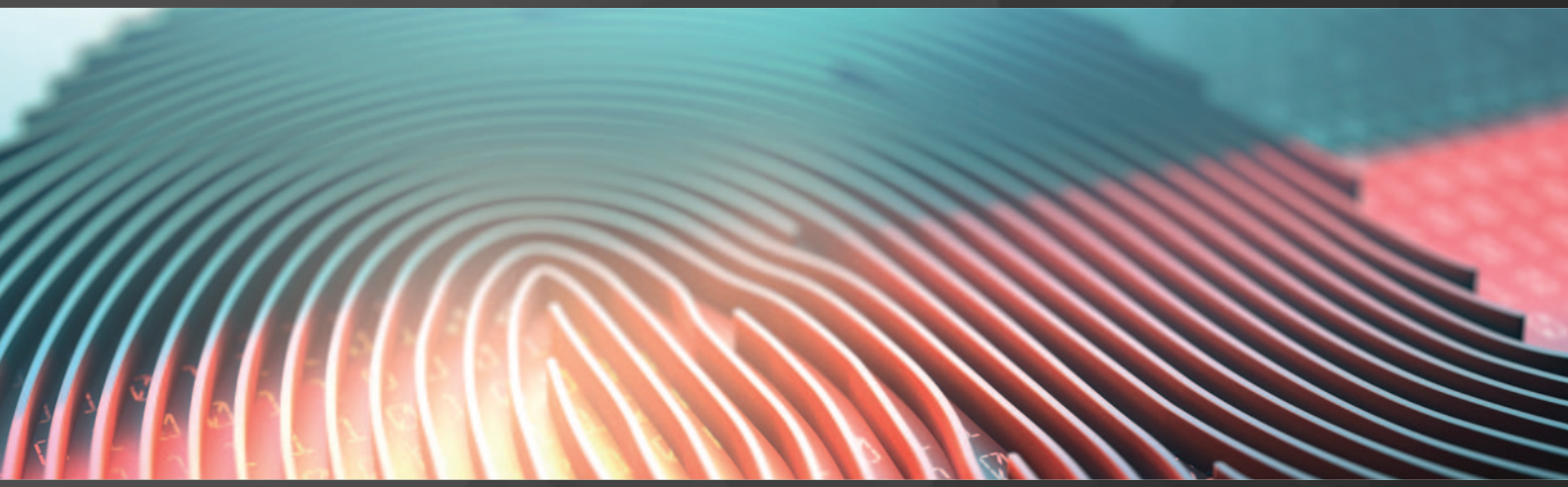
# International Comparative Legal Guides



# Cybersecurity 2020

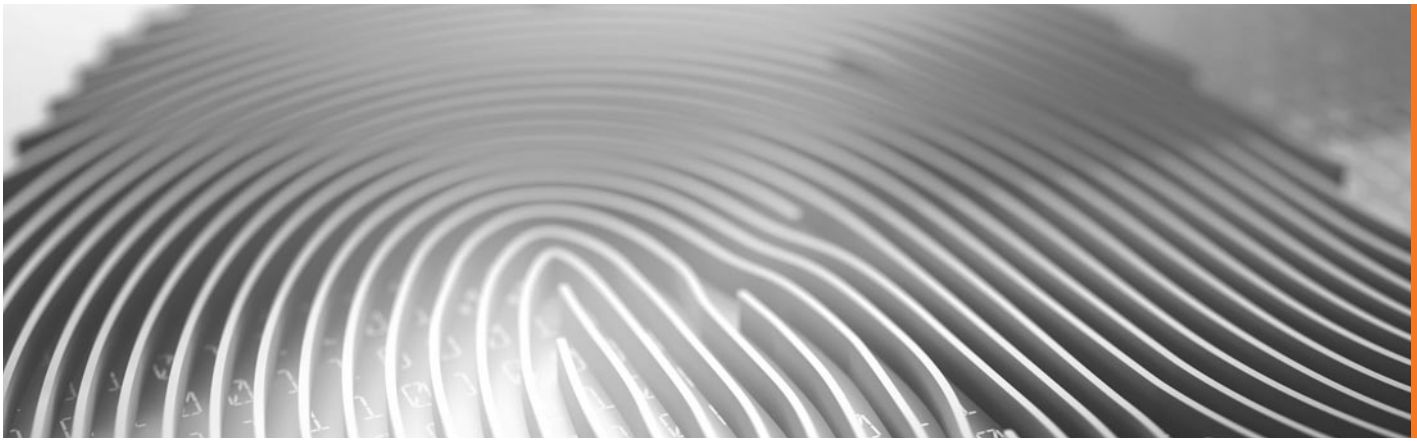
A practical cross-border insight into cybersecurity law

## Third Edition

**Featuring contributions from:**

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Boga & Associates
Christopher & Lee Ong
Cliffe Dekker Hofmeyr
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Faegre Baker Daniels
G+P Law Firm
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L.
Iwata Godo
King & Wood Mallesons
Lee & Ko
Lee and Li, Attorneys-at-Law
LEĜA
Lesniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Ropes & Gray
SAMANIEGO LAW
Shardul Amarchand Mangaldas & Co.
Siqueira Castro – Advogados
Sirius Legal
Stehlin & Associés
Synch

ICLG.com



ISBN 978-1-83918-005-7
ISSN 2515-4206

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
www.iclg.com

Group Publisher
Rory Smith

Associate Publisher
James Strode

Senior Editors
Caroline Oakley
Rachel Williams

Deputy Editor
Hollie Parker

Creative Director
Fraser Allan

Printed by
Stephens & George
Print Group

Cover Image
www.istockphoto.com

# Cybersecurity 2020

## Third Edition

Contributing Editors:
Nigel Parker and Alexandra Rendell
Allen & Overy LLP

Strategic Partners

# Expert Chapters



# Country Q&A Chapters

ICLG.com

# From the Publisher

Dear Reader,

Welcome to the third edition of *The International Comparative Legal Guide to Cybersecurity*, published by Global Legal Group.

This publication, which is also available at www.iclg.com, provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to cybersecurity laws and regulations around the world.

This year, there are three general chapters which provide an overview of key issues affecting cybersecurity, particularly from the perspective of a multi-jurisdictional transaction.

The question and answer chapters, which cover 32 jurisdictions in this edition, provide detailed answers to common questions raised by professionals dealing with cybersecurity laws and regulations.

As always, this publication has been written by leading cybersecurity lawyers and industry specialists, to whom the editors and publishers are extremely grateful for their invaluable contributions.

Global Legal Group would also like to extend special thanks to contributing editors Nigel Parker and Alexandra Rendell of Allen & Overy LLP for their leadership, support and expertise in bringing this project to fruition.

**Rory Smith**
**Group Publisher**
**Global Legal Group**

# Switzerland


Clara-Ann Gordon

Dr. András Gurovits

Niederer Kraft Frey Ltd.


## 1 Criminal Activity

**1.1 Would any of the following activities constitute a criminal 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)**

Hacking can constitute a criminal offence in Switzerland. Pursuant to Article 143*bis* of the Swiss Criminal Code (SCC), 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, is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty. If the hacker for their own or for another's unlawful gain obtains specially secured data which is not intended for them, they are liable, according to Article 143 SCC, to a custodial sentence not exceeding five years or to a monetary penalty.

In its decisions BGer 6B_615/2014 and 6B_456/2007, the Swiss Federal Supreme Court held that unauthorised access to another person's password-protected email account falls under the scope of the "hacking offence". In 2016, several hackers and persons threatening to hack IT systems of banks, universities and private enterprises could have been identified and arrested in Switzerland or abroad with the help of mutual legal assistance from foreign authorities.

**Denial-of-service attacks**

Denial-of-service attacks can constitute a criminal offence in Switzerland. Pursuant to Article 144*bis* SCC, any person who without authorisation alters, deletes or renders unusable data that is stored or transmitted electronically is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty. Moreover, data can also be regarded as rendered unusable if such data still exists but is temporarily inaccessible for authorised users, e.g. due to a denial-of-service attack.

Moreover, depending on the *modus operandi* of the individual case, the following further criminal provisions can be applicable in the context of denial-of-service attacks:

- extortion (Article 156 SCC) – penalty: a custodial sentence not exceeding five years; or a monetary penalty;
- coercion (Article 181 SCC) – penalty: a custodial sentence of up to three years; or a monetary penalty;
- misuse of a telecommunications installation (Article 179*septies* SCC) – penalty: a fine upon complaint; and
- obstructing, disrupting or endangering the operation of a telecommunication service or utility provider (Article 239 SCC) – penalty: a custodial sentence of up to three years; or a monetary penalty.

**Phishing**

Depending on the individual design and purpose of a phishing mail or website, such phishing can constitute the following criminal offences:

- fraudulent use of a trademark or a copyright-protected work (Article 62 of the Swiss Trade Mark Protection Act, Article 67 of the Swiss Copyright Act);
- forgery of a document (Article 251 SCC); or
- computer fraud: unauthorised use of data and the transferring of financial assets through phishing (Article 147 SCC),

each of which is punishable by a custodial sentence not exceeding five years, or by a monetary penalty if committed for commercial gain.

Furthermore, in phishing cases, the criminal offence of money laundering (Article 305*bis* SCC), with a penalty of a custodial sentence not exceeding three years or a monetary penalty, can be part of the accusation (see the decision by the Swiss Federal Criminal Court, BG.2011.43).

The Office of the Attorney General of Switzerland has reported that, from 2012 to 2016, 455 criminal complaints with regard to phishing were filed by banks, authorities and private persons. Many cases were closed without an outcome due to lack of evidence or offenders remaining unidentified. Other cases, especially those involving requests for mutual legal assistance of foreign authorities, are still pending. As per the end of 2018, 173 cases of phishing are still pending.

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

Such infections can be covered by Article 144*bis* SCC, prescribing that whoever alters, deletes or renders unusable data that is stored or transmitted electronically is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty ("virus offence").

Especially in connection with ransomware attacks, the following further criminal provisions can be applicable:

- fraud for commercial gain (Article 146 SCC) – penalty: a custodial sentence not exceeding 10 years; or a monetary penalty of not less than 90 daily penalty units;
- extortion (Article 156 SCC) – penalty: a custodial sentence not exceeding five years; or a monetary penalty; and
- money laundering (Article 305*bis* SCC) – penalty: a custodial sentence not exceeding three years; or a monetary penalty.

**Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)**

While the mere possession of hacking tools is not illegal, the provision or use of hacking tools can constitute a criminal offence. According to Article 144*bis* paragraph 2 SCC, whoever manufactures, imports, markets, advertises, offers or otherwise makes accessible programs that will be used to alter, delete or render unusable data without authorisation is liable to a custodial sentence

of up to three years or to a monetary penalty. In its decision BGE 129 IV 230, the Swiss Federal Supreme Court held that instructions and manuals explaining how to create programs that infect, destroy or render data unusable fall under the scope of this virus offence.

Moreover, any person who markets or makes accessible passwords, programs or other data that are intended to be used to obtain unauthorised access to a data processing system is liable to a custodial sentence not exceeding three years or to a monetary penalty as prescribed by Article 143*bis* paragraph 2 SCC.

Finally, exporting or brokering certain goods for monitoring the internet or mobile telecommunications without official permission can be liable to a custodial sentence of up to three years or to a monetary penalty pursuant to Article 9 of the Ordinance on the Export and Brokering of Goods for Monitoring Internet and Mobile Communication.

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

There is no explicit regulation for identity theft or identity fraud in Switzerland. Depending on the intention of the offender and his *modus operandi*, it can be covered by different articles of the SCC, such as Article 143 (unauthorised obtaining of data), Article 146 (fraud), Article 147 (computer fraud), Article 143*bis* (hacking) or Article 173 *et seqq.* (offences against personal honour).

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

Electronic theft can be covered by several criminal offences. Article 143 SCC prescribes the penalty for an unauthorised data acquisition. The maximum penalty is a custodial sentence of five years. Furthermore, any person who betrays a manufacturing or trade secret that is not to be revealed under a statutory or contractual duty, or anyone who exploits such a betrayal, can face a custodial sentence of up to three years or a monetary penalty under Article 162 SCC. Finally, according to Article 67 *et seqq.* of the Swiss Copyright Act, a copyright infringement that has been committed wilfully and unlawfully can be punished with a custodial sentence of up to one year or a monetary penalty; in cases of committing the offence for commercial gain, the penalty is a custodial sentence not exceeding five years or a monetary penalty.

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

The following further criminal offences impairing security, confidentiality, integrity and availability have to be considered under Swiss law:

- falsification or suppression of information in connection with a telecommunications service (Article 49 of the Swiss Telecommunications Act (TCA)) – penalty: a custodial sentence of up to three years; or a monetary penalty;
- unauthorised misuse or disclosure of information received by means of a telecommunications installation that was not intended for the receiver (Article 50 TCA) – penalty: a custodial sentence of up to one year; or a monetary penalty;
- interfering in telecommunications or broadcasting (Article 51 TCA) – penalty: a custodial sentence of up to one year; or a monetary penalty;
- obstructing, disrupting or endangering the operation of a telecommunication service or utility provider (Article 239 SCC) – penalty: a custodial sentence of up to three years; or a monetary penalty;
- breach of professional confidentiality (Article 321 SCC) – penalty: a custodial sentence of up to two years; or a monetary penalty. Article 35 of the Swiss Federal Act on Data Protection (FADP) – penalty: monetary penalty. Article 47 of the Banking Act – penalty: a custodial sentence of up to three years; or a monetary penalty. Article 147 of the Financial Market Infrastructure Act (FMIA) – penalty: a custodial sentence not exceeding three years; or a monetary penalty;
- breach of postal or telecommunications secrecy (Article 321ter SCC) – penalty: a custodial sentence not exceeding three years; or a monetary penalty. Articles 43 and 53 TCA – penalty: fine not exceeding CHF 5,000; and
- unsolicited distribution of spam massages (Article 3 *lit. o* in conjunction with Article 23 of the Swiss Federal Law on Unfair Competition) – penalty: a custodial sentence of up to three years; or a monetary penalty.

**Failure by an organisation to implement cybersecurity measures**

There is no generally applicable regulation in Switzerland specifically requiring the implementation of certain cybersecurity measures (for sector-specific requirements, see question 3.2 below). However, general compliance obligations require the implementation of an internal control system (relevant for companies limited by shares, see Article 20 of the Swiss Code of Best Practice for Corporate Governance) and technical and organisational measures to ensure the confidentiality, integrity and availability of information and IT systems, which can include the implementation of an adequate information security management system (relevant for all organisations, see Article 7 FADP).

The Swiss Federal Council adopted the second "National Strategy on Switzerland's Protection against Cyber Risks" (NCS) in 2018 for the years 2018–2022. The strategy builds on the work of the first NCS (2012–2017), expands it where necessary and supplements it with new measures so that it corresponds to the current threat situation. It was developed in collaboration with industry, the cantons and universities and thus forms the basis for the necessary joint efforts to reduce cyber risks.

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

The extraterritorial application of the SCC, with regard to the offences mentioned above, requires that the offender is present in Switzerland and will not be extradited (Articles 6, 7 SCC). In the context of phishing, it is currently in dispute between the Swiss Office of the Attorney General and the criminal courts whether, on the basis of the Council of Europe's Cybercrime Convention in conjunction with Article 6 SCC, such offences committed abroad are even subject to Swiss criminal jurisdiction where the offender and victim are not Swiss citizens.

### 1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Yes, Swiss criminal law incorporates the mitigating principles of withdrawal and active repentance. If a person of his own accord does not complete the criminal act. or if he assists in preventing the completion of the act, the court may reduce the sentence or waive any penalty (Article 23 SCC).

### 1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

The following other provisions can be applicable in the context of cybersecurity:

- causing fear and alarm among the general public (Article 258 SCC);

- public incitement to commit a felony or act of violence (Article 259 SCC);
- participating in or supporting a criminal organisation (Article 260*ter* SCC);
- financing terrorism by collecting or providing funds (Article 260*quinquies* SCC);
- foreign operations and activities directed against the security of Switzerland (Article 266*bis* SCC);
- diplomatic treason: endangering the interest of Switzerland: (i) by making a secret accessible to a foreign country; or (ii) by falsifying, destroying, disposing of or stealing documents relating to Switzerland's legal relations with a foreign state (Article 267 SCC);
- political, industrial or military espionage in the interest of a foreign state or organisation (Articles 272, 273, 274 SCC);
- founding of an unlawful association (Article 275*ter* SCC); and
- criminal provisions concerning the representation of acts of violence (Article 135 SCC), pornography (Article 197 SCC) or racial discrimination (Article 261*bis* SCC).

Please note the decisions of the Swiss Federal Criminal Court, SK.2013.39, and the Swiss Federal Supreme Court, BGer 6B_645/2007, both regarding cases of "cyber-jihad/cyber-terrorism", included several of the above-mentioned offences as part of the subject of the accusation.

## 2 Applicable Laws

**2.1 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, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.**

The Applicable Laws are as follows:

- Federal Act on Data Protection.
- Ordinance to the Federal Act on Data Protection.
- Swiss Criminal Code.
- Telecommunications Act.
- Ordinance on Telecommunications Services.
- Federal Act on Copyright and Related Rights.
- Trade Mark Protection Act.
- Civil Code, Code of Obligations.
- Banking Act.
- Ordinance on Banks.
- Financial Market Infrastructure Act.
- Financial Market Supervision Act.
- Federal Law on Unfair Competition.
- Federal Act on the Implementation of International Sanctions.
- Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods.
- Ordinance on the Export, Import and Transit of Dual Use Goods, Specific Military Goods and Strategic Goods.
- Ordinance on the Export and Brokering of Goods for Monitoring Internet and Mobile Communication.
- Federal Act on the Intelligence Service.
- Federal Information Security Act.

**2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.**

In Switzerland, there are no generally applicable mandatory cybersecurity requirements for critical infrastructures so far (for sector-specific requirements, see question 3.2 below). In 2017, the Swiss Federal Council adopted the "National Strategy on the Protection of Critical Infrastructures" (SKI) for the years 2018–2022. The Swiss Federal Office for Civil Protection was mandated to implement the strategy and published a "Guideline for the Protection of Critical Infrastructures" in 2015 (updated in 2018), outlining recommended risk, crisis and continuity concepts based on international standards. Furthermore, the Swiss Federal Information Security Act prescribes certain security measures for Swiss Federal authorities and offers support to private operators of critical infrastructures to minimise network and system disruptions.

**2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.**

There is no generally applicable requirement in Switzerland to take measures to monitor, detect, prevent or mitigate Incidents. However, Article 7 FADP in conjunction with Articles 8 and 9 of the Ordinance to the FADP provide that personal data must be protected against unauthorised processing, destruction, loss, technical faults, forgery, theft or unlawful use through the implementation of adequate technical and organisational measures including mandatory controls of the following IT and data-related circumstances: entrance; personal data carrier; transport; disclosure; storage; usage; access; and input.

With regard to specific cybersecurity safeguards to be implemented in the financial and telecommunications sector, see question 3.2 below.

**2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.**

Such conflicts of laws cannot currently be perceived.

**2.5 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.**

So far, there is no general reporting obligation for cyberattacks in Switzerland. However, a duty to notify the Swiss Federal Data Protection and Information Commissioner in cases of unauthorised data processing or loss of data has been included in the preliminary draft of the revised FADP. Specific reporting obligations are currently only imposed on certain industries such as the financial and the telecommunication sector, see question 3.2 below.

**2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share 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) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?**

Organisations have the possibility (not the obligation) to inform MELANI, the Swiss Reporting and Analysis Centre for Information Assurance. Such a notification can be filed anonymously with a simple message on MELANI's website. Furthermore, it is also possible to inform the Swiss Coordination Unit for Cybercrime Control (CYCO).

**2.7 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 no such explicit obligation to inform affected individuals under Swiss law. However, in the legal literature, it is partially held that organisations are obligated to report such Incidents to the affected individuals in accordance with Article 4 paragraph 2 FADP, incorporating the principle of good faith. The necessity and extent of such information depends on the circumstances, e.g. the gravity of the breach and the necessity to prevent any damages and potential abuse of the disclosed data. The preliminary draft of the revised FADP provides for obligations to notify affected data subjects in cases of unauthorised data processing or loss of data.

**2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?**

The responses do not change.

**2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.**

The supervisory authorities monitoring and enforcing the above-mentioned requirements pertaining to general data protection and sector-specific cybersecurity are the following:

- Federal Data Protection and Information Commissioner.
- Cantonal Data Protection Commissioners.
- Federal Office of Communications (OFCOM).
- Financial Market Supervisory Authority (FINMA).

**2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?**

Due to the absence of a general obligation to implement safeguards against cyberattacks or to report Incidents to an authority, there are no penalties for not complying.

For penalties triggered by not complying with sector-specific obligations to report Incidents to the supervisory authorities, see question 3.2 below.

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

So far, to our knowledge, the competent supervisory authorities have enforced sector-specific reporting provisions only in cases that had no connection with cybersecurity. However, in 2016, FINMA ordered banks of supervisory category 1 (extremely large, important and complex market participants; very high risk) and category 2 (very important, complex market participants; high risk) to conduct an additional examination and invited those of category 3 (large and complex market participants; significant risk) to conduct a self-assessment pertaining to the status of the implementation of safeguards against cyberattacks.

**2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?**

**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 general permission or prohibition for organisations to use Beacons; however, each organisation must analyse whether with the use of this measure, and the way it is used, provisions of the Swiss Criminal Act, Data Protection Act, Unfair Competition Act, etc. could be infringed. The Swiss Federal Intelligence Service (FIS) is subject to certain conditions permitted to use such kind of measures based on the Federal Act on the Intelligence Service.

**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 general permission or prohibition for organisations to use Honeypots, however each organisation must analyse whether with the use of this measure and the way it is used, provisions of the Swiss Criminal Act, Data Protection Act, Unfair Competition Act, etc. could be infringed. The Swiss Federal Intelligence Service (FIS) is permitted to use such kind of measures, subject to certain conditions, based on the Federal Act on the Intelligence Service.

**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 general permission or prohibition for organisations to use Sinkholes; however, each organisation must analyse whether with the use of this measure and the way it is used, provisions of the Swiss Criminal Act, Data Protection Act, Unfair Competition Act, etc. could be infringed. The Swiss Federal Intelligence Service (FIS) is permitted to use such kind of measures, subject to certain conditions, based on the Federal Act on the Intelligence Service.

## 3 Specific Sectors

**3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.**

Yes, market practice varies across business sectors as the legal requirements are different (see question 3.2 below).

In addition, please note that, on 18 April 2018, the Swiss Federal Council adopted "The National Strategy for the Protection of Switzerland against Cyber Risks" which will certainly impact all sectors in Switzerland.

**3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?**

(a) Yes, Article 14 of the Financial Market Infrastructure Act (FMIA) requires financial market infrastructures (*i.a.* stock exchanges, trading facilities, payment systems) to operate robust IT systems which are appropriate for their activities, provide for effective emergency arrangements, ensure the continuity of business activity, and provide for measures to protect the integrity and confidentiality of information regarding their participants and their transactions. Article 3f of the Banking Act and Article 12 paragraph 4 of the Ordinance on Banks require banks to implement appropriate risk management, including an internal control system, in order to detect, limit and monitor, *i.a.*, relevant operational risks. These requirements are specified in the recently updated FINMA Circular 2008/21 "Operational Risks – Banks" where the minimum details of a cyber risk management concept to be implemented based on international standards are outlined (protection of processes/IT systems/sensitive data, detection and recording of cyberattacks, remedial measures, recovery of normal operations, regular vulnerability analysis and penetration testing). FINMA Circulars are not legally binding, but they elaborate the regulator's intended enforcement practice and are regularly accepted and complied with by the industry.

According to Article 29 paragraph 2 of the Financial Market Supervision Act (FINMASA), FINMA has to be informed about any Incident that is of substantial importance to supervision, which can include Incidents that could have a negative impact on the reputation or operation of the financial institution or the financial centre of Switzerland. Pursuant to Articles 45 and 46 FINMASA, the wilful provision of false information to FINMA or failing to make a mandatory report to FINMA can be punished with a custodial sentence of up to three years or a monetary penalty and, in cases of negligence, with a fine of up to CHF 250,000. In case of a serious infringement of the supervisory provisions, the licence of a supervised person or entity can, according to Article 37 FINMASA, be revoked, its recognition withdrawn or its registration cancelled.

(b) On the basis of Article 96 paragraph 2 of the Ordinance on Telecommunications Services (OTS), OFCOM has published a currently non-binding "Guideline on Security and Availability of Telecommunications Infrastructures and Services" recommending telecommunications service providers to implement, monitor and update: (i) an information security management system as described in the international standards relating to information security, such as ISO/IEC 27001:2005 and ITU-T X.1051; (ii) a business continuity plan; and (iii) a disaster recovery plan, and to comply with international security recommendations in the ICT sector, such as the "ETSI White Paper No. 1 – Security for ICT" and the "ITU-T ICT Security Standards Roadmap". OFCOM has the competence to declare the mentioned guideline to be binding. Article 96 OTS prescribes the obligation of telecommunications service providers to immediately inform OFCOM of disruptions in the operation of their networks which (potentially) affect at least 30,000 customers (landline, over-the-top, broadcasting) or 25 transmitter sites (mobile communications). OFCOM requires the operators to include in the report, *i.a.*, a description of the disruption, the categories of causes (cable rupture, energy/hardware/software/human failure, cyberattack, malicious interference), and the measures taken to end the disruption. Pursuant to Article 53 of the Telecommunications Act, anyone who infringes any provision of the telecommunications legislation, such as the reporting obligation under Article 96 OTS, is liable to a fine not exceeding CHF 5,000.

Finally, there are further sector-specific requirements, particularly in connection with aviation, the railway industry and nuclear energy.

## 4 Corporate Governance

**4.1 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' duties in your jurisdiction?**

If the failure results from not having an adequate compliance management system (including risk management, internal reporting and control, and sufficient supervision) in a company limited by shares or a limited liability company, this can constitute a breach of the directors' obligation to perform their duties with all due diligence and to safeguard the interests of the company in good faith (Articles 717, 812 Code of Obligations) and to supervise the persons entrusted with managing the company, in particular with regard to compliance with the law (Article 716a Code of Obligations). These duties are only explicitly imposed on members of the board of directors, managing directors and executive officers of companies limited by shares, and managing directors of limited liability companies.

**4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (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?**

(a) There is no such general obligation to designate a CISO under Swiss law.

(b) Apart from special sector-related requirements (see question 3.2 above), there is no such general obligation to establish a written Incident response plan or policy.

(c) Apart from special sector-related requirements (see question 3.2 above), there is no such general obligation to conduct periodic cyber risk assessments, including for third-party vendors.

(d) Apart from special sector-related requirements (see question 3.2 above), there is no such general obligation to perform penetration tests or vulnerability assessments.

**4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?**

There are no generally applicable disclosure requirements in relation to cybersecurity risks or Incidents for companies in Switzerland (for sector-specific requirements, see question 3.2 above). However, if an Incident may result in damage claims or penalties, these risks have to be assessed and appropriate provisions have to be established and included in the balance sheet in the annual reports.

Furthermore, in the event that a large number of data subjects are affected, there may be an exceptional duty to report the Incident publicly according to the data procession principle of good faith (see question 2.7 above). This can particularly be the case if the data subjects concerned cannot be informed individually.

**4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?**

There are no other specific requirements.

## 5 Litigation

**5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.**

According to Article 15 paragraph 1 FADP in conjunction with Article 28 *et seqq.* of the Swiss Civil Code, the affected person of a cybercrime-induced data breach has the possibility to bring actions relating to the protection of privacy, provided that there is a violation of personality rights, e.g. due to data theft or illegal data processing. This can include actions for damages, prohibitive injunctions, information/disclosure and notification of third parties or the publication of judgments. Furthermore, members of the board of directors, managing directors and executive officers of companies limited by shares, and managing directors of limited liability companies, are liable both to the company and to the individual shareholders and creditors, for any losses or damage arising from any intentional or negligent breach of their duties (Articles 754, 827 Code of Obligations); see question 4.1 above.

**5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.**

To date, we are not aware of any civil actions that have been filed by affected persons or companies in relation to cybersecurity Incidents in Switzerland. The few judgments pertaining to liability for data breaches derive from administrative investigations conducted by the supervisory authorities.

**5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?**

If the claimant is able to prove damages and the violation of a legally protected right or norm, the purpose of which is to protect from such damages, he is entitled to compensation for moral sufferings and the payment of damages by virtue of Articles 49 and 41 of the Code of Obligations. Furthermore, according to Article 423 of the Code of Obligations, data subjects can request the handing-over of profits arising from violations of their privacy rights.

## 6 Insurance

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

Since 2000, organisations have the possibility to take out insurance against cyberattacks. The offered coverage includes, for example, loss or theft of data, damages due to hacking and malware, and the unauthorised disclosure of data.

**6.2 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 regulatory limitations to insurance coverage concerning such Incidents.

## 7 Employees

**7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?**

(a) There are no such specific requirements.
(b) A general reporting obligation of cyber risks and other potential Incidents for employees *vis-à-vis* the employer can, according to Article 321a of the Code of Obligations, be derived from the duty of care and loyalty.

**7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?**

Laws with possibly inhibiting effects on reporting cyber risks and similar Incidents may be triggered by the secrecy provisions mentioned under the last heading of question 1.1 above. Furthermore, in Switzerland, there is no explicit protection for whistleblowers, so far, who report Incidents with regard to their employers to public authorities or the media. However, a draft bill of the Code of Obligations, which is still under the scrutiny of the legislative institutions, introduces such whistleblower protection from termination and other detriments (Article 336 paragraph 2 *lit.* d, Article 328 paragraph 3 Code of Obligations).

## 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.**

KOBIK, the Swiss Coordination Unit for Cybercrime, does not only function as a notification office for cybercrimes, but also looks actively for criminally relevant content on the internet. However, after its verification, KOBIK passes the information to the competent criminal law enforcement authorities, which are the local, cantonal and Swiss Federal police departments and public prosecutors' offices.

**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?**

There are no such requirements under Swiss law.

**Clara-Ann Gordon** is specialised in the areas of TMT/outsourcing, data privacy, internal investigations/e-discovery and compliance. She regularly advises clients in the above areas on contractual, governance/compliance and other legal matters, represents clients in transactions and before the competent regulatory and investigating authorities as well as before state courts, arbitral tribunals and in mediation proceedings, and renders opinions on critical regulatory and contract law topics in the said industry-specific areas.
She has advised on and negotiated a broad range of national and international IT, software and outsourcing transactions (also in regulated markets), has represented clients in technology-related court proceedings and international arbitration, and is experienced in data protection and secrecy laws, white-collar investigations and e-discovery, telecom regulations (including lawful interception), e-commerce, and IT law.
Ms. Gordon regularly publishes in the field of technology (ICT) and frequently speaks at national and international conferences on emerging legal issues in technology law.

**Niederer Kraft Frey Ltd.**
Bahnhofstrasse 53
CH-8001 Zurich
Switzerland

Tel: +41 58 800 8426
Email: clara-ann.gordon@nkf.ch
URL: www.nkf.ch

**András Gurovits** specialises in technology (IT, telecoms, manufacturing, regulatory) transactions (including acquisitions, outsourcing, development, procurement, distribution), data protection, corporate, dispute resolution (including administrative proceedings) and sports.
He regularly advises clients on contractual, compliance, governance, disputes and other legal matters in the above areas.
He, thus, not only advises in these areas, but also represents clients before the competent regulatory and investigating authorities, state courts and arbitral tribunals.
Dr. Gurovits is distinguished as a leading lawyer by various directories such as *Chambers* and *The Legal 500*. Dr. Gurovits has been a lecturer at the University of Zurich for more than a decade. Presently, he is a listed arbitrator with the Court of Arbitration for Sport (CAS/TAS) in Lausanne and a member of the Legal Committee of the International Ice Hockey Federation.

**Niederer Kraft Frey Ltd.**
Bahnhofstrasse 53
CH-8001 Zurich
Switzerland

Tel: +41 58 800 8377
Email: andras.gurovits@nkf.ch
URL: www.nkf.ch

# ICLG.com

## Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Law
Business Crime
Cartels & Leniency
Class and Group Actions
Competition Litigation
Construction & Engineering Law
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investments
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Sanctions
Securitisation
Shipping Law
Telecoms, Media and Internet Laws
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by global legal group