA)).
  - Medical devices: Medical devices are mainly governed by the Medical Devices Ordinance (MedDO). As a general rule, medical devices, including software (Art. 3 MedDO), shall meet the general safety and performance requirements set out in Annex I of the EU-Regulation 2017/745 of 5 April on medical devices (e.g. clause 14.2 of Annex I regarding software interaction and IT environment), taking into account their intended purpose (Art. 6 para. 2 MedDO). Art. 74 MedDO explicitly addresses cybersecurity and obliges healthcare institutions to put in place all technical and organisational resources required by the state of the art to ensure that network-compatible devices are protected against electronic attacks and unauthorised access. Hospitals are obliged to maintain a risk management system for this purpose.
  - Human research: The Human Research Act (HRA) states that anyone who stores biological material or health-related personal data for research purposes must take appropriate technical and organisational measures to prevent unauthorised use thereof (Art. 43 HRA). According to the Human Research Ordinance (HRO), this includes the prevention of unauthorised or accidental disclosure, alteration, deletion and copying of health-related personal data (Art. 5 HRO).
- **Special reporting obligations:** Operators of EPRs must report Incidents classified as security-relevant in their data protection and data security system to the Federal Office of Public Health (FOPH) pursuant to Art. 12 para. 3 of the Ordinance to the EPRA. A special legal reporting obligation can also be found in Art. 66 MedDO regarding medical devices. Pursuant to Art. 66 MedDO, manufacturers must report any serious Incident that has occurred in Switzerland or Liechtenstein involving a medical device, as well as corrective measures taken, to the Swiss Agency for Therapeutic Products (Swissmedic).

Telecommunications

- **Cybersecurity standards:** In Switzerland, telecommunications service providers are subject to the Telecommunications Act (TCA). Pursuant to Art. 48a TCA, telecommunications service providers must take measures to protect against hazards, avoid damage and minimise risks as regards their infrastructures and services. Regarding details, the Federal Council is entitled to issue provisions on information security (Art. 48a para. 2 TCA):
  - Telecommunications installations (Internet of Things): The Ordinance on Telecommunications Installations (TIO) of the Federal Council and the Ordinance issued by the Federal Office of Communications (ILO) both contain rules regarding the cybersecurity of wireless devices available on the Swiss market, such as smartphones, smartwatches, fitness trackers and wireless toys.
  - Internet domains: Registries for the ".ch" and ".swiss" domain are, under certain conditions, required to block domain names suspected of being used for phishing, for distribution of harmful software (malware) or to support other harmful activities (Art. 15 of the Ordinance on Internet Domains).
- **Special reporting obligations:** Pursuant to Art. 96 of the Ordinance on Telecommunications Services (OTS), telecommunications service providers must immediately report faults in telecommunications installations and services (including cybersecurity Incidents) that could affect at least 10,000 customers to the National Emergency Operations Centre (NEOC) and provide information on the faults on a publicly accessible website. The NEOC shall inform the Federal Office of Communications (OFCOM) of the faults reported. Non-compliance may be punishable pursuant to Art. 53 TCA.

Federal administration

For federal authorities and organisations, the ISA and its four implementing ordinances entered into force on 1 January 2024 and define minimum requirements for information (cyber) security based on international standards. A reporting obligation for operators of critical infrastructures shall be introduced as of 1 January 2025 (*cf.* question 2.2 above).

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

In Switzerland, there are legal provisions according to which an Incident can amount to a breach of directors' or officers' duties and lead to personal liability, notably:

- Decision-making persons such as directors and officers carry the duty to implement minimum requirements for data security as stipulated by the Federal Council in Art. 8 para. 3 FADP and the DPO. Wilful failure to comply with such duty leads to liability and a fine not exceeding CHF 250,000 (Art. 61 lit. c FADP).
- Cyber Incidents may constitute a breach of the duty of care and loyalty of the Board of Directors (Art. 717 CO) as regards their management duties (Arts 716–716b CO) and lead to their personal liability pursuant to Art. 754 CO. Where the management has been delegated (Art. 716 para. 2 CO), the persons engaged in the business management may be liable (Art. 754 CO).

Responsible corporate governance requires that persons at management level educate themselves on cybersecurity risks and, where they do not have the know-how, engage internal or external consultants. The NCSC provides up-to-date information on current cybersecurity topics as a helpful resource.[19] By the time of writing, according to the NCSC, the most frequent types of threats are ransomware, data leaks, CEO fraud, business e-mail compromise, cheque fraud and domain registration fraud.[20]

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

This depends on the laws that are applicable to the company. The designation of a CISO is legally required for certain public authorities and organisations (e.g. the Swiss National Bank) pursuant to Art. 81 ISA. As regards personal information, the FADP does not provide for an obligation to appoint a CISO. However, federal bodies shall appoint a data protection officer (Art. 10 para. 4 FADP, Art. 2 5 *et seqq.* DPO), whose duties include the maintenance of an appropriate level of data security (Art. 26 para. 2 DPO, Art. 8 FADP). The IT measures and assessments as outlined in (b), (c) and (d) may be necessary to comply with Arts 8 and 22 as well as Art. 9 para. 2 FADP (outsourcing) and the minimum cybersecurity standards for the federal administration (e.g. Art. 8 ISA and Art. 8 of the Information Security Ordinance (risk management)). As regards the financial sector, the FINMA emphasised in its guidance 03/2024 the importance of realistic response plans and scenario-based cyber risk exercises.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met. Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Civil actions against cybercriminals may be based on Art. 41 *et seqq.* CO. This requires a financial damage, an unlawful act, causality and guilt (intent or negligence).

Failure to prevent an Incident may lead to civil actions based on the following legal bases:

- Where an Incident related to personal data leads to a violation of personality rights (e.g. theft of personal data for identity fraud), affected persons may take actions based on Art. 32 para. 2 FADP in conjunction with Arts 28 and 28*a*, as well as Arts 28*g*-28*l* of the Swiss Civil Code (e.g. claim of damages).
- Civil action may also be taken based on the Product Liability Act (PLA). The manufacturer is liable for the damage if a defective product (including software) leads to: (a) a person being killed or injured; or (b) an object being damaged or destroyed that, by its nature, is normally intended for private use or consumption and was mainly used privately by the injured party (Art. 1 PLA).

- Where a contract is in place and a breach of contract takes place, private actions may be brought based on contractual liability rules, e.g. Arts 97, 197, 368 and 398 CO.
- As regards companies limited by shares (Art. 620 *et seqq.* CO), the Board of Directors and all persons engaged in the business management can be subject to private actions based on Art. 754 CO where a cybersecurity Incident leads to damages. Slight negligence is sufficient for liability pursuant to Art. 754 CO.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

Judgment of the FSC "4A_344/2020, 4A_342/2020" dated 29 June 2021 is notable: the FSC confirmed an order to pay compensation against a member of the Board ruled by the previous cantonal court. The member of the Board was deceived by the means of social engineering and falsified e-mails to transfer a large sum of money to an unknown recipient at a bank in China. The member of the Board should have detected the fraud.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes. Insuring cybersecurity Incidents is permitted, and well-known Swiss insurance companies offer such insurance policies.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no explicit national regulatory provisions that prohibit the insurance of certain types of loss.

7.3 Are organisations allowed to use insurance to pay ransoms?

In Switzerland, there is no *per se* prohibition on paying ransoms, hence insurance companies can offer this service. When paying ramsons, however, it must be ensured that no terrorist financing is carried out (Art. 260^{quinquies} SCC) and that the obligations of the Anti-Money Laundering Act are not violated. Further, U.S. sanction law may be violated if ransom payments are paid to entities on the Specially Designated Nationals and Blocked Persons List (SDN list). Also, a non-U.S. person (hence a Swiss insurance company) may be liable under U.S. sanction laws if they enable an offence by a U.S. person. This can already be the case if a ransom payment is made in U.S. dollars because the clearing and settlement systems of such payments mandatorily require involving a U.S. financial service provider in the transaction.[21] Certain insurance companies have excluded the payment of ransoms.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. anti-terrorism laws) that may be relied upon to investigate an Incident.

In Switzerland, there is no central authority for the investigation of cyber Incidents. Hence, the investigatory powers vary depending on the Applicable Laws and the competent authority.

The provisions of the SCC (*cf.* section 1 above) are prosecuted by the cantonal criminal justice authorities and, in some cases, the Office of the Attorney General of Switzerland (Art. 22 *et seqq.* Swiss Criminal Procedure Code, CrimPC). The means for collecting evidence are outlined in Art. 139 *et seqq.* CrimPC and the compulsory measures in Art. 196 *et seqq.* CrimPC.

In investigations involving personal data (Art. 49 *et seqq.* FADP), the FDPIC can obligate the investigation addressees to cooperate and, in the case of failure to cooperate, order access to information and documents required for the investigation, access to premises and installations, questioning of witnesses and appraisals by experts (Art. 50 FADP).

For the enforcement of the FINMASA (*cf.* question 4.2 above), the FINMA has the investigatory measures of the Administrative Procedure Act (APA). Investigatory powers include the obtainment of official documents, information from the parties, information or testimonies from third parties, inspections and expert opinions (Art. 12 APA).

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No. There is no such requirement. In the case of an investigation, however, the organisations may have to cooperate and provide law enforcement authorities with encryption keys (*cf.* question 8.1 above).

9 International Compliance

9.1 How do international compliance regimes impact country-specific cybersecurity rules?

In Switzerland, international standards (e.g. ISO) are applied, even if these are usually of a non-binding nature. There are further laws, such as the GDPR, which have extraterritorial applicability and shall therefore be considered as applicable cybersecurity rules (*cf.* question 2.1 above).

10 Future Developments

10.1 How do you see cybersecurity restrictions evolving in your jurisdiction?

It can be expected that the cybersecurity regime will become stricter in the coming years: nationwide measures are foreseen to strengthen cyber resilience according to the NCS III. Specific sectors will also be affected: the FINMA has identified cyber risks as one of the main risks for the Swiss financial

sector and has recently introduced additional cyber-specific supervisory instruments (e.g. "read teaming" or "table-top exercises"). For critical infrastructures, the introduction of an extensive reporting obligation is foreseen for 2025 (*cf.* question 2.2 above).

10.2 What do you think *should* be the next step for cybersecurity in your jurisdiction?

At the current stage, a listed organisation may be subject to reporting obligations under the FADP (*cf.* question 2.4 above), sector-specific reporting obligations (e.g. Art. 29 para. 2 FINMASA, *cf.* question 4.2 above), *ad hoc* reporting requirements for listed companies (e.g. Art. 53 of the listing rules of the Swiss Exchange (SIX)) as well as the reporting obligation for critical infrastructures under the revised ISA (*cf.* question 2.2 above), which leads to coordination efforts that should not be underestimated and may interfere with correction of the problem. Hence, harmonisation would be desirable. Further, one major cybersecurity risk lays in the outsourcing of services. In this regard, the EU has enacted the Cyber Resilience Act (CRA), which aims to safeguard consumers as well as businesses buying or using products or software with a digital component. The CRA introduces an adequate level of cybersecurity in all products or software with a digital component from the development stage to the end of life (entire lifecycle). A similar approach in Switzerland may set a minimum standard of security requirements covering the entire supply chain and tackling the existing outsourcing problem.

Endnotes

1 Judgment "BGE 145 IV 185" of the Swiss Federal Supreme Court (FSC).

2 Judgment "CREP 29. Dezember 2023/692" of the cantonal court of Waadt dated 29 December 2023.

3 Judgment "S 2022 25" of the High Court of the Swiss canton of Zug dated 18 January 2023.

4 Judgment of the FCC "CA.2021.12" dated 29 November 2021.

5 Judgment "BGE 129 IV 230" of the FSC.

6 This guideline is available here: https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/datenschutz/MERKBLATT%20White%20Hat%20Hacker%20EN.pdf.download.pdf/MERKBLATT%20White%20Hat%20Hacker%20EN.pdf (last consulted 23 August 2024).

7 This checklist is available here: https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/infos-unternehmen/ncsc-merkblatt-kmu-sicherheit.pdf.download.pdf/ncsc-merkblatt-kmu-sicherheit_en.pdf (last consulted 23 August 2024).

8 The ICT minimum standards are available here: https://www.bwl.admin.ch/bwl/en/home/bereiche/ikt/ikt_minimalstandard.html (last consulted 23 August 2024).

9 This guide of the FDPIC is available here: https://www.edoeb.admin.ch/edoeb/en/home/kurzmeldungen/km2024/23012024_leitfaden_tom.html (last consulted 23 August 2024).

10 The notification form is available here: https://databreach.edoeb.admin.ch/report (last consulted 23 August 2024).

11 The circular is available here: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2017-01-20200101.pdf?sc_lang=en&hash=40C9AA3758DA15953D000B3B0497146D (last consulted 23 August 2024).

12 The circular is available here: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf?sc_lang=en&hash=1529FC7CCFD70F24BCC75C4D1B033ECF (last consulted 23 August 2024).

13 The circular is available here: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2017-02.pdf?la=en (last consulted 23 August 2024).

14 The guidance is available here: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20200507-finma-aufsichtsmitteilung-05-2020.pdf (last consulted 23 August 2024).

15 The guidance is available here: https://www.finma.ch/en/news/2024/06/20240607-mm-am-cyberrisiken/ (last consulted 23 August 2024).

16 Further details regarding EHP are available here: https://www.finma.ch/en/finma/digital-exchange/ehp,-c-,-submit-applications,-reports-and-data-or-transmit-an-ac-change/ (last consulted 23 August 2024).

17 Details can be found in the annual reports issued by the FDPIC 2022/23, p. 37 *et seqq.* and 2023/24, p. 38 *et seqq.*, which are available here: https://www.edoeb.admin.ch/edoeb/en/home/deredoeb/taetigkeitsberichte.html (last consulted 23 August 2024).

18 These minimum standards are available here: https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2022/empfehlungen-gesundheitssektor.html (last consulted 23 August 2024).

19 This information is available here: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen.html (last consulted 23 August 2024).

20 This information is available here: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/cyberangriffe-gegen-firmen.html (last consulted 23 August 2024).

21 Judgment of the FSC "4A_206/2023" dated 17 August 2023.

Daniela Fábián is the founder and executive director of FABIAN PRIVACY LEGAL GmbH.
Daniela has more than 30 years of experience in data protection, employment law, risk and programme management, security and related areas, including 19 years in-house. She advises multinational companies, SMEs and start-ups from various industries, mainly in the EU, Switzerland and the U.S., on data, data protection, security and related issues, particularly in the life sciences, pharmaceutical and medical technology sectors.
Daniela supports her clients in the assessment, development, implementation and monitoring of data and privacy strategies, governance models and global data protection programmes, as well as data transfer mechanisms with a pragmatic approach. She advises her clients on technology and IT issues, digitalisation strategies, outsourcing projects, data protection and cybersecurity, in particular on prevention, as well as on the creation and implementation of data Incident response plans.
Daniela is a member of various data protection associations, the founder and chair of the Privacy Expert Roundtable (Life Sciences) in Switzerland, and a lecturer at FernUni Switzerland for CAS Data Protection and at the Swiss Health Quality Association for Digital Marketing.

FABIAN PRIVACY LEGAL GmbH
Bäumleingasse 10
4051 Basel
Switzerland

Tel: +41 61 544 44 01
Email: daniela.fabian@privacylegal.ch
LinkedIn: www.linkedin.com/in/daniela-fábián-masoch-106b67a

Aranya di Francesco is a lawyer who focuses on areas with major sanctions and currently works with all types of issues deriving from global data protection regulation, GDPR and the FADP. She is passionate about finding practical and pragmatic solutions for clients regarding day-to-day data protection challenges. Before joining the area of privacy governance, she worked for several years at the Swiss Competition Commission where she conducted proceedings in the healthcare and financial sectors and participated in cross-border exchanges with EU authorities.

FABIAN PRIVACY LEGAL GmbH
Bäumleingasse 10
4051 Basel
Switzerland

Tel: +41 61 544 44 01
Email: aranya.difrancesco@privacylegal.ch
LinkedIn: www.linkedin.com/in/aranya-di-francesco-59a305125

FABIAN PRIVACY LEGAL GmbH is a boutique law firm specialising in privacy and data protection laws and related issues, information security, data and privacy governance, risk management, programme implementation and legal compliance.
Our strengths are the combination of expert knowledge and practical in-house experience, a strong network with industry groups and privacy associations, and close cooperation with experts in data protection, cybersecurity and cybercrime, in jurisdictions around the world. We approach mandates with a global, solution-oriented and practical approach, to deliver pragmatic and sustainable solutions.

www.privacylegal.ch

FABIAN PRIVACY LEGAL

iclg International Comparative Legal Guides

The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Cybersecurity 2025 features two expert analysis chapters and 21 Q&A jurisdiction chapters covering key issues, including:

- Cybercrime
- Cybersecurity Laws
- Preventing Attacks
- Specific Sectors
- Corporate Governance
- Litigation
- Insurance
- Investigatory and Police Powers
- International Compliance
- Future Developments

The International Comparative Legal Guides are published by: glg Global Legal Group