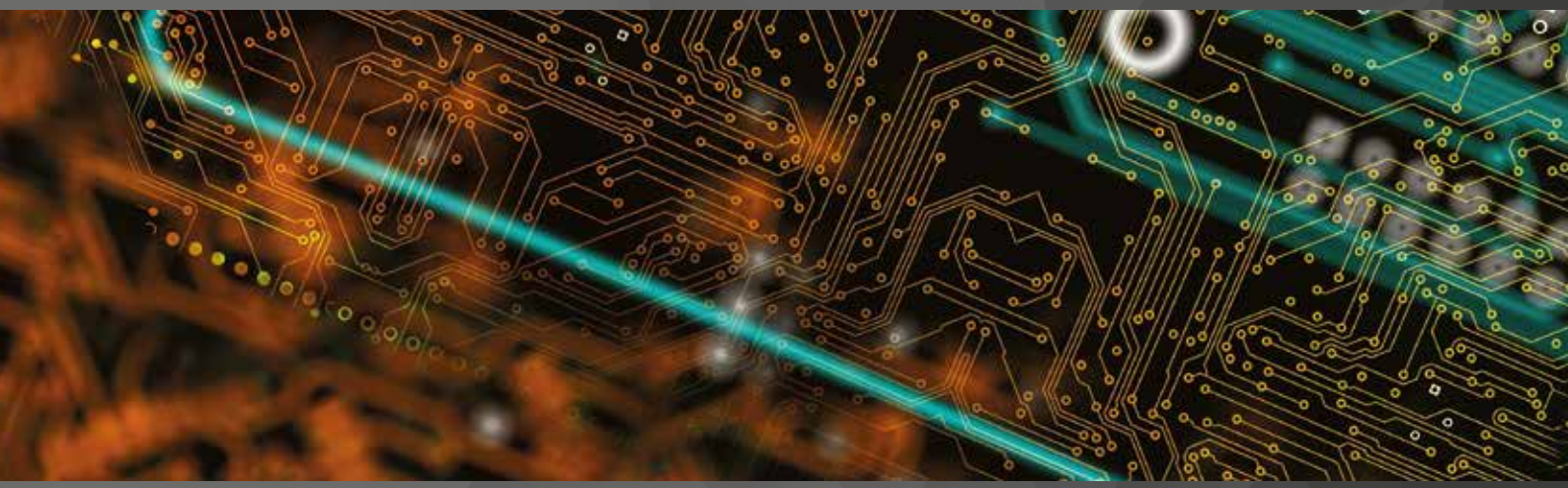
International Comparative Legal Guides



Cybersecurity 2021

A practical cross-border insight into cybersecurity law

Fourth Edition

Featuring contributions from:

Alburhan
Allen & Overy LLP
Ankura Consulting Group
Creel, García-Cuéllar, Aiza y Enríquez
Drew & Napier LLC
Eversheds Sutherland (Germany) LLP
Hamdan AlShamsi Lawyers & Legal Consultants
Ince
Iwata Godo
Kellerhals Carrard
King & Wood Mallesons
Kluge Advokatfirma AS
Lee & Ko
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan LLP
Mori Hamada & Matsumoto
Nikolinakos & Partners Law Firm
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Ropes & Gray LLP
Rothwell Figg
Rubino Avvocati
Schönherr Rechtsanwälte GmbH
Simion & Baciu
Sirius Legal
Stehlin & Associés
TIME DANOWSKY Advokatbyrå AB

ICLG.com

Expert Chapters

Q&A Chapters

Austria


Christoph Haid


Veronika Wolfbauer


Michael Lindtner

Schönherr Rechtsanwälte GmbH

1 Cybercrime

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

Hacking (i.e. unauthorised access)

Hacking may constitute the criminal offences of illegal access to a computer system (Sec. 118a of the Austrian Criminal Code, "**ACC**") or illegal interception of messages or data (Secs 119, 119a ACC). Depending on the circumstances of the case, these offences provide a fine of up to 360 daily rates or imprisonment of up to six months, and in severe cases even up to three years (i.e. if critical infrastructure is affected and the perpetrators act within a criminal organisation).

Hacking may involve unlawful access, use, alteration or disclosure of personal data. If personal data is processed unlawfully, this constitutes an administrative offence, with a fine of up to EUR 20 million or up to 4% of the total worldwide annual turnover, whichever is higher (Art. 83 General Data Protection Regulation, "**GDPR**"). If not covered by Art. 83 GDPR, intentionally and illegally gaining access to data processing or maintaining an obviously illegal means of access may lead to an administrative fine of up to EUR 50,000 (Sec. 62 (1) Austrian Data Protection Act, "**ADPA**").

Furthermore, the unlawful processing of personal data may also constitute the criminal offence of data processing with the intention to make a profit or to cause harm (Sec. 63 ADPA), with a fine of up to 720 daily rates or imprisonment of up to one year.

Denial-of-service attacks

Denial-of-service attacks may constitute the criminal offence of disruption of IT systems, pursuant to Sec. 126b ACC. According to this provision, anyone who seriously disrupts the functioning of an IT system, which he may not have at his disposal or not alone in his disposal, by entering or transmitting data shall be punished by imprisonment of up to six months or a fine of up to 360 daily rates, and in severe cases by imprisonment of between six months and five years (e.g. if the damage exceeds EUR 300,000). Further, denial-of-service attacks could also constitute data corruption, pursuant to Sec. 126a ACC, if data is destroyed or manipulated by the attack. Sec. 126a ACC provides punishment by imprisonment of up to six months or a fine of up to 360 daily rates or, in severe cases, by imprisonment of between six months and five years (e.g. if the damage exceeds EUR 300,000).

Denial-of-service attacks usually do not involve the processing of personal data. However, in case personal data is processed unlawfully, see "Hacking (i.e. unauthorised access)" above.

Phishing

Phishing can constitute various criminal offences, which highly depends on the circumstances of the case. If the victim is, for example, deceived and misled to a self-damaging act (e.g. a bank transfer), phishing may constitute fraud according to Sec. 146 *et seq.* ACC, which shall be punished in severe cases by imprisonment of between one and 10 years (if the damage exceeds EUR 300,000). Phishing could also constitute misuse of software or access data, pursuant to Sec. 126c ACC, under certain conditions, e.g. if the perpetrator thereby obtains access data (e.g. passwords) with the intent to damage the respective IT system. Sec. 126c ACC will be punished by imprisonment of up to six months or a fine of up to 360 daily rates. Moreover, phishing can constitute a breach of Sec. 241h ACC, which covers, *inter alia*, spying-out data of non-cash means of payment with the intent to illegally enrich oneself or third parties thereby, and will be punished by imprisonment of up to one year or 720 daily rates (in severe cases, imprisonment of up to three years).

Phishing typically involves the unlawful processing of personal data. For further information on the administrative and criminal penalties, see "Hacking (i.e. unauthorised access)" above.

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

Infection of IT systems with malware may constitute various offences under the ACC. Malware that manipulates or destroys data may, for example, constitute data corruption (Sec. 126a ACC), which will be punished by imprisonment of up to six months or a fine of up to 360 daily rates or, in severe cases, imprisonment of between six months and five years (e.g. if the damage exceeds EUR 300,000). If the IT system is seriously disrupted by the infection, this could also constitute disruption of IT systems (Sec. 126b ACC), which shall be punished

by imprisonment of up to six months or a fine of up to 360 daily rates, and in severe cases, by imprisonment of between six months and five years. Further, infection of IT systems with malware could also constitute illegal interception of messages or data (Secs 119, 119a ACC) under certain conditions, which will be punished by imprisonment of up to six months or a fine of up to 360 daily rates. The use of ransomware may further constitute blackmail (Sec. 144 ACC) punished by imprisonment of between six months and five years (in severe cases between one year and 10 years).

Where malware is used to unlawfully access, use, alter or disclose (or, more generally, process) personal data, the administrative and criminal penalties listed under "Hacking (i.e. unauthorised access)" apply.

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

Distribution of software or hardware or other tools which are, according to their specific nature, designed for certain cyber-crimes (e.g. spy-software, worms, trojans, viruses, etc.), may be punished under Sec. 126c ACC (misuse of software or access data) by imprisonment of up to six months or a fine of up to 360 daily rates.

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

The possession of such means is punishable under Sec. 126c ACC (misuse of software or access data) if the perpetrator also has the intent to use these means for cyber-crimes. Otherwise, the mere possession of such means is not punishable under the ACC.

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

Austrian criminal law does not provide for a specific offence covering identity theft. However, identity theft may constitute processing with the intention to make a profit or to cause harm according to Sec. 63 ADPA, or data falsification under Sec. 225a ACC, which covers the creation of false data or falsification of data by entering, manipulation, deletion or suppression with the intent of using them in legal transactions to prove a right, a legal relationship or a fact. Breaches of Sec. 225a ACC will be punished by imprisonment of up to one year or a fine of up to 720 daily rates. Further, depending on the specifics of the case, fraud (Sec. 146 ACC), defamation (Sec. 297 ACC) or insult (Sec. 115 ACC) could be relevant, providing penalties ranging from (i) imprisonment of one to 10 years (severe fraud), to (ii) imprisonment of up to three months or a fine of up to 180 daily rates (insult).

Identity theft or identity fraud requires the unlawful processing of personal data and thus constitutes an administrative offence with a fine of up to EUR 20 million or up to 4% of the total worldwide annual turnover, whichever is higher (Art. 83 GDPR).

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

Electronic theft may in particular constitute the criminal offences of (i) processing with the intention to make a profit or to cause harm according to Sec. 63 ADPA (imprisonment of up to one year or a fine of up to 720 daily rates), (ii) violation of business secrets according to Sec. 11 of the Austrian Unfair Competition Act (imprisonment of up to three months or a fine of up to 180 daily rates), (iii) spying-out business secrets, pursuant to Sec. 123 ACC, if the secrets were not accessible by the perpetrator in his/her ordinary business activities and he/she acts also with the intent to disclose or utilise the business secrets (imprisonment of up to two years) or, under certain conditions, (iv) illegal access to a computer system according to Sec. 118a ACC if the perpetrator overcomes specific security measures in the IT system. Moreover, Secs 121 and 122 ACC protect special business secrets and could thus be relevant. However, the scope of these offences is, in practice, rather narrow. Depending on the circumstances of the case, the above-mentioned offences relating to phishing can also be relevant regarding electronic theft.

In case personal data is processed unlawfully, see "Hacking (i.e. unauthorised access)" above. In addition, transmitting data intentionally in violation of the rules on confidentiality (in particular by employees) is an administrative offence punishable by a fine of up to EUR 50,000 (Sec. 62 (1) (2) ADPA).

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Austrian criminal law does not explicitly govern "white-hat-hacking", which is why such cases need to be assessed on a case-by-case basis. However, there are good arguments that unsolicited testing of IT systems only to determine their vulnerabilities and weak points should not trigger criminal liability if the hacker does obviously not act with the intent to commit a criminal act and ensures the protection of the IT system, its data and third parties during the test.

In case personal data is processed unlawfully, see "Hacking (i.e. unauthorised access)" above.

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 most relevant cyber-crime provisions in the ACC consist of illegal access to a computer system (Sec. 118a ACC), violation of telecommunication secrecy (Sec. 119 ACC) and illegal interception of data (Sec. 119a), data corruption (Sec. 126a), disruption of IT systems (Sec. 126b ACC), misuse of software or access data (Sec. 126c ACC) and spying-out data of non-cash means of payment (Sec. 241h ACC).

In case personal data is processed unlawfully, see "Hacking (i.e. unauthorised access)" above.

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

The GDPR may be applicable to controllers established outside the EU/EEA in accordance with Art. 3 (2) GDPR.

The offences in the ACC, mentioned under question 1.1 above, have no explicit extraterritorial application. However, the ACC applies on all acts committed within Austria, which is the case if the perpetrator either acted in Austria or the effects of the offence occurred in Austria. Therefore, the ACC may also apply in cases where the perpetrator is physically not present in Austria but, for example, attacks an Austrian-based IT system from abroad.

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)?

If the hacker does not act with the intent to constitute the

respective criminal offence and ensures that there will be no damage, criminal liability would probably not be given. However, due to lack of jurisdiction, clear legal guidelines for ethical hacking are still missing, which is why we recommend assessing such cases on an individual basis. Nonetheless, even if a criminal offence would be constituted, Sec. 34 ACC stipulates mitigating factors for setting the actual punishment such as "noteworthy motives" or "absence of damages although the offence was committed", which could lower the penalty.

If personal data is processed unlawfully, the administrative fines under the GDPR and the ADPA apply irrespective of the intentions of the perpetrator or any ethical considerations. However, such considerations may be relevant when deciding the severity of the penalty (see Sec. 11 ADPA and Art. 82 (2) GDPR). Furthermore, in the case of first-time infringements, the ADPA shall use its corrective powers in accordance with Art. 58 GDPR, in particular by issuing reprimands.

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.

The most relevant laws on cybersecurity include the GDPR, ADPA and the Network and Information System Security Act (*Netz- und Informationssystemsicherheitsgesetz*, "**NISG**"). For sector-specific laws on cybersecurity, please refer to question 4.2 below.

From a criminal law perspective, the ACC, with its cybercrime provisions under Sec. 118a *et seq.*, is the most relevant law in terms of cybersecurity. Further, the Austrian Unfair Competition Act also contains certain laws indirectly relating to cybersecurity, such as provisions protecting business secrets.

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

Austria has implemented the NIS Directive (Directive EU 2016/1148) with the NISG. According to Sec. 17 NISG, operators of essential services shall take *appropriate and proportionate technical and organisational measures* ("**TOMs**") to manage the risks posed to the security of network and information systems that they use in their operations. Those measures shall ensure a level of security of network and information systems appropriate to the risk posed and conform to the state of the art.

The NISG applies to services in the sectors of energy, transport, banking, financial market infrastructures, health, drinking water supply and digital infrastructure. The service must be essential, in particular, for the maintenance of the public health service, the public supply of water, energy and vital goods, public transport or the functioning of public information and communication technology, and whose availability depends on network and information systems.

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.

With regard to personal data, the principle of integrity and confidentiality (Art. 5 (1) (f) GDPR) requires organisations to ensure appropriate security of the data and implement technical and/or organisational measures including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (also in relation to Arts 24, 25 and 32 GDPR).

According to Secs 17 and 21 NISG, operators of essential services and digital service providers shall take appropriate and proportionate TOMs to manage the risks posed to the security of network and information systems that they use in their operations.

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.

In the case of a personal data breach, the notification requirements of Art. 33 (1) GDPR apply. The notification must be made to the Austrian Data Protection Authority ("**DSB**"). The nature and scope of information that must be provided is stipulated by Art. 33 (3) GDPR. The DSB provides a German/English bilingual template on its website, to provide some guidance on the information required under the GDPR: https://www.dsb.gv.at. The reported data breaches are not published.

According to Secs 19 and 21 (2) NISG, operators of essential services and digital service providers shall notify any incident to the computer security incident response team (and in case no such team is established, to GovCERT). The notice must contain all relevant information on the incident and the technical framework conditions that are known at the time of the initial report, in particular the suspected or actual cause, the technology involved and the type of facility or system involved (Sec. 19 (3) NISG).

Operators of public communications networks or services must notify to the RTR-GmbH (the regulatory authority for telecommunications in Austria) any security breaches or losses of integrity where the incident has a significant impact on the operation of networks or services (Sec. 16a (5) Telecommunications Act "**TKG**"). The RTR-GmbH provides a template on its website to provide some guidance (only available in German): https://www.rtr.at. In case the incident involves a breach of the security of personal data, the provider of public communications services shall, without delay, notify the personal data breach to the DSB (Sec. 95a TKG).

Sec. 286 para. 1 ACC stipulates that anyone who intentionally fails to prevent an imminent or already in-progress intentional criminal act or, in cases where notification makes prevention

possible, does not notify the authority or the person threatened, shall be punished by imprisonment of up to two years, if the offence to prevent has at least been attempted and is punishable by imprisonment exceeding one year. Nonetheless, the punishment may not be more severe in nature than the law threatens for the act not prevented.

According to Sec. 286 para. 2 ACC, however, the offender shall not be punished if he:

(i) could not easily prevent or notify the act without exposing himself or a relative to a risk of considerable harm;
(ii) has become aware of the offence subject to punishment exclusively by means of a communication entrusted to him in his capacity as a pastor; or
(iii) would violate another legally recognised duty of confidentiality by the prevention or notification and would have weighed the consequences threatening from the violation of this duty more heavily than the adverse consequences from the omission of the prevention or notification.

Sec. 286 ACC is thus very complex, but ultimately states a general legal duty to prevent specific (cyber-)crimes under certain conditions, for example by notifying the authorities (i.e. the criminal police, the public prosecutor or the Cybercrime-Competence-Center at the Federal Criminal Police Office).

The nature and scope of information to be reported is not defined by the law, but we understand that the notification shall contain all information available and necessary to enable the authorities to prevent the respective crime and to protect the potential victim. However, if such information could harm the organisation if it were to be disclosed, an in-depth assessment to establish exceptions from the notification duty under Sec. 286 para. 2 ACC is recommended.

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

A personal data breach must be notified to the data subject when it is likely to result in a *high risk* to the rights and freedoms of the data subject (Art. 34 GDPR). The nature and scope of information that must be provided is stipulated by Art. 34 (2) GDPR. The overall approach is to provide the data subject with information on the nature of the personal data breach as well as recommendations for the person affected as to how to mitigate potential adverse effects. Such communication has to be made in a timely manner, as soon as reasonably feasible.

From a criminal law perspective, such a notification obligation could arise from Sec. 286 para. 1 ACC (notification of the authorities or the affected person to prevent certain crimes). We thus refer to our answers under question 2.4 above.

Similar to the GDPR obligations, providers of public communications services must notify the affected individuals in cases where a breach is likely to adversely affect their privacy or personal data (Sec. 95a TKG). The content of the notification must comply with Art. 3 of the EU Regulation 611/2013, which, *inter alia*, requires the description of the nature and content of the personal data concerned, the circumstances and the likely consequences of the breach. A notification to the individuals affected can only be omitted if the operator demonstrates to the satisfaction of the DSB that it has implemented appropriate technological protection measures in accordance with Regulation (EU) 611/2013.

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

In Austria, the supervisory authority, according to Art. 55 GDPR, is the DSB. With regard to the NISG, the competent authority is the Federal Ministry of the Interior.

The RTR-GmbH is the regulatory authority for telecommunications in Austria.

From a criminal law perspective, in particular the criminal police and the public prosecutors' offices are competent to prevent and prosecute Incidents. Further, there exists the so-called "Cybercrime-Competence-Center", which is established at the Federal Criminal Police Office and offers a reporting line for cyber-crimes (against-cybercrime@bmi.gv.at).

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

Violations of the GDPR may lead to an administrative fine of up to EUR 20 million or up to 4% of the total worldwide annual turnover, whichever is higher (Art. 83 GDPR).

Violations of the NISG may lead to an administrative fine of up to EUR 50,000, or up to EUR 100,000 in case of repeat offences (Sec. 26 NISG).

Violations of the TKG may lead to an administrative fine of up to EUR 58,000.

A violation of Sec. 286 ACC shall be punished by imprisonment of up to two years; however, the punishment may not be more severe in nature than the law provides for the crime not prevented. Further, civil law claims of the victim against the perpetrator are also possible in case of a violation of Sec. 286 ACC (e.g. tort claims).

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

The primary means of enforcement are the fines mentioned in question 2.7 above.

The DSB has the corrective powers stipulated by Art. 58 (2) GDPR, e.g. to issue warnings, orders, impose a temporary or definitive limitation including a ban on processing, etc.

There is currently no relevant case law on Sec. 286 ACC and Incidents.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems 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)

Austrian law does not explicitly regulate the use of beacons. However, beacons could, *inter alia*, conflict with applicable data protection laws if they collect personal data (such as IP addresses). The justification of the use of beacons should thus be assessed on a case-by-case basis, and from a criminal law perspective.

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)
Austrian law does not regulate the use of honeypots. However, if honeypots are used to counteract an actual cyber-attack, we believe that their usage could be justified from a criminal law perspective and subject to an individual assessment.

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)
Austrian law does not regulate the use of sinkholes. However, if sinkholes are used to counteract an actual cyber-attack and do not harm third parties, their usage could, subject to an individual assessment, be justified.

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?

In general, according to the secrecy of communication (Sec. 93 (3) TKG), eavesdropping, recording, intercepting or other monitoring of messages and the associated traffic and location data as well as the disclosure such information by persons other than a user without the consent of all users involved is not permitted.

Furthermore, all processing of personal data must comply with the GDPR. Control measures and technical systems to control employees as well as systems that automatically process employees' personal data may also require consent by the works council (Secs 96 and 97 ArbVG).

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?

Austrian law does not specifically regulate the import or export of such technology. However, if such technology is to be regarded as military- or weapons-related, restrictions could arise from both Austrian and EU law. We thus recommend legal assessment on a case-by-case basis.

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.

Under the GDPR, every data controller (and also every processor) is obliged to guarantee a level of data security that is appropriate to the risk. Such a level of "adequate" data protection must be assessed on a case-by-case basis. The requirements with respect to the TOMs depend, *inter alia*, on the state of the art, the cost of implementation and the nature, scope, context and purposes of data processing as well as the risks involved. Thus, the required TOMs differ significantly depending on the business sector, the specific activities, the categories of data processed, the size of the company, etc.

The authors are not aware of any market practice deviating from the legal requirements.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Specific rules exist that aim to mitigate potential risks in sectors where Incidents may endanger society as a whole and/or constitute a grave invasion of the privacy of individuals. These sectors include, *inter alia*, operators of essential services and digital service providers (NISG), telecommunication service providers (TKG), healthcare service providers (the Health Telematics Law or "**GTelG**"), financial and payment service providers (e.g. the Payment Services Act or "**ZadiG**") and energy/gas providers (the Electricity Industry and Organisation Act or "**ElWOG**"; the Gas Act or "**GWG**").

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?

Austrian company law (e.g. Sec. 84 of the Austrian Stock Corporation Act) requires the management to act with due diligence and in the best interest of the company. From this general duty of care, it may also follow that directors need to prevent, mitigate, manage and respond to Incidents in order to avoid or at least reduce damages of the company. Therefore, if the directors violate their duty of care relating to Incidents, civil liability of the directors is possible. However, the actual requirements and conditions of such a liability highly depend on the circumstances of the case (e.g. the size and sector of the company and the actual possibility of the directors to take adequate actions), which is why we recommend a case-by-case assessment. In that context, Sec. 286 ACC should also be taken into consideration (*cf.* question 2.4 above).

In general, according to the Austrian Act on Administrative Criminal Law ("**VStG**"), a legal representative of a company (e.g. a managing board member) is responsible under penal law for the legal compliance of the company (Sec. 9 VStG). Thus, administrative fines will be preliminarily imposed on the legal representative of a company. This, however, requires that the legal representative acted culpably, e.g. by neglecting duties of control and supervision. In recent years (and due to the rather high possible fines deriving from EU regulations), exceptions to this rule have been stipulated in national administrative provisions. Such an exception is in place, e.g., with regard to fines under the GDPR. According to Sec. 30 (2) ADPA, administrative fines are primarily imposed on *a legal entity* (and only in exceptional cases on individuals) if infringements of provisions of the GDPR were committed by persons who acted on behalf of the legal entity.

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?

There are no explicit legal obligations to designate a CISO, to

establish an Incident response plan or policy, to conduct periodic cyber risk assessments or to perform penetration tests/vulnerability assessments. However, depending on the specific case (in particular the size of the company, the scope of processing activities and the risks involved), such measures may be required to be implemented as state-of-the-art TOMs. Also, the designation of CISOs is common in most bigger companies, depending on the common practice within the specific industry.

Besides, the GDPR requires the designation of a Data Protection Officer ("**DPO**") in some specific cases; accordingly, a DPO has to be designated if: (i) the controller is a public authority/body; (ii) the core activity of the controller requires large-scale, regular and systematic monitoring of individuals; or (iii) the core activity of the controller consist of large-scale processing of special categories of data (e.g. health data) or data relating to criminal convictions and offences. Kindly note that there are no further obligations to designate a DPO under Austrian national law.

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 are no specific statutory provisions in this regard. However, disclosure obligations could arise in special situations or industries (e.g. capital markets and *ad hoc* reports). We thus recommend an individual assessment in this regard.

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.

A company may face tort claims from persons who suffered damages by the company's failure to act with due care. Nonetheless, victims would generally need to prove, *inter alia*, the damage and a breach of legal duties by the company, or, respectively, its management.

However, please note that anyone can file a criminal complaint (even anonymously) against a suspected company or person (e.g. the director of a company) and induce the criminal authorities thereby to investigate possible criminal conduct. It is also possible for victims to participate in a criminal proceeding as a "private party" to enforce their civil claims in the criminal proceeding.

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 are currently no such examples publicly available.

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

Yes. Civil law liability in tort may result if damage occurred due to a breach of legal duties. As mentioned under question 5.1 above, the legal duty to prevent Incidents may arise from general company law but also from Sec. 286 ACC (*cf.* question 2.4 above), which could then be a legal basis for tort claims of victims.

7 Insurance

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

Yes, companies are permitted to do so.

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 no regulatory limitations.

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.

The investigatory powers differ between the various authorities and depend on the respective laws they act on (e.g. criminal police, public prosecutor, data protection authority). However, in general, authorities have a wide scope to investigate Incidents and can under certain conditions, *inter alia*, perform house searches, request information from witnesses or seize IT hardware.

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 is currently no specific obligation to implement backdoors. However, it is recognised that witnesses have to disclose encryption keys, passwords and generally answer questions from law enforcement authorities under their obligation to testify completely and correctly. Further, *everyone* must grant access to information to be seized and stored on data carriers under certain conditions stipulated in the Austrian Criminal Procedure Code, which may thus also include the provision of encryption keys to the criminal authorities.

Christoph Haid is co-head of our crisis management & internal investigations practice. Christoph helps clients respond to crisis situations and conducts investigations for corporates and financial institutions, covering all relevant compliance aspects.

Schönherr Rechtsanwälte GmbH
Schottenring 19
1010 Vienna
Austria

Tel: +43 1 534 375 0119
Email: c.haid@schoenherr.eu
URL: www.schoenherr.eu

Veronika Wolfbauer has been with Schoenherr's regulatory practice group since 2013, became an attorney at law in 2016 and counsel in February 2019. Prior to joining Schoenherr, Veronika gained experience at well-known national law firms in Vienna and worked as legal counsel at a gas trading hub.
Veronika is a leading member in the firm's privacy and data protection team. In addition, she leads the technology regulation and audiovisual media law team. Veronika serves not only national but also international corporate clients, and lectures in those areas. She has vast experience in giving strategic and legal advice, as well as leading administrative law proceedings before the DP regulator and "appeal proceedings", including addressing the Austrian Highest Administrative Court, the Austrian Constitutional Court and the European Court of Justice.

Schönherr Rechtsanwälte GmbH
Schottenring 19
1010 Vienna
Austria

Tel: +43 1 534 375 0791
Email: v.wolfbauer@schoenherr.eu
URL: www.schoenherr.eu

Michael Lindtner has been an associate in Schoenherr's Vienna office since 2016 and his main area of practice is criminal compliance and white-collar crime, with a focus on anti-corruption law. Michael graduated from Vienna University of Economics and Business (Bachelor of Laws, 2012; Master of Laws, 2014; Doctorate, 2019). Before joining Schoenherr, he worked as an associate at a well-known national law firm in Vienna, completed the judicial clerk in Vienna and gained experience as a legal intern in well-known national law firms and as a consultant in an international tax consultancy firm.

Schönherr Rechtsanwälte GmbH
Schottenring 19
1010 Vienna
Austria

Tel: +43 1 534 375 0260
Email: m.lindtner@schoenherr.eu
URL: www.schoenherr.eu

Schoenherr is a leading full-service law firm in Central and Eastern Europe. Operating in a rapidly evolving environment, we are a dynamic and innovative firm with an effective blend of experienced lawyers and young talent. As one of the first international law firms to move into CEE/SEE, we have grown to be one of the largest firms in the region. Our comprehensive coverage of the region means we can offer solutions that perfectly fit the given industry, jurisdiction and company.

www.schoenherr.eu

schönherr

ICLG.com

Other 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
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
Outsourcing
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
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

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