Cybersecurity 2021

Contributing editors
Benjamin A Powell and Jason C Chipman

LEXOLOGY®
Getting The Deal Through

GDR

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2015
Seventh edition
ISBN 978-1-83862-643-3

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

Cybersecurity
2021

Contributing editors
Benjamin A Powell and Jason C Chipman
Wilmer Cutler Pickering Hale and Dorr LLP

Lexology Getting The Deal Through is delighted to publish the seventh edition of *Cybersecurity*, which is available in print and online at www.lexology.com/gtdt.

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

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes a new chapter on Belgium and the European Union.

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

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

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

LEXOLOGY
Getting The Deal Through

London
February 2021

Reproduced with permission from Law Business Research Ltd
This article was first published in March 2021
For further information please contact editorial@gettingthedealthrough.com

Contents

Austria

Árpád Geréd
MGLP Rechtsanwälte | Attorneys-at-Law

LEGAL FRAMEWORK

Legislation

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

Even though cybersecurity and, as a related topic, cybercrime have a long history in Austrian rules of law, efforts to establish dedicated and detailed rules on cybersecurity that are binding, not only for governmental agencies and (partially) state-owned companies but also the private sector, are fairly recent.

The first legal provision on cybersecurity in its widest sense was article 10 of the then new Austrian Data Protection Act (DSG 1978), which entered into force in 1980. In this provision, data processors were obliged to set up work rules regarding data security, such as measures for access security or software testing. While the provision did not contain any details on the required rules and, further, took economic and technical feasibility into account, it required these internal rules to be approved by the Austrian Data Protection Commission (now the Data Protection Authority, or DSB), thus granting at least a minimum level of homogeneity.

In hindsight, article 10, despite its lack of detail, provided a solid basis for a unified understanding of required data security measures. But in 1987 this provision was amended with far-reaching consequences: first, the new article 10 no longer required data security measures to be compiled in a set of work rules; and second, the requirement for approval by the now DSB was removed. However, the modified provision still took into account the economic and technical feasibility of the measures as well as their adequacy related to the processed data.

In Austria, a country dominated by small and medium-sized enterprises, the flexibility of article 10 DSG 1978, coupled with a legal and factual lack of control of the security measures taken, has led to wide variation of levels of cybersecurity and has, in extreme cases, led to very small enterprises not taking any relevant security measures at all, arguing that they were neither economically feasible nor required by the type of processed data. Unfortunately, this relatively toothless rule has found its way into article 14 of the current Austrian Data Protection Act (DSG 2000) in mostly unmodified form. While article 14 DSG 2000 applies to data controllers and data processors alike and corresponds in essence to article 17 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the EU Data Protection Directive), it is, nevertheless, a step backward from its predecessor, article 10 DSG 1978. As of 25 May 2018, however, the DSG 2000 was replaced by Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation), which provides for slightly more detailed rules on data security in its article 32.

The first cybercrime-related rules were established in 1987 with articles 126a and 148a of the Austrian Criminal Code (StGB). These provisions penalised the damaging of data and the abuse of automated data processing (including the modification of processed data as well as the processing software), respectively. Depending on the damage caused, these actions were punishable by imprisonment for up to five or 10 years respectively.

In 2002, Austria adopted the Council of Europe's Convention on Cybercrime, modifying the StGB to also penalise acts such as the illegitimate access to a computer system (article 118a) or the abusive interception of data (article 119a).

With these provisions of the DSG 2000 and the StGB, a first basic set of cybersecurity rules was in place, obliging enterprises to take protective measures while at the same time protecting their efforts and systems by means of the Criminal Code.

While it was not until 2014 that new legal rules on cybersecurity were announced, Austrian private entities as well as the federal government were far from inactive in the meantime.

The first industry-wide initiative to centrally collect and manage cybersecurity incidents from the private as well as the public sector was the Computer Incident Response Coordination Austria (CIRCA), established by the Internet Service Providers Association in cooperation with the Austrian Federal Chancellery. In 2008, CIRCA was incorporated into the newly created Austrian Computer Emergency Response Team (CERT) as well as the Austrian Government Computer Emergency Response Team (GovCERT) with the former being primarily operated by NIC.at, the Austrian domain registry, and the latter by the Federal Chancellery. Though factually important and well-recognised, the main purpose of both CERT institutions lies in the collection of information on incidents and the coordination of the incident response. As such, both institutions may only advise on prevention measures but have no authority to demand certain actions.

Apart from these two most important CERTs, there are others established at authorities or formerly state-owned enterprises, such as the City of Vienna, A1 (the former state-owned telephone operator) or the Austrian Federal Computing Centre (BRZ), which is the former federal data centre and now e-government partner of the federal administration in Austria. These are all organised in the Austrian CERT-network, which was established in 2011.

The most recent addition to the Austrian organisations active in the field of cybercrime is the Cyber Crime Competence Centre (C4), which was established in 2012. In contrast to the CERTs, the C4's aim is to actively combat cybercrime. Therefore, its personnel consists of members of the Austrian Federal Police as well as the Austrian Federal Ministry for Internal Affairs.

In May 2014, the Austrian government announced the introduction of a dedicated Austrian Cybersecurity Act. This announcement came in

the wake of similar efforts in Europe, most notably the presentation of the draft version of a Network and Information Security Directive by the European Commission in February 2012, in the meantime published as Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, and of a German law on cybersecurity (the IT Security Act) in March 2013. In June 2016, a White Paper was published that contains recommendations for the planned Austrian Cybersecurity Act. Following these recommendations, the new Act will be a transposition of the Network and Information Security Directive into Austrian law, taking into account Austria's experiences in combatting cybercrime so far, as well as the government's Austrian Strategy for Cybersecurity, which is based not only on general experience but also on the results of larger scale cybersecurity exercises held for the purpose of evaluating and improving cyber defence readiness.

While the promised draft of the Austrian Cybersecurity Act was still outstanding, another law has in fact established itself as the first legal act to require Austrian companies to ascertain an appropriate level of cybersecurity: Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, better known as the General Data Protection Regulation (GDPR). This Regulation, which entered into force on 25 May 2018, first and foremost aims at protecting personal data (ie, data by which a natural person can be identified). However, in contrast to the existing rules on data protection back then, the GDPR is no longer satisfied with requiring companies to have appropriate contractual provisions in place but explicitly also requires appropriate technical and organisational measures, thus, basically, cybersecurity measures.

In the meantime, the Austrian government has revived the Cybersecurity Act as the Network and Information Systems Security Act (NISG), which entered into force on 29 December 2018. Furthermore, on 18 July 2019 the Network and Information Systems Security Ordinance (NISV), which determines the businesses to be considered providers of critical infrastructure, defines security precautions and regulates the sectors and security incidents according to the NISG in more detail, entered into force.

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

The NISG established measures to ensure a high level of security of network and information systems of providers of critical infrastructure in the following sectors: energy; transportation; banking; financial market infrastructures; health care; drinking water supply; and digital infrastructure, plus digital services and public administration institutions. The details regarding which businesses active in the mentioned industry field actually fall within the scope of the NISG have been determined in the NISV (eg, by the amount of megawatts they generate in their power plants).

The Austrian communication industry, including internet service providers, already has a head start in the field of cybersecurity. This is not only because of IT forming the core or at least a substantial part of its business, but also owing to the involvement of the Austrian communication industry in the CIRCA and now CERT. The same applies to a few public authorities, most notably the Austrian Federal Chancellery and the BRZ. These entities are also the ones to have made the most progress towards promoting cybersecurity.

Other industries, however, still need to improve to varying degrees. For instance, the financial sector in Austria features some leading as well as, unfortunately, some less stellar examples. The Austrian energy sector has in the past mostly focused on downplaying the potential risks of networked power grids and smart metering in the media. The transportation sector has also appeared unevenly prepared to face cybersecurity challenges, with, for example, the Austrian Federal Railway (ÖBB) being one of the positive examples.

In 2014, the initiative Trust in Cloud (www.trustincloud.org) was launched by EuroCloud Austria, the Austrian association of EuroCloud Europe, an independent non-profit organisation. Participants include national and international enterprises from the IT sector, but also public and private entities from other sectors, such as the Austrian Federal Chancellery, the ÖBB, an international supermarket chain and an international producer of skiing equipment. While the aim of the initiative is to promote cloud computing in general, cybersecurity is one of the major focal points.

In any case, since the entry into force of the GDPR on 25 May 2018, binding rules on cybersecurity apply to any and all companies for the first time.

In general, the discussion around cybersecurity in recent years, fuelled again by the accelerated digitalisation during the covid-19 pandemic and lockdowns, has benefited Austrian businesses, turning a problem most would refuse to talk about for fear of gaining the reputation of not being secure enough into something that could affect anyone, no matter how well prepared. A significant degree of improvement of awareness, as well as of readiness, could be noted in the course of the many expert discussions during the conception of the Cybersecurity Act, as well as during the cybersecurity exercises held for the same purpose. The Austrian government today claims that Austria is a model example of cyberthreat readiness. While this evaluation may need to be taken with a grain of salt, it is nevertheless true that Austria is among the better-prepared member states of the European Union.

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

The Austrian Standards Institute, which is the Austrian member of the European Committee for Standardization and the International Organization for Standardization, has adopted all relevant international standards related to cybersecurity, most notably, ISO/IEC 27001:2013 (currently ÖVE/ÖNORM EN ISO/IEC 27001: 2017 07 01 in Austria).

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

While Austrian law knows the concept of responsible persons (ie, employees responsible for certain areas of business within their company) this concept does not extend to cybersecurity or (unlike, for example, Germany) even data protection. Thus, managerial employees or directors in Austria are liable only according to the general legal rules, which basically means that they need to act with due diligence and with the care of a prudent businessperson, as set forth by Austrian law and further detailed by rulings of Austrian courts.

The GDPR requires any company or organisation to periodically verify the effectiveness of the technical and organisational measures they have taken and document the results. This obligation exists indifferent of whether the company or organisation in question is required to have a dedicated data protection officer. However, as before the GDPR entered into validity, the consequences of default are generally borne by the company rather than any internally responsible employee or the director.

5 How does your jurisdiction define cybersecurity and cybercrime?

Austrian law knows no definition of either cybersecurity or cybercrime. While article 32 GDPR does stipulate data security measures, it does not define data security, much less cybersecurity. Also, the StGB penalises and defines certain acts of cybercrime, though it lacks a general definition of cybercrime as a whole.

In any case, cybersecurity in Austria is distinct from data privacy. Even though neither term is defined in Austrian law, from the provisions of the laws containing relevant provisions, above all the GDPR and the StGB, it becomes apparent that data privacy in Austria primarily deals with the rights and obligations related to the usage of data obtained legitimately, while the aim of data security as an aspect of cybersecurity is to prevent illegitimate access to and use or abuse of data.

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

Article 32 GDPR requires any controller or processor of personal data to implement measures to ensure data security. However, such measures need to take into account the type, extent and purpose of the processed data, the state of the art and the economic feasibility.

Therefore, even though this provision does stipulate minimum protective measures, it is not clear what the minimum requirements in each case may be. Further, this provision only applies to personal data rather than any type of data.

As a result, in the field of cybersecurity, industry standards and the recommendations of the CERT and GovCERT are more important in Austria than legal rules. This is especially true for relatively new technology such as cloud computing or the issues associated with various forms of 'bring your own device'.

Of course, the GDPR explicitly mentions that the European Commission, national data protection authorities and industry-specific organisations should define recommendations and standards for appropriate technological and organisational measures. These will, in the end, set forth the minimum requirements for cybersecurity any company will need to meet. Currently, however, except for individual rulings, the only binding rules and guidelines issued by the Austrian Data Protection Authority are two regulations on privacy impact assessments (PIA), one listing processing operations that do not require a PIA to be performed (DSFA-AV, published on 25 May 2018) and one listing processing operations that in any case require a PIA to be performed (DSFA-V, published on 9 November 2018).

However, providers of critical infrastructure and federal institutions do have to take measures in order to ensure a high level of security of network and information systems according to the NISG. For this purpose, according to articles 17, 21 and 22 NISG, appropriate measures need to take into account the state of the art and be appropriate to any risk that can be determined with reasonable effort. Therefore, providers of critical infrastructure will have to take into account the following: safety of systems and facilities; management of security incidents; business continuity management; monitoring; verification and testing; and compliance with international rules. In order to enable the verification of the measures taken, providers of critical infrastructure have to submit a list of the security measures they have carried out, including evidence of certification or inspections – and, if applicable, security deficiencies discovered – to the Federal Minister of Internal Affairs at least every three years. The Federal Minister is also authorised to issue recommendations regarding measures providers will have to take.

Scope and jurisdiction

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

Articles 40(e) and 40(f) of the Austrian Intellectual Property Act stipulate rules on decompilation of software and the use of databases, respectively. While these rules do not address cyberthreats specifically, they are the only ones addressing this subject explicitly within the context of intellectual property.

Where cyberthreats to intellectual property involve acts of cybercrime, the rules of the StGB apply.

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

In Austria, cyberthreats to critical infrastructure are specifically addressed by the NISG and NISV, which are in effect transpositions of the EU NIS Directive into Austrian law. With the entry into force of the NISG on 29 December 2018 and the NISV on 18 July 2019 the new EU standards have therefore been belatedly introduced to Austria.

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

The NISG obliges providers of critical infrastructure and digital services to immediately report any security incident concerning any essential or digital service they provide. The obligation on providers of digital services to report a security incident only applies if they have access to information needed to assess the impact of a security incident.

In this context, security incidents are defined by law as disruptions to the availability, integrity, authenticity or confidentiality of network and information systems which have led to a reduction in the availability, or failure, of the service operated with significant impact. In order to assess whether the impact is significant or not, the anticipated number of users affected, duration, geographical spread as well as the expected impact on economic and social activities have to be taken into account.

The GDPR also sets forth data breach notification requirements. However, according to the GDPR the national data protection authorities only need to be informed if the breach may result in a risk to the rights and freedoms of a natural person. Such risks, however, may be avoided by appropriate technical and organisational measures (eg, pseudonymisation, encryption).

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

The principal acts of cybercrime, relevant to businesses, which are penalised by the StGB depending on the amount of damage caused, are:

- illegitimate access to a computer system (article 118a);
- breach of telecommunication secrecy (article 119);
- abusive interception of data (article 119a);
- abuse of audio recording or listening devices (article 120, para 2a);
- damaging of data (article 126a);
- disruption of the functionality of a computer system (article 126b);
- abuse of software or access data (article 126c);
- fraudulent abuse of data processing (article 148a); and
- forgery of data (article 225a).

The fines are determined by the income of the culprit. Therefore, neither a minimum nor a maximum amount is stipulated by Austrian law.

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

For the time being, the Austrian government, on the one hand, has not specifically addressed any of the challenges associated with cloud computing. On the other hand, private and non-profit organisations, such as EuroCloud Austria and the Austrian Chamber of Commerce, have made significant efforts to educate providers and especially (private and business) users of cloud computing solutions, be it by means of events or publications, such as White Papers or even a recommendation catalogue relating to cloud contracts (some of these publications are available in English and can be obtained from the website of EuroCloud Austria: www.eurocloud.at).

Currently, the most important Austrian initiative regarding cloud computing is Trust in Cloud (www.trustincloud.org), which has formulated recommendations to the Austrian government, among others, in the field of cybersecurity. As the Austrian Federal Chancellery takes part in this initiative, it is realistic that those recommendations will be taken into account in the future.

In the NISG, cloud computing is defined as a type of 'digital service', therefore the regulations of the NISG for providers of digital services also apply to cloud computing offerings.

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

The NISG regulates the obligations of providers of critical infrastructure and digital services as well as public administration institutions. It defines them as institutions with a branch office in Austria that provide an essential service, respectively legal entities or registered partnerships with a main office in Austria that provide a digital service in Austria and are not defined as 'micro' or 'small enterprises'. However, providers of digital services without a main office in the European Union, that have appointed a representative, are treated in the same way. Therefore, foreign companies without a branch office in Austria, and which have not appointed a representative, are not subject to the NISG.

Concerning the regulations of the GDPR, they are, according to article 3, para 1 GDPR, applicable to the processing of personal data, insofar as it is related to the activities of an establishment of a person responsible for it or a processor established in the European Union, whether or not the processing takes place in the Union.

With regard to the processing of personal data relating to data subjects in the European Union by a controller or a processor not established in the European Union, article 3, para 2 GDPR applies. The GDPR therefore is applicable if the processing is carried out in order to:

- offer goods or services to persons in the European Union, irrespective of any obligation to pay; or
- monitor the behaviour of persons within the European Union.

The GDPR also applies to responsible persons and processors not established in the European Union but in a place which is subject to the law of a member state by virtue of international law, such as diplomatic or consular representations of a member state. Thus the GDPR applies to all organisations participating in the EU market, which also includes foreign companies.

In any case, the rules of the European Union regarding the free movement of goods and services will need to be observed. In principle this would mean that businesses already established in the European Union, be it with a seat or a representative, should fall under the jurisdiction of the member state in which they are established.

BEST PRACTICE

Increased protection

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

As there are currently no substantial laws on cybersecurity in Austria nor binding guidelines or best practices established on grounds of the data security requirements set forth in the General Data Protection Regulation (GDPR), enterprises need to rely on industry standards and recommendations by various organisations and authorities.

The first contact in the field of cybersecurity in Austria is the Austrian Computer Emergency Response Team (CERT) for private entities and the Austrian Government Computer Emergency Response Team (GovCERT) for the public sector. Both institutions not only coordinate responses to cyberthreats but also advise on prevention measures. Thus, they constitute the most important contributors to a harmonised understanding of required and recommended cybersecurity measures. To facilitate intra-sectoral exchange of information, sector-specific CERTs are planned with the Austrian Energy CERT for the energy sector already being established. Additionally, sector-specific cybersecurity exchanges for providers of various critical infrastructures have been established in the form of the Austrian Trust Circles.

Further, interested parties can find a multitude of freely available publications on this topic; for example, from the Federal Ministry for Internal Affairs, the Chamber of Commerce or associations specialised in IT topics.

In addition, a coordination committee was established with the introduction of the NISG which advises the Federal Minister of Internal Affairs and the Federal Government on the decision whether a 'cyber crisis' is occurring or not as well as the operative measures required in order to cope with such a crisis and the coordination of public relations.

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

While the Austrian government is very active in promoting cybersecurity directly as well as indirectly (eg, by means of GovCERT), there are currently no incentives in this context.

The Network and Information Systems Security Act (NISG) also follows the 'classical' approach and penalises inadequate cybersecurity measures, but otherwise does not provide any incentives for compliance.

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

In Austria, ÖNORM ISO/IEC 27001: 2017 07 01 (which can be obtained from the ASI against payment) as well as the recommendations of the CERT (available from their homepage: www.cert.at) can be regarded as the main industry standards and codes of practice in the field of cybersecurity.

Comprehensive guidelines summarising the relevant rules and recommendations, as well as a checklist created specifically for very small enterprises, have been created by the Austrian Chamber of Commerce and can be obtained from the microsite: www.it-safe.at.

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

Best practices and procedures can be derived from industry standards or recommendations of the CERT. They may vary depending on the type, severity and potential danger of a breach. Thus, there are no general rules apart from containing the breach and saving any information for later analysis.

After the incident it is considered best practice to have the existing data analysed by a trustworthy and independent third party to determine the methods and reasons for which the system could be breached and to take measures to prevent such occurrences in the future.

While the various decisions and recommendations of the data protection authorities, both in Austria and abroad, have provided some guidance in regard to cybersecurity, it is still either rather general or very case specific. In the latter cases best practices can be seen slowly developing based on the decisions and recommendations.

Information sharing

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

Voluntary information on cyberthreats should be addressed to the CERT (or the GovCERT, in the case of a public entity) by means of an email containing:

- details of where the incident has occurred (eg, IP address, website);
- details of the nature of the incident (eg, a virus, a DoS attack);
- details of how the incident has been noticed (eg, log files);
- a request for feedback; and
- an electronic signature.

As there are no recommended standard procedures that the notifying entity can follow in the meantime, it will need to wait for a response from the CERT. In any case, records of the incident should be saved in case they are destroyed or modified during the incident. For providers of critical infrastructure and digital services, the NISG stipulates that these voluntary reports are forwarded to the Federal Ministry for Internal Affairs by the CERT.

Unfortunately, there are currently no incentives to voluntarily disclose information on cyberthreats, apart from peer pressure within the industry.

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

In the field of cybersecurity, cooperation between the private and the public sector has a long tradition in Austria, its first highly visible project being the Computer Incident Response Coordination Austria, established in 2003 by the Internet Service Providers Association and the Federal Chancellery.

Nowadays, the cooperation continues mainly within the Austrian CERT network, where the most important stakeholders from the private and public sectors are united either directly or indirectly through the participating CERTs. Within this network, not only is the collected information on incidents or threats exchanged, but the incident response and the advice on prevention measures are also coordinated.

The results are then propagated by the participants to other organisations, such as the Chamber of Commerce, which issue recommendations to their members, usually in the form of publications. Of course, the flow of information works both ways.

In December 2014, Curatorship Safe Austria, an independent association focused on issues related to internal security, organised a large-scale cybersecurity exercise focused on threats to critical infrastructures, in which, among others, the CERTs, the Federal Ministry for Internal Affairs and various private enterprises participated. The aim of the exercise was to optimise communication between the participants, especially the stakeholders as well as the organisations serving as information hubs for their respective sectors. Smaller exercises were conducted annually in the following years. The results and experience gained during those exercises were taken into consideration in White Papers on cybersecurity published by Curatorship Safe Austria in early summer of the following year, containing recommendations for the planned Austrian Cybersecurity Act, now the NISG.

Further cooperation is expected in the issuing of industry-specific recommendations according to the GDPR.

Insurance

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

Insurance against cybersecurity incidents, covering the costs of, for example, data recovery or downtime, are offered by every major insurer active in Austria. In detail, the covered risks of course vary from offer to offer, with some covering even in the case of negligence or fault.

Despite the availability, cybersecurity insurance is as yet far from common. This has not changed with the introduction of the NISG.

ENFORCEMENT

Regulation

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

Concerning the provisions of the General Data Protection Regulation (GDPR), the Data Protection Authority (DSB) is responsible for enforcing data security rules and penalising non-compliance in Austria.

According to article 83, para 4 GDPR, the DSB may impose a fine of up to €10 million or up to 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, on any business that has failed to implement the data security measures set forth in article 32 GDPR.

The prosecution of cybercrime is handled by the Cyber Crime Competence Centre (C4), which acts as a special unit of the Austrian Federal Police or the Austrian Federal Ministry for Internal Affairs, as the case may be. Therefore, the powers of the C4 equal those of the authority they represent.

It should be noted that breaches of the GDPR (thus, also a breach of the provision on data security measures) constitute an act of unfair competition under Austrian law. As a consequence, enterprises may call upon the courts if they accuse a competitor of breaching data privacy or data security provisions. In practice, owing to the very low fines the DSB has imposed in the few months since the GDPR has entered into validity despite much higher ones being possible by law, this poses the most relevant risk of litigation in the context of the GDPR.

The enforcement of the Network and Information Systems Security Act (NISG) is incumbent upon the Federal Government, the Federal Chancellor, the Federal Minister of Internal Affairs, the Federal Minister of National Defence and the Federal Minister for Europe, Integration and Foreign Affairs within the scope of their respective areas of responsibility. The regional administrative authorities are responsible for the prosecution of infringements of the NISG. They may impose a fine of up to €50,000 for each infringement (€100,000 in case of recurrence).

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

In the case of a data breach notification according to article 33 GDPR or an alleged breach of data security provisions, the DSB initiates formal proceedings in which it can request statements and documents from any company concerned. Should the DSB find that the company has failed to comply with or document the data security rules set forth in article 32 GDPR, the DSB, similar to Austrian courts, is entitled to base its decision on the facts at hand but it cannot force the company to disclose any further information.

The C4, on the other hand, has access to all measures available to the Austrian Federal Police or the Austrian Federal Ministry for Internal Affairs. Thus, they are, for instance, even able to have documents confiscated. Since they are limited to the prosecution of cybercrime; however, they may not use their powers to merely monitor compliance with or prosecute infringements of data security rules.

Regarding providers of critical infrastructure or digital services, article 17, paras 4 and 5 and article 21, para 4 NISG provide that, in case the Federal Minister of Internal Affairs becomes aware that providers of critical infrastructure or digital services have failed to meet their obligation to take suitable and adequate security measures, he or she is authorised to demand providers to submit evidence of the security measures taken, including evidence of certification or inspections and, if applicable, security deficiencies discovered. The Federal Minister of Internal Affairs is also authorised to ensure inspection of the network and information systems used for the provision of critical infrastructure or digital services as well as any relevant documents. For this purpose, he or she is entitled to authorise the entry for inspection of locations where network and information systems are located, after prior notification. However, such inspection shall only be carried out to the extent absolutely necessary and with the greatest possible protection of the rights of the affected provider and third parties.

In addition, the Federal Minister of Internal Affairs is authorised to issue recommendations regarding measures providers will have to take within a reasonable period of time, otherwise they will be ordered by notice.

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

Because of the current state of cybersecurity rules in Austria, no enforcement actions have been brought against the concerned companies by the Austrian authorities. While this most likely will change owing to the GDPR (the DSB has already fined companies for lacking technical and organisational measures, though not yet after cybersecurity incidents), changes are not expected to take place before binding and thus enforceable rules and guidelines exist. In the publicly known cybercrime cases, especially attacks by the hacktivist group Anonymous, Austrian police have prosecuted the participating persons with varying degrees of success. However, no enforcement measures have been taken against the companies and institutions whose IT systems have been breached. Rather, they have received support from cybersecurity organisations to better secure their systems for the future.

23 What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

Apart from industry standards and recommendations, the NISG obliges providers of critical infrastructure and digital services to immediately report any security incident concerning any essential or digital service they provide. The obligation on providers of digital services to report a security incident only applies if they have access to information needed to assess the impact of a security incident.

In this context, security incidents are defined by law as disruptions to the availability, integrity, authenticity or confidentiality of network and information systems that have led to a reduction in the availability, or failure, of the service operated with significant impact. In order to assess whether the impact is significant or not, the anticipated number of users affected, the duration, the geographical spread as well as the expected impact on economic and social activities have to be taken into account.

The GDPR also sets forth data breach notification requirements. According to the GDPR, the national data protection authorities need to be informed if the breach may result in a risk, no matter how small, to the rights and freedoms of a natural person. Such risks, however, may be avoided by appropriate technical and organisational measures (eg, pseudonymisation, encryption).

Penalties

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

Apart from court actions by competitors (a breach of the GDPR constitutes an act of unfair competition under Austrian law), according to article 83, para 4 GDPR the DSB may impose fines of up to €10 million or up to 2 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, for infringements of the GDPR.

Concerning violations of the NISG, the regional administrative authorities may impose fines of up to €50,000 (€100,000 in case of recurrence).

The prosecution of cybercrime is handled by the C4, which acts as a special unit of the Austrian Federal Police or the Austrian Federal Ministry for Internal Affairs, as the case may be. Therefore, the powers of the C4 equal those of the authority they represent.

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

The two data breach provisions in Austrian law are article 33 and 34 GDPR.

According to article 33, the controller has to notify the DSB without undue delay and not later than 72 hours after having become aware of a personal data breach. A notification may only be omitted in if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where a breach has occurred at a processor, he or she must notify the controller who will then notify the DSB.

Irrespective of whether a personal data breaches may result in a risk to the rights and freedoms of natural persons, and thus require notification to the DSB, or not, a controller is obliged to document each breach, comprising the facts relating to the personal data breach, its effects and the remedial action taken. This documentation has to be presented to the DSB upon request to enable the DSB to verify compliance with article 33.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller is furthermore obliged to notify the affected data subject, ie, the natural persons, without undue delay. However, appropriate remedial or technological measures (eg, a secure encryption of the personal data) may be considered to lower the risk enough to relieve controllers from the notification duty of article 34 GDPR. Unlike the former Austrian notification rule of the Austrian Data Protection Act 2000, the controllers may not omit notification of the data subjects in case that individual notifications would be considered disproportionate. Rather, they are now obliged to instead publicly communicate the personal data breach.

The DSB may review the controller's interpretation of the severity and possible consequences of an incident and oblige him or her to inform the data subjects or confirm that level of risk is sufficiently low for such notification to be omitted.

These provisions however only apply to breaches where personal data is affected. As a result, no notification requirement exists for cyberthreats or breaches where no personal data is involved (though the latter is statistically quite unlikely).

Article 83, para 4 of the GDPR allows the DSB to impose fines of up to €10 million or 2 per cent of the total worldwide annual turnover of the preceding financial year if the data breach notification and documentation requirements are not met.

The NISG introduced data breach notification requirements for providers of critical infrastructure and digital services that go beyond the scope of articles 33 and 34 GDPR. If these requirements are not met, fines of up to €50,000 pre-infringement (€100,000 in case of recurrence) may be imposed.

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

As a result of the lack of any specific rules on cybersecurity and the consequences of non-compliance, private redress can only be sought before civil courts following general tort rules. This means that any person seeking redress would need to claim a concrete amount for damages and also prove that the damages in the desired amount have actually been caused by the defendant.

Even in the case of a breach of data protection rules, parties would need to call upon civil courts for any redress as the DSB and the regional administrative authorities may only impose fines. Nevertheless, the decision of the DSB or a regional administrative authority would be required in such a case to determine whether a breach of data protection rules has occurred in the first place.

THREAT DETECTION AND REPORTING

Policies and procedures

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

Apart from industry standards and recommendations, article 32 of the General Data Protection Regulation (GDPR) requires any controller or processor of personal data to implement measures to ensure data security. However, such measures need to take into account the type, extent and purpose of the processed data, the state of the art and the economic feasibility. Therefore, even though this provision does stipulate minimum protective measures, it is not clear what the minimum requirements in each case may be. Further, this provision only applies to personal data rather than any type of data. As a result, in the field of cybersecurity, industry standards and the recommendations of the Austrian Computer Emergency Response Team (CERT) and Austrian Government Computer Emergency Response Team (GovCERT) are more important in Austria than legal rules. This is especially true for relatively new technology such as cloud computing, IoT or the issues associated with various forms of 'bring your own device'.

Also, recommendations and standards for appropriate technological and organisational measures defined by the European Commission, national data protection authorities and industry-specific organisations will, in the end, set forth the minimum requirements for cybersecurity any company will need to meet. Currently, however, except for individual rulings, the only binding rules and guidelines issued by the Austrian Data Protection Authority are two regulations on privacy impact assessments (PIA), one listing processing operations that do not require a PIA to be performed ('Exceptions from the PIA', DSFA-AV, published 25 May 2018) and one listing processing operations that in any case require a PIA to be performed (DSFA-V, published 9 November 2018).

Furthermore, providers of critical infrastructure have to take measures in order to ensure a high level of security of network and information systems according to articles 17, 21 and 22 of the Network and Information Systems Security Act (NISG).

According to articles 17, 21 and 22 NISG, appropriate measures need to take into account the state of the art and be appropriate to any risk that can be determined with reasonable effort. Therefore, providers of critical infrastructure will have to take into account the following: safety of systems and facilities; management of security incidents; business continuity management; monitoring; verification and testing; and compliance with international rules. The security measures should include: governance and risk management; dealing with service providers, suppliers and third parties; security structure; system administration; identity and access management; system maintenance and operation; physical security; detection and handling of security incidents; business continuity; and crisis management. These security measures are regulated in more detail in appendix 1 to the Network and Information Systems Security Ordinance.

In order to enable the verification of the measures taken, providers of critical infrastructure have to submit a list of the security measures they have carried out, including evidence of certification or inspections and, if applicable, security deficiencies discovered, to the Federal Minister of Internal Affairs at least every three years. The Federal Minister is also authorised to issue recommendations regarding measures providers will have to take.

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

As such records do not fall within the scope of Austrian legal rules on the keeping of documents (eg, contracts, invoices), the only applicable rules are article 32 GDPR and those determined by industry standards or recommendations, such as ISO/IEC 27001 (which can be obtained from the ISO or ASI against payment), the recommendations of the German Federal Office for Information Security and the recommendations of the CERT (available from their respective websites: www.bsi.bund.de and www.cert.at). These three can be regarded as the main industry standards and codes of practice in the field of cybersecurity.

In addition, comprehensive guidelines summarising the relevant rules and recommendations, as well as a checklist created specifically for very small enterprises, have been created by the Austrian Chamber of Commerce and can be obtained from their microsite www.it-safe.at.

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

Apart from industry standards and recommendations, the NISG obliges providers of critical infrastructure and digital services to immediately report any security incident concerning any essential or digital service they provide. The obligation of providers of digital services to report a security incident only applies if they have access to information needed to assess the impact of a security incident.

In this context, security incidents are defined by law as disruptions to the availability, integrity, authenticity or confidentiality of network and information systems that have led to a reduction in the availability, or a failure, of the service operated with significant impact. In order to assess whether the impact is significant or not, the anticipated number of users affected, duration, geographical spread and expected impact on economic and social activities have to be taken into account.

The GDPR also sets forth data breach notification requirements. However, according to the GDPR the national data protection authorities only need to be informed if the breach may result in a risk to the rights and freedoms of a natural person. Such risks, however, may be avoided by appropriate technical or organisational measures (eg, pseudonymisation, encryption).

Time frames

30 | What is the timeline for reporting to the authorities?

As of 25 May 2018, the date the GDPR entered into validity, companies need to notify the national data protection authority in case of any risk to the rights and freedoms of a natural person without undue delay and as far as possible within 72 hours after the person responsible has become aware of the breach; any delay has to be justified. If said risk is high, the natural person will also need to be notified. In addition, according to the NISG, providers of critical infrastructure and digital services are obliged to report security incidents without undue delay to the national computer emergency team, or if none has been set up or the incident occurred in a federal institution, to the GovCERT, which will immediately forward the report to the Federal Minister of Internal Affairs.

However, the obligation of providers of digital services to report a security incident only applies if they have access to information needed to assess the impact of a security incident.

In this context, security incidents are defined by law as disruptions to the availability, integrity, authenticity or confidentiality of network and information systems that have led to a reduction in the availability, or a failure, of the service operated with significant impact. In order to assess whether the impact is significant or not, the anticipated number of users affected, duration, geographical spread and expected impact on economic and social activities have to be taken into account.

If a security incident involving a provider of digital services affects one or more EU members, the Federal Minister of Internal Affairs or the competent computer emergency team has to inform the single point of contact (SPOC) in the affected state.

Reporting

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

According to article 34 GDPR providers are obliged to notify the affected data subject, ie, natural persons, in case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, without undue delay. However, appropriate remedial or technological measures (eg, a secure encryption of the personal data) may be considered to lower the risk enough to relieve providers from this notification duty. Unlike the former Austrian notification rule of the Austrian Data Protection Act 2000, the controllers may not omit notification of the data subjects in case that individual notifications would be considered disproportionate. Rather, they are now obliged to instead publicly communicate the personal data breach. The Data Protection Authority may review the controller's interpretation of the severity and possible consequences of an incident and oblige him or her to inform the data subjects or confirm that level of risk is sufficiently low for such notification to be omitted.

These provisions, however, only apply to breaches where personal data is affected. As a result, no notification requirement exists for cyberthreats or breaches where no personal data is involved (though the latter is statistically quite unlikely).

The NISG, on the other hand, does not provide any reporting obligations to others in the industry, customers or the general public.

UPDATE AND TRENDS

Update and trends

32 | What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

After the entry into effect of the General Data Protection Regulation (GDPR), currently the biggest legal challenge businesses are facing is the increased focus of the data protection authorities on accountability for the technical and organisational measures implemented. Thus, where the lenient treatment of infringements and lax cybersecurity in 2018 led many companies to consider their implementation of the GDPR rules as future-proof, a sharp increase in fines in 2019 caused a trend in re-evaluating the existing measures. The sometimes forced and hurried implementation of conferencing and collaboration solutions by many Austrian companies to enable work to continue during the covid-19 related lockdowns created another potential problem, not only in regard to data protection, but also in regard to IT security.

A further open question is the impact of the relatively recent NIS Act (the Austrian transposition of the EU Directive on Security of Network and Information Systems (NIS Directive)) on cybersecurity best practices solutions. While, in principle, it is only binding for providers of critical infrastructure, decisions and recommendations on best practices are also expected to influence measures taken by other, non-critical businesses. Such decisions and recommendations are, however, slow in coming.

Coronavirus

33 | What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programmes, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

Covid-19 has posed, and still does pose, a significant challenge for companies. One of the main issues they have faced was keeping their offices and businesses operational, first during lockdown and afterwards with strict distancing rules in force. As a solution, many companies have, sometimes hurriedly, implemented software solutions for tele- and collaborative working, enabling their employees to (also) work from home. Originally, Austrian social security law was very strict regarding home offices, requiring employers and employees to not only specify in writing the address, but also the exact room from which the work would take place. Without such a specific agreement, any accident occurring in a home office would not be regarded and insured as a work accident.

This rule was amended after the onset of the covid-19 pandemic, originally until 31 March 2021, requiring only the home office address to be specified. On 27 January, the Austrian government announced that, after lengthy discussions with organisations representing employees and employers, an agreement had been reached on amending employment law to, for the first time, specify rules on home offices. Among others, the as yet temporary change requirement to only specify the home office address is to be made permanent. The amendments may enter into force as soon as early March or April.

This change, which actually does not contain any rules on technology itself (and none are currently expected from the upcoming amendments to employment law), has thus not only made home offices in Austria practically feasible but also enabled companies to make heavy use of communication and collaboration solutions intended for remote

and teleworking. It can, therefore, be regarded as the most important, but as yet temporary, change affecting the use of digital and remote technology in Austria. This should, in principle, also proportionally raise the demand for security technology, either by means of secure implementation into IT infrastructures or licensing of appropriate add-on solutions. Unfortunately, this is not the case in practice. Thus, while the demand for cybersecurity consultancy and solutions did rise, the number of potential cybersecurity risks rose even more.

Other amendments are more specific and, as a common feature, enable the use of communication technology where previously a physical presence was required. These changes affect, for example, shareholders' meetings, court hearings (except for criminal proceedings) and identification processes in banking. However, these changes are (still) intended to be temporary, and are currently limited until 30 June 2021.

A programme that was not created as a result of covid-19, but has proved quite important due to it, is the 'Vienna digital' programme of the city of Vienna. Within the scope of the programme, small and medium-sized enterprises with up to 250 employees could receive funding of 30 per cent of their investments in remote working technology, including cybersecurity measures. Owing to the sudden and increased implementation of such technologies during the covid-19 pandemic, however, the subsidies, which should have lasted well into 2021, were used up by March 2020. In the meantime, this programme has been relaunched.

MGLP
RECHTSANWÄLTE | ATTORNEYS-AT-LAW

Árpád Geréd
a.gered@mglp.eu

Museumstraße 5
1070 Vienna
Austria
Tel: +43 1 997 19 66
www.mglp.eu

Other titles available in this series

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

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-643-3