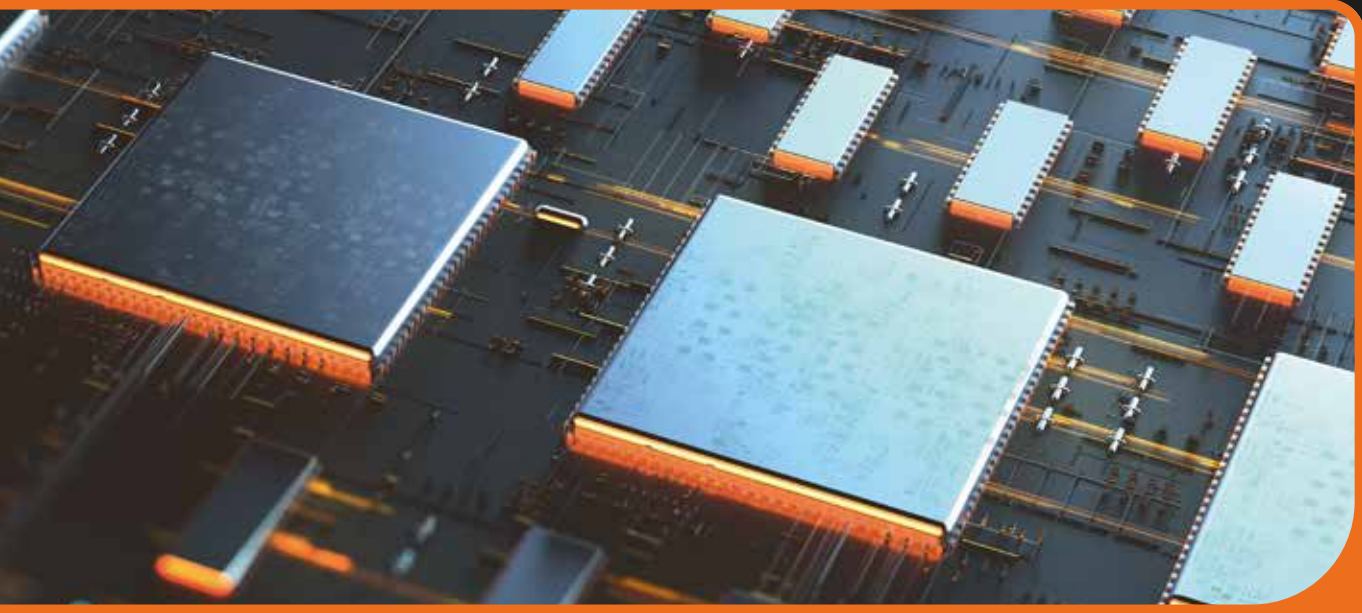
International
Comparative
Legal Guides



Practical cross-border insights into cybersecurity

Cybersecurity 2022

Fifth Edition

Contributing Editor:
Nigel Parker
Allen & Overy LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Switzerland


Dr. Oliver M. Brupbacher


Dr. Nicolas Mosimann


Dr. Claudia Götz Staehelin


Marlen Schultze

Kellerhals Carrard

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)

According to art. 143bis Swiss Criminal Code (SCC), hacking may constitute a criminal offence: any person who obtains unauthorised access, by means of data transmission equipment, to a data-processing system that has been specially secured to prevent such access, may be prosecuted upon complaint and be liable for a custodial sentence not exceeding three years or a monetary penalty. Art. 143bis SCC was revised to reflect Switzerland's implementation of the Budapest Convention on Cybercrime.

Unauthorised access to another person's password-protected email account constitutes hacking and is punishable under art. 143bis SCC (BGer 6B_615/2014 and 6B_456/2007; *cf.* also BGE 130 III 28). According to a ruling by the Swiss Federal Supreme Court (FSC), it is irrelevant in the application of art. 143bis SCC how the offender came into possession of the password (BGE 145 IV 185).

Data theft is covered by art. 143 SCC: any person who for their own or for another's unlawful gain obtains data for themselves or another, which is stored or transmitted electronically or in some similar manner and which is not intended for them and has been specially secured to prevent their access, is liable for a custodial sentence not exceeding five years or a monetary penalty.

In 2020, there were 27 convictions for crimes under art. 143bis SCC and 10 convictions for crimes under art. 143 SCC in Switzerland.

Denial-of-service attacks

Denial-of-service attacks may constitute damage to data (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, may be prosecuted upon complaint, and be liable for a custodial sentence not exceeding three years or a monetary penalty. There is no requirement that the process is irreversible; even the temporary denial of access is punishable. A custodial sentence of a minimum of one to five years may be imposed on an offender who has caused major damage. Other than hacking, this offence is prosecuted *ex officio*.

In 2020, there were 13 convictions for crimes under art. 144bis SCC.

Depending on the specific *modus operandi* of the attack, further criminal provisions may apply, including extortion (art. 156 SCC), misuse of a telecommunications installation (art. 179^{septies} SCC) or coercion (art. 181 SCC).

Phishing

Depending on the circumstances, phishing may be covered by multiple criminal offences under the SCC, in particular:

- Unauthorised obtainment of data (art. 143 para. 1, custodial sentence not exceeding five years or a monetary penalty).
- Unauthorised access to a data-processing system (art. 143bis para. 1, prosecution upon complaint, custodial sentence not exceeding three years or a monetary penalty).
- Obtainment of personal data without authorisation (art. 179^{novies}, prosecution upon complaint, custodial sentence not exceeding three years or a monetary penalty).
- Forgery of a document (art. 251, custodial sentence not exceeding five years or a monetary penalty).
- Computer fraud (art. 147, custodial sentence not exceeding five years or a monetary penalty; if offenders act for commercial gain, they are liable for a custodial sentence not exceeding 10 years or a monetary penalty of a minimum of 90 daily penalty units).
- Fraud (art. 146, custodial sentence not exceeding five years or a monetary penalty; if offenders act for commercial gain, they are liable for a custodial sentence not exceeding 10 years or a monetary penalty of a minimum of 90 daily penalty units; for the interplay with art. 147 *cf.* BGE 129 IV 22, at 4.2).

The fraudulent use of a trademark or a copyright-protected work may be prosecuted under art. 62 Trade Mark Protection Act or art. 67 Copyright Act, each of which provides for a custodial sentence not exceeding one year or a monetary penalty.

2019 saw the first prosecution and conviction for "voice phishing" (Federal Criminal Court (FCC) SK.2019.9). One hundred and twenty-nine cyber-/phishing investigations by the Office of the Attorney General of Switzerland were pending at the end of 2020.

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

Apart from the application of the specific criminal provisions applicable to denial-of-service and phishing attacks (*cf.* above), the infection of IT systems with malware may be prosecuted under art. 143bis SCC, which penalises hacking, and art. 144bis para. 1 SCC, which covers damage to data.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

According to the so-called "virus offence" (art. 144bis para. 2 SCC), any person who without authorisation manufactures,

imports, markets, advertises, offers or otherwise makes programs accessible, that they know or must assume will be used to cause damage to data (art. 144bis para. 1 SCC; *cf.* "Denial-of-service attacks" above), or provides instructions on the manufacture of such programs, is liable for a custodial sentence not exceeding three years or a monetary penalty. If the offender acts for commercial gain, a custodial sentence of a minimum of one to five years may be imposed. The FSC held that this provision also applies where the instructions have not been created by the offender, and even if they are incomplete, so long as they contain specific and relevant information for the manufacture of programs used to cause damage to data (BGE 129 IV 230).

Any person who markets or makes accessible passwords, programs or other data that they know or must assume are intended to be used to commit a hacking offence (art. 143bis para. 1 SCC; *cf.* "Hacking" above), is liable for a custodial sentence not exceeding three years or a monetary penalty (art. 143bis para. 2 SCC).

Possession or use of hardware, software or other tools used to commit cybercrime

The mere possession of such tools is not illegal.

Identity theft or identity fraud (e.g. in connection with access devices)

While not explicitly regulated, identity theft can be punishable under arts 143bis, 143 SCC (unauthorised access to a data-processing system and unauthorised obtainment of data; *cf.* "Hacking" above), arts 146, 147 SCC (fraud or computer fraud), arts 173–178 SCC (offences against personal honour), or art. 179^{novies} SCC (obtainment of personal data without authorisation).

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Data theft is covered by art. 143 SCC (*cf.* "Hacking" above).

Further, the betrayal of a manufacturing or trade secret amounts to a criminal offence if the offender is under a statutory or contractual duty of confidentiality (art. 162 SCC). This offence may be prosecuted upon complaint and is punishable with a custodial sentence not exceeding three years or a monetary penalty.

Depending on the circumstances, political, industrial or military espionage (arts 272–274 SCC) may also apply. These offences are generally punishable with a custodial sentence not exceeding three years, a monetary penalty or, in serious cases, a custodial sentence of a minimum of one year.

A wilful breach of a professional duty of confidentiality (e.g. banking secrecy, medical secrecy or attorney-client privilege) concerning sensitive personal data collected in the exercise of the profession is punishable, upon complaint, with a monetary penalty (art. 35 Federal Act on Data Protection (FADP)).

Deliberate and unlawful copyright infringements are covered by arts 67 *et seqq.* Copyright Act and are punishable with a custodial sentence not exceeding one year 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)

Unsolicited penetration testing may qualify as hacking and be sanctioned under art. 143bis SCC (*cf.* "Hacking" above), given that this offence does not require an intent of unjust enrichment.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Beyond the above, notable other criminal offences, both general and sector-specific, include the following:

- Criminal mismanagement (art. 158 SCC): a custodial sentence not exceeding three years or a monetary penalty; or a custodial sentence of one to five years if the offender acts to secure an unlawful financial gain for himself or another.
- Participation in a criminal organisation (art. 260ter SCC): a custodial sentence not exceeding five years or a monetary penalty (*cf.* rulings on "cyber jihad/cyber terrorism" by the FCC (SK.2013.39) and the FSC (BGer 6B_645/2007)).
- Money laundering (art. 305bis SCC), which is of particular importance in connection with denial-of-service and ransomware attacks (*cf.* above): a custodial sentence not exceeding three years or a monetary penalty, in serious cases not exceeding five years or a monetary penalty whereby a custodial sentence is to be combined with a monetary penalty.
- Breach of official, postal or telecommunications secrecy and of professional confidentiality (arts 320 *et seqq.* SCC): generally, a custodial sentence not exceeding three years or a monetary penalty; further punishable breaches of confidentiality are covered in particular by art. 47 Banking Act, art. 147 Financial Market Infrastructure Act (FinMIA), and arts 43, 53 Telecommunications Act (TCA).
- Disruption of public services, in particular of the railway, postal, telegraphic or telephone services, or of a public utility or installation that provides water, light, power or heat (art. 239 SCC): a custodial sentence not exceeding three years or a monetary penalty.
- Falsification or suppression of information (art. 49 TCA): a custodial sentence not exceeding three years or a monetary penalty.
- Misuse of information (art. 50 TCA): a custodial sentence not exceeding one year or a monetary penalty.
- Unsolicited distribution of spam messages (art. 3 para. 1 lit. o, art. 23 Unfair Competition Act): a custodial sentence of up to three years or a monetary penalty.

Because IT security is regulated in Switzerland with respect to specific objects (data, systems and products) and industries, further criminal offences may apply, depending on the circumstances.

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

Generally, the above-mentioned offences have extraterritorial application only if they are also liable for prosecution at the place of commission (or the place of commission is not subject to criminal law jurisdiction), if the offender is located in Switzerland, and if he/she is not extradited (arts 6, 7 SCC).

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Sentencing under Swiss law is determined by multiple factors pertaining to the offender. Mitigating factors include: acting with honourable motives, under duress or in serious distress; excusable emotional strain; psychological stress; serious provocation; a show of genuine remorse, in particular if the offender has made reparations; or the time elapsed since the crime where the offender has exercised good behaviour (art. 48 SCC). Withdrawal from the act or active repentance are further potential mitigating factors (art. 23 SCC).

The competent authority shall refrain from prosecuting the offender, bringing him to court or punishing him if the level of culpability and the consequences of the offence are minor (art. 52 SCC).

Notably, "hacking" according to art. 143bis SCC does not require an intent of harm or unjust enrichment.

2 Cybersecurity Laws

2.1 *Applicable Law*: 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, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Cybersecurity Incidents may trigger the application of many different statutes. Rather than in a comprehensive manner, Switzerland regulates cybersecurity with respect to specific objects (data, systems and products) and specific industries. Moreover, minimum cybersecurity measures are rarely defined by law, but are left to self-regulation. There is hardly any case law to clarify the standards, either.

The 2018–2022 National Strategy for the Protection of Switzerland against Cyber Risks (NCS II) has acknowledged the need for greater standardisation and regulation across various objects and sectors. According to the Federal Council's September 2021 interim report, implementation is proceeding according to plan.

Among the general laws applicable in the cybersecurity field are the following:

- Civil Code.
- Code of Obligations (CO).
- SCC.
- Council of Europe Budapest Convention on Cybercrime of November 23, 2001 (ETS No. 185; in force in Switzerland since January 1, 2012).
- Employment Act.
- Unfair Competition Act.
- Copyright Act.
- Trade Mark Protection Act.

Among the object-specific or sector-specific laws are the following:

- FADP (revised Act approved by Parliament on September 25, 2020) and related Ordinance (the total revision of the Ordinance has been in the consultation process since June 23, 2021; both acts are expected to enter into force in the second half of 2022), as well as cantonal data protection laws.
- Revised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108; not yet ratified and in force but approved by Parliament on June 19, 2020 – the referendum deadline expired on October 8, 2020 and ratification is subject to the entry into force of the new FADP).
- Product Safety Act.
- Product Liability Act.
- Banking Act and related Ordinance.
- FinMIA.
- Financial Market Supervision Act (FINMASA).
- Revised Therapeutic Products Act (entered into force on May 26, 2021) and related Ordinances.
- Electronic Health Records Act and related Ordinance.
- Revised Medical Devices Ordinance (MedDO) (main provisions entered into force on May 26, 2021).
- TCA and related Ordinance.
- Embargo Act.
- Revised Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods (entered into force on January 1, 2021) and related Ordinance.
- Ordinance on the Export and Brokerage of Goods for Internet and Mobile Communication Surveillance.
- Intelligence Service Act.
- Ordinance on Protection against Cyber Risks in the Federal Administration.

In the globalised universe of cybersecurity, laws often have an extraterritorial effect. Foreign laws, such as the EU General Data Protection Regulation (*cf.* art. 3), may therefore have to be taken into account as well when assessing Incidents in Switzerland.

Provisions on cybersecurity may also include guidelines and standards. While generally non-binding, they may be taken into account when interpreting statutory provisions. They may also be declared binding by sector-specific associations or by reference in contracts. For example, the National Cyber Security Centre (NCSC) maintains an "Information security checklist for SMEs". The Federal Office for National Economic Supply (FONES) issued "Minimum standards for improving ICT resilience" for operators of critical infrastructures that may be adopted by interested private parties as well. Non-governmental initiatives include the Swiss Code of Best Practice for Corporate Governance and the International Organisation for Standardisation's ISO/IEC 27000 family of standards focusing on security of digital information, as well as its standard ISO/IEC 30141:2018 regarding IoT Reference Architecture.

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?

Currently, there are no generally applicable mandatory cybersecurity requirements for critical or essential infrastructure and services. The regulation of cybersecurity for such infrastructure and services is fragmented and inconsistent, and it often lacks a precise definition of the required security measures (*cf.* question 4.2 below).

However, the need for further standardisation and regulation has been recognised in the NCS II, as adopted by the Federal Council on April 18, 2018. One of its focus areas remains the improvement of ICT resilience of critical infrastructures.

Accordingly, the 2018–2022 Critical Infrastructure Protection Strategy (CIP II) defines the overriding goals and principles of action for all parties involved, and identifies 17 measures to improve the country's resilience, *i.e.* its resistance, versatility and regeneration capacity, with regard to its critical infrastructures. The CIP II lists the following nine critical infrastructures for Switzerland: financial and insurance services; healthcare; telecommunications; and public administration (set out in greater detail in question 4.2 below), as well as: public transport; energy; food supply; waste management; and public security.

The draft of a new Federal Information Security Act was accepted by Parliament in December 2020 and is expected to enter into force by the end of 2021. It contains minimum requirements for the protection of information and IT infrastructure hosted by the federal authorities. The Ordinance on Protection against Cyber Risks in the Federal Administration entered into force on July 1, 2020. It regulates the organisation of the Federal Administration's protection against cyber risks as well as the tasks and responsibilities of the various offices in the cybersecurity domain, in particular the NCSC (*cf.* question 8.1 below).

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

Other than for critical or essential infrastructures and services (*cf.* question 2.2 above) and sector-specific regulations (*cf.* question 4.2 below), there are currently no specific legal requirements with respect to the measures listed above.

Their implementation may instead be driven by general legal requirements that, depending on the circumstances, may include the implementation of some or all of the above measures. They include, notably, the overall responsibility for the due management of a company and individual professional confidentiality obligations as well as data protection requirements. Guidelines and standards may also include provisions on cybersecurity. While generally non-binding, they may be taken into account when interpreting statutory provisions. They may also be declared binding by sector-specific associations or by reference in contracts (*cf.* questions 5.1 and 5.2 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.

Currently, Switzerland knows no general obligation to report Incidents or potential Incidents to the authorities. However, the introduction of such an obligation is contemplated as part of the federal government's NCS II. With the exception of in cases involving serious security incidents in critical infrastructures, Incident reporting is currently encouraged on a voluntary basis, typically via the recently established NCSC, which incorporates the former Reporting and Analysis Centre for Information Assurance (MELANI) and serves as a new national contact point (*cf.* question 8.1 below). Reports can be made through a message on the NCSC's website and can also be submitted anonymously. The NCSC's statistics for the second half of 2020 show a continued high activity in all areas of cybersecurity risk.

Illegal activity on the internet can also be reported to the Cybercrime Coordination Unit Switzerland (CYCO), which may forward the matter to the competent domestic and foreign law enforcement authorities.

Sector-specific regulations for critical infrastructures regularly require the reporting of serious security incidents without delay. The scope of serious security incidents generally extends beyond, but may include, Incidents. More precise criteria may be specified in non-binding guidelines that explain the regulator's intended enforcement practice and are regularly accepted and complied with by the industry. Among the most prominent cybersecurity reporting obligations for critical infrastructures are those for financial and insurance services (*cf.* art. 29 para. 2 FINMASA; Financial Market Supervisory Authority (FINMA) Guidance 05/2020; FINMA Circular 08/25), healthcare (*cf.* art. 12 para. 3 Electronic Health Records Ordinance; art. 66 revised MedDO), as well as telecommunications (art. 96 para. 2 Ordinance on Telecommunication Services) (*cf.* question 4.2 below).

In December 2020, the Federal Council instructed the Federal Department of Finance to prepare a consulting draft concerning the introduction of a reporting obligation for operators of critical infrastructure in the event of cyber-attacks and the discovery of security vulnerabilities. The Federal Council has set corresponding benchmarks for the design of the bill: a central reporting office is to be designated at the legislative level and defined uniformly for all sectors. The criteria for who is to report which incidents and within what timeframe are also to be defined. The concrete provisions on the structure of the reporting obligation are to be defined in corresponding decrees, adapted to the sector-specific circumstances. The reporting obligation should be coordinated with existing sectoral and data protection reporting obligations.

A specific reporting obligation for Incidents relating to personal data will be introduced by the revised FADP. Data controllers will have to notify the Federal Data Protection and Information Commissioner (FDPIC) as soon as possible of data breaches that are likely to result in a high risk for the personality or the fundamental rights of data subjects. Correspondingly, data processors will have to inform the data controller as soon as possible of any data breach. A notification of the FDPIC must at least refer to the nature of the data breach, its consequences, and any measures taken or planned. In any subsequent criminal proceeding, the notification may only be used against the notifying company or person with their consent (arts 24 paras 1–3 and 6 revised FADP; *cf.* art. 7 revised Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).

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.

There is currently no specific requirement under the FADP to notify data subjects of an Incident. Depending on the seriousness of the data breach, however, such a requirement may arise under the general principle of data processing in good faith (art. 4 para. 2).

The revised FADP will explicitly require data controllers to inform affected data subjects of a data breach if it is necessary for their protection or if the FDPIC – after having been informed of the data breach (*cf.* question 2.4 above) – so orders (art. 24 paras 1, 4 revised FADP). Exceptions will apply in particular in cases of overriding public or private third-party interests or where reporting would be impossible or require a disproportionate effort (art. 24 para. 5 lit. a, b revised FADP).

Further obligations to report Incidents or potential Incidents to affected individuals or third parties may derive from the generally required lawfulness of all data processing (art. 4 para. 1 FADP; art. 6 para. 1 revised FADP), as well as from specific contractual obligations.

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

Where applicable, the general Incident reporting is overseen by the NCSC, CYCO, FDPIC, and the cantonal Data Protection Commissioners.

Sector-specific reporting is overseen by the respective regulatory authorities, most notably by the FINMA for financial and insurance services, by the Federal Office of Public Health (FOPH) for healthcare, and by the Federal Office of Communications (OFCOM) for telecommunications (*cf.* question 4.2 below).

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

For lack of a general reporting obligation for Incidents, there are currently no generally applicable penalties for non-compliance with reporting obligations.

Sector-specific sanctions may apply, such as in case of financial and insurance services, healthcare and telecommunications (*cf.* question 4.2 below). Under the revised FADP, object-specific sanctions will apply for violations of the minimum security requirements for personal data and for non-compliance with orders by the FDPIC (arts 8, 24, 61 lit. c, and 63).

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

Cyber risks are a key part of the prudential supervision by the FINMA, which has stepped up its efforts in the area. These risks are monitored directly, for example through focused on-site audits by the FINMA, and monitored by audit firms as part of the regulatory audit process. In 2020, the FINMA strengthened its cyber risk resources and introduced a new cyber supervisory approach to monitor all supervised entities. The concept provides for supervision in the following areas: threat analysis; ongoing supervision; and incident response or crisis management.

In addition, larger institutions are regularly reminded of the need to take appropriate precautions against cyber risks during self-assessments. According to the FINMA's Annual Report 2019, self-assessments in the second half of 2018 focused on the ability of the participating institutions to identify cyber threats arising from institution-specific vulnerabilities, perform a commensurate risk assessment and define countermeasures (threat intelligence). The outcome of the self-assessments was that most of the participating institutions had made adequate provision for those risks. The FINMA's on-site supervisory reviews in 2020 focused, *inter alia*, on cyber risks and cybersecurity, including in the investment banking, asset management and insurance sectors.

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)

There is no law specifically allowing or prohibiting the use of beacons. However, companies that intend to use beacons for such purposes should analyse, in each case, whether their use is in compliance with Applicable Laws, including the SCC, the Unfair Competition Act and the FADP.

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 specifically allowing or prohibiting the use of honeypots. Companies should, however, keep the same regulations in mind as with beacons.

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)

There is no law specifically allowing or prohibiting the use of sinkholes. The same considerations apply as with 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?

Organisations may monitor the electronic communication of their employees, provided that they comply with the provisions pertaining to the processing of personal data in the CO (art. 328b) and the FADP. Consequently, such monitoring must, in particular, be: carried out lawfully; in good faith; proportionate (i.e. suitable, necessary and affecting the data subject's privacy in the mildest possible way); and known to the data subjects.

Depending on the circumstances, the monitoring of employee data can be justified on the basis of the employment contract, industry-specific laws applicable to the employer (e.g. in case of banks) or the overriding interest of the employer to prevent or detect cyber-attacks. Relying on employee consent as justification for the processing, however, entails certain risks due to the usually limited ability of employees to refuse consent. Under the principle of transparency, employers are recommended to issue a monitoring regulation setting out the specifics of the surveillance measures.

Ordinance 3 to the Employment Act prohibits surveillance and monitoring systems that monitor the behaviour of employees (art. 26). Employers must ensure that the health of employees is not affected by the monitoring. However, a non-personal – anonymous or pseudonymous – evaluation of employee data is usually sufficient in order to prevent cyber-attacks, and it is, in principle, lawful under this provision, even if conducted systematically. In certain individual cases (e.g. after a cyber-attack), an individualised analysis of employee data may also be permissible.

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?

The Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods, as well as the respective Ordinance and Annexes, provide for certain import and export restrictions for dual-use goods, including technology and software. Annex 2, part 2, 4A005, 4D004 and 4E001.c set forth export restrictions for technology for the development of intrusion software, whereby certain exceptions exist with regard to vulnerability disclosures and reactions to cyber Incidents. Moreover, according to Annex 2, part 2, 5A002, systems for

information security and their components, including cryptographic technology for the confidentiality of data with a specific security algorithm, are subject to export restrictions.

Exceptions are available, such as for technology that is available to consumers, cryptographic technology for digital signatures, symmetric algorithms below 56 bit-encryption and many more. Furthermore, export restrictions may apply to equipment, and its components, for the interception and interruption of mobile communication and surveillance equipment (Annex 2, part II, 5A001.f), and to systems and equipment, and its components, for the surveillance of IP communication networks (Annex 2, part II, 5A001.j).

The Ordinance on the Export and Brokerage of Goods for Internet and Mobile Communication Surveillance must also be taken into consideration.

4 Specific Sectors

4.1 Does 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.

The Applicable Laws and market practice vary across the different business sectors in Switzerland. The NCS II has acknowledged the need for greater standardisation and regulation across the different sectors (*cf.* question 2.1 above).

4.2 Excluding 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 or telecommunications)?

Financial and insurance services

The focus of cybersecurity regulations in Switzerland has traditionally been on its financial and insurance services sector.

Financial market infrastructures, as defined in art. 2 lit. a FinMIA (e.g. stock exchanges, multilateral trading facilities, payment systems), are obliged to operate IT systems that: ensure the fulfilment of the duties imposed by the FinMIA; are appropriate for the activities conducted; provide for effective emergency procedures; and ensure the continuity of the business activity (art. 14 FinMIA). Special IT systems requirements apply to financial market infrastructures with systemic importance in order to protect against the risks to the stability of the financial system (art. 23 FinMIA).

According to the FINMA, cyber risks are among the most significant operational risks for banks and insurance companies. Accordingly, they are required to implement appropriate risk management measures to tackle operational risks, including cyber risks, and must safeguard their infrastructure against various types of attacks (art. 3f para. 2 Banking Act; art. 12 Ordinance on Banks; and the non-legally binding FINMA Circulars 2008/21 "Operational Risks – Banks" and 2017/2 "Corporate governance – insurers").

Supervised persons and entities must immediately report Incidents that are of substantial importance to the supervision to the FINMA (art. 29 para. 2 FINMASA; FINMA Guidance 05/2020; FINMA Circular 08/25). Violations of the reporting obligations may face sanctions, including: a custodial sentence of up to three years or a monetary penalty for the wilful provision of false information or the omission of reporting to the FINMA; a fine of up to CHF 250,000 in case of negligence (arts 45 *et seq.* FINMASA); and a revocation of the licence, a withdrawal of the recognition or a cancellation of the registration in case of serious infringements (art. 37 FINMASA).

Healthcare

Cybersecurity in the healthcare sector has recently received increased attention in Switzerland, in particular in view of the cybersecurity risks relating to the electronic patient record and medical devices connected to the internet.

The first electronic patient records were certified at the end of 2020. Certification requires a risk-based data security and data protection system, the technical and organisational specifications of which are defined by the FOPH. Relevant security Incidents have to be notified to the FOPH. The violation of these requirements may lead to a suspension or removal of the certification (art. 12 para. 1 lit. b Electronic Health Records Act; art. 12, 38 para. 1 Electronic Health Records Ordinance).

In line with the developments in the EU, in particular the Medical Devices Regulation 2017/745 of April 5, 2017 (MDR), Switzerland has revised its MedDO, the main provisions of which entered into force on May 26, 2021. Accordingly, medical devices have to fulfil the general safety and performance requirements in Annex I of the MDR, both with respect to hardware and software (art. 6 paras 1, 2 MedDO). Manufacturers of medical devices may have to notify severe Incidents as well as their corrective measures (art. 66 MedDO).

Telecommunications

Another emphasis of cybersecurity regulations lies on the telecommunications sector.

The OFCOM issued the non-binding "Directives on the security and availability of telecommunication infrastructures and services" (based on art. 96 para. 2 Ordinance on Telecommunications Services (OTS)). They specify security requirements and define minimum security levels that each telecommunication services provider should maintain in order to contribute to the reliability and availability of the national telecommunications network. With the revision of the TCA (entered into force January 1, 2021), a specific obligation to protect against cyber-attacks was introduced (art. 48a revised TCA).

Telecommunications service providers are required to immediately inform the OFCOM of faults in the operation of their networks that affect a relevant number of customers (art. 96 para. 1 OTS). Such disturbances may also result from cyber-attacks. Failure to report may result in a fine not exceeding CHF 5,000 (art. 53 TCA).

Federal Administration

The draft of a new Federal Information Security Act was accepted by Parliament in December 2020 and is expected to come into force by the end of 2021. It contains minimum requirements for the protection of information and IT infrastructure hosted by the federal authorities.

The Ordinance on Protection against Cyber Risks in the Federal Administration entered into force on July 1, 2020. It regulates the organisation of the Federal Administration`s protection against cyber risks as well as the tasks and responsibilities of the various offices in the cybersecurity domain, in particular the NCSC (*cf.* question 8.1 below).

Other important sectors

Further sector-specific regulations apply, including for critical infrastructures. The NCS II and CIP II aim to implement measures to improve cybersecurity across various sectors on the basis of periodically updated risk and vulnerability analyses (*cf.* questions 2.1 and 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?

As a general principle, the primary responsibility for cybersecurity lies with the organisation (*cf.* question 5.2 below) rather than with the individuals entrusted with the task.

The board of directors, managing directors and executive officers of companies limited by shares, as well as the managing directors of limited liability companies, have a duty of loyalty and care and in particular a non-transferable and inalienable responsibility for the overall management of the company, the company's organisation, including accounting and financial controls, as well as the overall supervision of the persons entrusted with managing the company (arts 716a, 717, 810, 812 CO). Hence, the ultimate responsibility for the cybersecurity strategy of such companies, including the adoption of an appropriate organisation and of the necessary directives, processes and controls, lies with the respective management. In light of the increasing importance of cybersecurity, management must either have the requisite know-how itself or obtain relevant advice and cannot simply delegate the task to the IT department. Accordingly, if such companies suffer loss because of an Incident that results from an intentional or negligent breach of their duties, management may become personally liable both to the company and to the individual shareholders and creditors (arts 754, 827 CO).

The current FADP does not provide for sanctions for breaches of data security (art. 7). As of the expected entry into force of the revised FADP in 2022, however, the company's management or – if data security has been internally delegated – its data protection officer, IT manager or compliance officer may face fines of up to CHF 250,000 for intentional violations of the statutory minimum data security requirements (art. 8 para. 3, art. 61 lit. c. revised FADP).

Criminal sanctions against individuals may also apply under various other, including sector-specific, laws, notably for intentional breaches of professional confidentiality (e.g. art. 35 FADP/art. 62 revised FADP; arts 320 *et seqq.* SCC), but also at times for negligence (e.g. art. 47 Banking Act; arts 43, 53 TCA; art. 16 Product Safety Act).

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?

Other than for critical or essential infrastructures and services (*cf.* question 2.2 above) and in sector-specific regulations (*cf.* question 4.2 above), there are currently no specific legal requirements with respect to the IT security measures listed above. Their implementation may instead be driven by general legal requirements that, depending on the circumstances, may include the implementation of some or all of the above IT security measures. They include, notably, the overall responsibility for the due management of a company and individual professional confidentiality obligations (*cf.* question 5.1 above) as well as data protection requirements.

Privacy by design requires that the confidentiality, availability, and integrity of personal data must be protected through adequate technical and organisational measures, taking into account the purpose, nature, and extent of the data processing, the possible risks and the current state of the art. The measures must be reviewed periodically. More specific requirements apply for the automated processing of personal data (arts 7 FADP and 8 *et seq.* Ordinance to the FADP; arts 7, 8 revised FADP). The revised FADP will introduce additional obligations to maintain an inventory of processing activities and to conduct privacy impact assessments (arts 12, 22).

Beyond the applicable regulations, guidelines and standards may also include provisions on cybersecurity (*cf.* question 2.1 above). While generally non-binding, they may be declared binding by sector-specific associations or by reference in contracts. They may also be taken into account when interpreting statutory provisions. For example, manufacturers of data-processing systems or programs, as well as private persons or federal bodies that process personal data, may obtain a data protection certification (art. 11 FADP). The applicable standard in such cases is ISO/IEC 27001:2013.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There is currently no specific requirement under the FADP to notify the public of an Incident. Depending on the seriousness and on the number of affected data subjects, however, the general principles of lawful and good-faith data processing (art. 4 paras 1, 2 FADP; *cf.* also art. 6 paras 1, 2 revised FADP) may require an Incident to be reported publicly (*cf.* questions 2.4 and 2.5 above). This option is explicitly foreseen in the revised FADP (art. 24 para. 5 lit. c).

If Incidents or cybersecurity risks lead to the expectation of a future cash outflow, a company may be required to book the probably required provisions and charge them to the profit and loss account (*cf.* art. 960e CO or other applicable financial reporting standards).

Companies listed on the SIX Swiss Exchange are subject to specific periodic disclosure requirements (art. 49 *et seq.* Listing Rules (LR)). They may also have to consider whether an Incident amounts to a qualified reportable event and, hence, triggers *ad hoc* publicity obligations (art. 53 LR; Directive on Ad Hoc Publicity). Whether an Incident represents a qualified reportable event has to be assessed on a case-by-case basis, considering whether it has a substantial impact on the development of a company's share price and therefore has the potential to influence average investors in their investment decision.

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.

Liability is a key consideration in cybersecurity. While legally possible, civil action against cybercriminals will regularly prove unfeasible. In practice, the focus is therefore on secondary liability: entities affected by an Incident may turn to the provider of a defective product or service; and third parties suffering damage from the Incident may look to the affected organisation for having failed to comply with appropriate data security standards.

In case of a contractual relationship that contains a respective IT security representation, the third party (client, supplier,

etc.) can bring a contractual liability claim against the organisation affected by the Incident, provided it can demonstrate a breach of contract, damage, causation as well as fault (arts 97 *et seqq.* CO). The latter is generally presumed, which is why it is for the defendant to prove that it was not at fault with respect to the Incident. Special contractual liability provisions may provide for strict liability, such as in case of direct losses caused to a buyer (art. 208 para. 2 CO).

If there is no IT security representation, the defendant's fault will be assessed against a standard of due care and the related threshold question of what level of cybersecurity is reasonable and appropriate to avert damage from a third party, taking into account the level of risk, applicable industry standards, and the state of technology.

General commercial terms often contain liability limitations for third-party actions and consequential damages. It is questionable whether such general terms would be upheld in the event of an Incident, and any advance exclusion of liability for gross negligence would in any case be void (art. 100 para. 1 CO). Difficult questions may also arise where a multitude of parties contribute, albeit unintentionally, to an Incident.

For liability based on tort, or other civil wrongs independent of contract (*cf.* question 6.3 below).

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.

There is no published case law in relation to Incidents for a failure to comply with appropriate data security standards or the delivery of defective security products or services.

Since Swiss law currently remains unfriendly to mass claim proceedings, data subjects affected by a security breach will, in most cases, encounter difficulties in asserting financial damages in an amount that merits a claim.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

In the absence of a contractual relationship (*cf.* question 6.1 above), entities may incur liability in tort, or *another* civil wrong independent of contract, for the harm that an Incident causes to third parties, irrespective of contractual disclaimers or limitations of liability.

General tort law provides relief for damages caused by an illicit act, whether wilfully or negligently (such fault not being presumed; arts 41 *et seqq.* CO). An illicit act exists in case of a breach of an absolute right of the victim (personality, intellectual property or similar rights) or a financial damage resulting from the breach of a specific legal provision that is designed to protect against such damage, which must be determined on a case-by-case basis. Disgorgement of profits arising from a cyber-attack may be sought based on unjust enrichment or on agency without authorisation (arts 62 *et seqq.*, 423 CO).

In the software and IoT context (e.g. hacked medical devices, cars, etc.), product liability rules may be of particular relevance: if a defective product, which does not provide the safety that would reasonably be expected, leads to an Incident, the manufacturer, importer or supplier is, in principle, strictly liable for personal injuries and damage to privately used property caused by the product (arts 1, 4 Product Liability Act).

If a company limited by shares or a limited liability company suffers loss because of a severe data breach that results from a lack of appropriate internal cybersecurity controls and procedures, the respective board members, managing directors and executive officers may become personally liable to both the company and the individual shareholders and creditors for any loss or damage arising from an intentional or negligent breach of their duties (arts 754, 827 CO; *cf.* question 5.1 above).

To the extent an Incident due to insufficient data protection or data security leads to a violation of personality rights, such as in case of data theft or illegal data processing, affected persons may bring an action seeking, e.g. damages, moral compensation, disgorgement of profits, injunctions and notification to third parties or publication (art. 15 para. 1 FADP/art. 32 para. 2 revised FADP; arts 28 *et seqq.* Civil Code; arts 41 *et seqq.*, 49, 423 CO).

7 Insurance

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

Organisations in Switzerland are permitted to take out insurance against Incidents, and insurers have offered cyber products for a number of years already. The respective offerings often close a coverage gap as many property and liability insurance policies exclude cyber risks.

Cyber insurance solutions are very much customised and can include almost every cyber risk, including denial-of-service and ransomware attacks, costs of internal investigations and crisis management, recovery of stolen, destroyed or damaged data, reputational damage, and the defence against third-party claims. The implementation of a customary and up-to-date cyber risk management and respective protective measures are a necessary condition of admission and coverage under many cyber insurances. Unless contractually excluded, art. 14 para. 2 Insurance Contract Act entitles the insurer to reduce its coverage in case of gross negligence of the insured.

In addition to the high degree of customisation, many key coverage terms have not been analysed by the courts, and cyber risks are complicated and constantly evolving. Accordingly, foreign cases such as *Mondelez International, Inc. v. Zurich American Insurance Co.*, No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct., Oct. 10, 2018) have also been monitored closely in the jurisdiction.

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?

No, there are not.

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. antiterrorism laws) that may be relied upon to investigate an Incident.

Switzerland does not have a central enforcement agency for cybercrimes. Instead, prosecution of the various cybercrimes lies with the competent police departments and public prosecutors' offices on cantonal and federal level. Equally, while reporting duties for serious security events, including Incidents, exist for critical infrastructures such as finance and insurance, healthcare and

telecommunications, there is currently no general and specific duty to notify cybersecurity breaches (*cf.* question 2.4 above).

The NCSC, headed by the Federal Cyber Security Delegate, is Switzerland's cybersecurity competence centre (*cf.* Ordinance on Protection against Cyber-Risks in the Federal Administration of July 1, 2020). Its aim is to enable the Confederation to play a more active role in protecting the country against cyber risks by supporting the general public, businesses and educational institutions as well as public administrations in their protection against cyber risks, by improving the security of the Federal Administration's own infrastructure. The MELANI, together with the national Computer Emergency Response Team (GovCERT), have been integrated into the NCSC as a national contact point and technical expertise hub. Incident reporting to the MELANI is voluntary. Upon receipt of a report, the MELANI will analyse it and provide assessments and recommendations. The MELANI can adopt an active lead role where an Incident jeopardises the proper functioning of the Federal Administration.

The CYCO at the Federal Office of Police (FEDPOL) is Switzerland's central office for anyone who wishes to report illegal activity on the internet. It also actively investigates illegal internet activity. The CYCO does not prosecute the matters itself but, after a first review and data backup, passes them on to the competent domestic and foreign law enforcement authorities.

Switzerland is a member of the Budapest Convention on Cybercrime. Besides committing its member states to increase their national efforts to effectively fight cybercrime, the Convention fosters increased, rapid, and well-functioning international cooperation.

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 are not.

Dr. Oliver M. Brupbacher is a partner at Kellerhals Carrard. He represents clients in litigation and arbitration in commercial matters as well as in investigations. He specialises in healthcare and life sciences, cross-border proceedings and mutual legal assistance, as well as data protection and information governance. He also advises clients on cybersecurity prevention and crisis management. As a former Senior Litigation Counsel, Head of Global Discovery and a global product lawyer at Novartis, Oliver Brupbacher combines deep expertise in his areas of practice with an intimate understanding of the industry and of clients' needs at all organisational levels, in both domestic and international contexts.

Kellerhals Carrard
Henric Petri-Strasse 35, P.O. Box 257
CH-4010 Basel
Switzerland

Tel: +41 58 200 30 00
Fax: +41 58 200 30 11
Email: oliver.brupbacher@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

Dr. Nicolas Mosimann is a partner at Kellerhals Carrard. His practice focuses on M&A, corporate law, technology and intellectual property law and commercial law. He advises both Swiss and international companies and institutions on transactions (e.g. acquisitions, joint ventures, financing rounds, licences and outsourcing) and technology projects (e.g. IoT and blockchain-based platforms), research and cooperation agreements, commercial contracts and data protection (including the EU GDPR). In addition, Nicolas specialises in advising both providers and customers on software and cloud projects. Moreover, as a founding member and co-head of the Startup Desk of Kellerhals Carrard, Nicolas knows the needs of founders and their companies in the seed and growth phases.

Kellerhals Carrard
Henric Petri-Strasse 35, P.O. Box 257
CH-4010 Basel
Switzerland

Tel: +41 58 200 30 00
Fax: +41 58 200 30 11
Email: nicolas.mosimann@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

Dr. Claudia Götz Staehelin, head of the Kellerhals Carrard Investigation practice group, is a litigation and investigation partner and specialises in international dispute resolution, as well as internal investigations across various industries. She advises her clients in compliance, internal investigations, cross-border proceedings, international mutual legal assistance and data privacy (CIPP/E), and supports her clients in dispute resolution crisis management. Claudia is also active as an arbitrator. Claudia combines investigation and dispute resolution expertise with significant business experience. Before joining the firm, Claudia was the head of litigation at Novartis, where she led large multi-jurisdictional disputes and investigations and advised senior management on company litigation risks, as well as on financial and reputational impact.

Kellerhals Carrard
Henric Petri-Strasse 35, P.O. Box 257
CH-4010 Basel
Switzerland

Tel: +41 58 200 30 00
Fax: +41 58 200 30 11
Email: claudia.goetz@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

Marlen Schultze is a member of the Kellerhals Carrard White-Collar Crime practice group at Kellerhals Carrard. She has extensive experience in criminal law and criminal procedural law, with a focus on white-collar crime and the prevention of corruption and money laundering. In addition, she advises clients on compliance and conducts internal investigations.

Kellerhals Carrard
Henric Petri-Strasse 35, P.O. Box 257
CH-4010 Basel
Switzerland

Tel: +41 58 200 30 00
Fax: +41 58 200 30 11
Email: marlen.schultze@kellerhals-carrard.ch
URL: www.kellerhals-carrard.ch

With more than 220 legal professionals (consisting of partners, of counsels, associates, tax advisors and notaries) and more than 400 employees, the firm, which has its origins in 1885, is one of the largest and most traditional law firms in Switzerland, with offices in Basel, Bern, Geneva, Lausanne, Lugano and Zurich, and representative offices in Binningen, Sion, Shanghai and Tokyo.

Kellerhals Carrard advises and represents companies and entrepreneurs from all industries and economic sectors, public authorities, national and international organisations and private individuals before all judicial and administrative bodies nationally and abroad in practically all areas of the law. Our activities are focused on:

- Company and corporate law, external legal department.
- Litigation, arbitration and insolvency law.
- M&A and capital markets law.
- Regulatory financial markets law, financial services, collective investments, leasing, insurance.
- IT/IP, distribution, competition and anti-trust law.
- International sports law.
- Tax.
- Public law.
- Employment and social insurance law.
- Commercial criminal law and international mutual assistance/compliance.
- Family and inheritance law for private customers.
- Notarial office.

Kellerhals Carrard focuses in particular on the areas of financial services, life sciences, IMT (Information, Technology and Media), sport, energy, real estate/construction, as well as on trading and retail.

www.kellerhals-carrard.ch

Kellerhals Carrard

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: glg global legal group