Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

Germany: Law & Practice

Thomas Jansen and Philip Kempermann
Heuking Kühn Lüer Wojtek

practiceguides.chambers.com

GERMANY

Law and Practice

Contributed by:
Thomas Jansen and Philip Kempermann
Heuking Kühn Lüer Wojtek see p.26

Contents

1. Basic National Regime

1.1 Laws

- Issues relating to the protection of personal data are regulated in the General Data Protection Regulation (GDPR), the German Federal Data Protection Act (*Bundesdatenschutzgesetz*, or BDSG) and in sectoral laws (ie, the Banking Law, the Energy Law, etc).
- Issues relating to the protection of personal data and privacy in electronic communications are regulated primarily in the Telecommunications Act (*Telekommunikationsgesetz*, or TKG) and in the Telecommunications and Telemedia Data Protection Act (*Telekommunikation-Telemedien-Datenschutzgesetz*, or TTDSG) as a result of the implementation of the E-Privacy Directive. These issues will be regulated by the E-Privacy Regulation, once it comes into force.
- The implementation of Directive (EU) 2016/1148 (NIS Directive) resulted in the amendment of various German laws, including the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, or BSIG) and the Energy Industry Act (*Energiewirtschaftsgesetz*, or EnWG).
- The EU Cybersecurity Act (Regulation (EU) 2019/881) provides a framework for EU-wide certification of information and communication technology (ICT) products, services and processes.
- The German Criminal Act (*Strafgesetzbuch*, or StGB) lays down penalties for data espionage, phishing, acts preparatory to data espionage and phishing, data tampering, computer sabotage and computer fraud.

It is further worth noting that on 15 September 2022 the EU Commission published the EU Cyber Resilience Act, which is the first ever EU-wide legislation that introduces mandatory cybersecurity requirements for software and connected hardware throughout their entire lifecycle. The proposed act directly impacts the manufacturers and retailers of any software and connected hardware, proposing various obligations upon them. One of its key takeaways is the obligation to adopt "cybersecurity by design", meaning that cybersecurity will have to be taken into account in the planning, design, development, production, delivery and maintenance phases.

The new obligations introduced in this act aim to ensure that cybersecurity is a key aspect in all design decisions that are made during a product development lifecycle. Although the act is still in its drafting stages, it worth keeping an eye on the manner in which it develops.

Differences Between Data Breach Incidents and Cybersecurity Incidents

A data breach incident is one that results in a violation of statutory provisions regarding the protection of personal data. The aim of data protection laws, such the GDPR, the BDSG or the data protection laws of the German federal states, is mainly to protect the general personal rights of the natural persons concerned.

In contrast to data protection, cybersecurity is about protecting data, regardless of whether it is personal or not. The term cybersecurity therefore also includes data which is not considered personal data.

Cybersecurity is about countering security risks and protecting data from, for example, manipulation, loss or unauthorised access and the measures that must be taken to protect the data against those risks.

Penalties

Infringements of the provisions set out in the German Data Protection Act and the GDPR with respect to cybersecurity are subject to administrative fines of up to EUR10 million or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The TKG and EnWG provide for fines of up to EUR100,000, while the BSIG provides for fines of up to EUR50,000. (If operators of public telecommunications networks do not submit the mandatory security concept to the Federal Network Agency immediately after the start of network operation, they are threatened with a fine of up to EUR100,000 under the TKG. Violations of the notification obligation are punishable with fines of up to EUR50,000 under the TKG. For non-compliance and in the case of disregard of the reporting obligations, the EnWG provides for fines of up to EUR100,000 and the BSIG for fines of up to EUR50,000.)

The penalties provided for by the StGB range from a fine to a prison sentence of up to five years (for computer fraud).

The penalties provided for within the scope of the EU Cyber Resilience Act, are comparable to those of the GDPR and fines for non-compliance with basic safety requirements can amount to up to EUR15 million or 2.5% of the previous year's worldwide group annual turnover, whichever is greater. For violations of other obligations, the limits are EUR10 million or 2% of the worldwide consolidated annual turnover of the previous year.

1.2 Regulators

Data Protection Authorities

In addition to the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*, BfDI), each federal state has data protection authorities. Each supervisory authority has powers of approval, advice, investigation and remedy. They conduct investigations into the application of the GDPR, including on the basis of information received from another supervisory authority or other public authority. They may also initiate legal proceedings.

National Cyber Defence Centre (Nationales Cyber-Abwehrzentrum, or Cyber-AZ)

The Cyber-AZ was established to optimise operational co-operation between various authorities and to co-ordinate protection and defence measures.

The following authorities are currently represented in the Cyber-AZ: the Federal Office for Information Security (BSI), Federal Criminal Police Office (BKA), Federal Police (BPol), Federal Office for the Protection of the Constitution (BfV), Federal Intelligence Service (BND), Federal Office for Military Counterintelligence (BAMAD), Federal Office of Civil Protection and Disaster Assistance (BBK), German Armed Forces (BW) and Federal Financial Supervisory Authority (BaFin).

In the Cyber-AZ, details on cyber-attacks on information infrastructure is compiled, evaluated and consolidated. This allows all authorities to benefit from the shared knowledge.

German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, or BSI)

In 1991 Germany established the BSI. The office provides security advice to users and standards for public and private bodies. The guiding principle of the BSI is: "As the federal cybersecurity authority, the BSI shares information security in digitisation through prevention, detection and reaction for the state, economy and society."

Federal Criminal Police (Bundeskriminalamt, or BKA)

As the central office of the German police, the BKA assumes responsibility for co-ordinating tasks in the area of cybercrime, provides information and tools, and is the hub for international co-operation. Furthermore, the BKA conducts investigations in the area of cybercrime within the scope of its responsibilities: for example, if federal authorities, institutions or security-sensitive units of vital institutions are affected, the BKA is usually in charge of the investigations.

Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, or BfV)

The BfV monitors and analyses the activities of foreign governments and states, directed against Germany and supports threatened agencies and victims of cyber-attacks.

UP KRITIS

The UP KRITIS is a public-private co-operation between operators of critical infrastructure, their associations and the responsible government agencies. The central objective of UP KRITIS is to maintain the supply of critical infrastructure in Germany. UP KRITIS is a cross-sector co-operation platform for IT security between operators of critical infrastructure and their supervisory authorities. The BSI provides all participants in the UP KRITIS with information and warnings on IT security. In addition, the operators and authorities in the working groups exchange information about new challenges in the area of IT security in critical infrastructure and possible solutions for these, as well as developing recommendations for this purpose. The UP KRITIS working groups are also used to develop industry-specific security standards. These serve as guidelines for implementing the legal requirements of the BSIG.

Economic Protection Initiative (Initiative Wirtschaftsschutz)

The Economic Protection Initiative has established itself as an umbrella organisation for a holistic economic protection model against digital or non-digital attacks – supported by all relevant state and economic players. In this alliance, the leading business associations as well as the security associations work together effectively with the security authorities, for the defence against concrete threats, especially from industrial espionage and white-collar crime.

German Competence Centre Against Cyber Crime (G4C)

The G4C is an independent, operational association and its members include various companies (especially banks). The BKA and BSI are co-operative partners of the G4C. It develops assistance, methods and recommendations for prevention of cybercrime based on the exchange of information about cybercrime phenomena.

Central Office for Information Technology in the Security Sector (Zentrale Stelle für Informationstechnik im Sicherheitsbereich, or ZITiS)

The Central Office for Information Technology in the Security Sector is an unincorporated federal agency under the authority of the Federal

Ministry of the Interior and Community. ZITiS is responsible for supporting and advising federal authorities with security tasks, in relation to information technology capabilities. For this purpose, the central office develops and researches methods and tools.

Computer Emergency Response Team for Federal Authorities (CERT-Bund)
The CERT-Bund is the central contact point for preventative and reactive measures in the event of security-relevant incidents in computer systems. It serves as a warning and information service for authorities and private internet users. It provides information about security leaks in software, provides a weakness indication (green/yellow/red) for commonly used software and lists present and past security holes.

1.3 Administration and Enforcement Process

The supervisory data protection authorities have powers of investigation and remedy. They conduct investigations on the application of the GDPR, including on the basis of information received from another supervisory authority or other public authority. They may also initiate legal proceedings.

They may use the following methods for their investigation purposes:

- on-the-spot checks on individual companies;
- dispatch of questionnaires; and
- automated online audits.

In general, data protection authorities tend to visit larger companies or those companies whose processing operations are likely to result in a high risk to the rights and freedoms of data subjects. Small and medium-sized enterprises are usually only marginally controlled by the authorities so as not to overburden them financially and in terms of personnel.

Companies that have received fines can file objections and take legal action.

Differences Between Personal Data Security Incidents and Other Cybersecurity Events
In the event of a personal data security incident, companies/institutions must report the incident to the competent authority (see **1.2 Regulators**). This is the essential difference from a security event. In principle, a personal data security incident is always also a cybersecurity event, whereas a cybersecurity event is not necessarily a personal data security incident.

1.4 Multilateral and Subnational Issues

Each federal state has its own data protection authorities and its own data protection laws, which do not contradict the federal or EU laws, but partly extend them. A federal state's data protection law only applies to that state's public bodies.

A good example of the manner in which EU laws have been implemented at the national level is the German NIS Directive Implementation Act (the "Implementation Act") which came into effect on 30 June 2017 as a transposition of the EU Network and Information Systems Directive (EU 2016/1148 (Directive)). The Implementation Act amended the BSIG, the Atomic Energy Act (*Atomgesetz*), the EnWG, the Social Security Code V (*Sozialgesetzbuch V*), and the TKG. The key requirements laid out in the Directive, had, however, already been part of the German IT Security Act (ITSA) which amended the BSIG before the Implementation Act. Therefore, the ITSA assumed the role of "pace-setter" for the Directive. As a consequence of the ITSA, the

changes required to be made to the German law resulting from the Directive were relatively small.

The Act to Increase the Security of Information Technology Systems (IT Security Act 2.0) came into force on 28 May 2021. This new act is aimed at strengthening the position of the BSI, heightened consumer protection, stronger precautionary corporate obligations and reinforcing the state's protective functions.

1.5 Information Sharing Organisations and Government Cybersecurity Assistance

The tasks of the BSI include:

- protection of federal networks, detection of and defence against attacks on government networks; and
- warning of malware or security holes in IT products and services.

The CERT-Bund informs about security leaks in software and lists present and past security holes.

Alliance for Cybersecurity

An example in this context is the Alliance for Cybersecurity (ACS), which provides companies with up-to-date information on the threat situation in cyberspace as well as practical assistance for the design and implementation of suitable protective measures. Membership is open to all companies and institutions having their headquarters/branch office in Germany. Several thousand companies and institutions have already joined the initiative, which was launched in 2012 by the BSI and the digital association Bitkom, making the Alliance for Cybersecurity a successful model for building trust and profitable co-operation between government and industry in the field of cybersecurity.

Member companies benefit from the expertise of the BSI and their ACS partners, the exchange of knowledge and experience with other companies and institutions on granular topics of cybersecurity and partner services, which in turn increases cybersecurity proficiency within member companies. Furthermore, companies that possess pre-existing expertise in the field of cybersecurity have the opportunity of becoming partners in the ACS to contribute to the network.

The Alliance for Cybersecurity's extensive information offering includes BSI recommendations on topics such as the secure configuration of software products, securing systems for manufacturing and process automation, and monitoring and detecting network anomalies.

Cybersecurity Council Germany e.V.

In August 2012, the Cybersecurity Council Germany e.V. was founded by well-known personalities. The Berlin-based association is politically neutral and aims to advise companies, authorities and political decision-makers in the field of cybersecurity and to strengthen them in the fight against cybercrime.

The members of the association include large and medium-sized companies, operators of critical infrastructure, numerous federal states, local authorities as well as experts and political decision-makers with an interest in cybersecurity. Through its members, the association represents more than three million employees from the industry and almost two million members of other associations and societies.

The Cybersecurity Council Germany e.V. pursues the following goals:

- intensification of the co-operation between politics, public administration, business and science to improve IT protection;
- initiatives and projects to promote awareness of cybersecurity;
- establishment of a Germany-wide cybersecurity network in a European and international context; and
- establishment of a knowledge platform, forum and network for association members.

Member companies are integrated into the council-network, which includes decision-makers in the field of politics, economics, science and society. Members are also integrated into an international network of leaders and heads of cybercommunities. Private member companies are afforded representation of their corporate interests in the political field of cybersecurity.

1.6 System Characteristics

With the introduction of the GDPR, the EU was the first polity to introduce new regulations in the area of data protection and security of personal data. Furthermore, the regulations apply in a supranational manner throughout the entire EU and other countries use the GDPR as the foundation of their own laws on data security.

The Second EU Data Protection Adaptation and Implementation Act (2.DSAnpUG – EU), was passed in 2019 in order to amend a total of 154 pre-existing laws in an "omnibus process" to further harmonise German data protection legislation with the GDPR. The vast majority of changes under the omnibus act involved aligning the terminology in German federal legislation with the terms used in the GDPR.

Germany also introduced the BSIG before the EU addressed similar topics with the NIS Directive. However, in certain areas, Germany's federal structure can lead to delays and a patchwork of laws and authorities.

The protection of critical infrastructure enjoys special attention because it is particularly at risk in the context of cybersecurity. The central security requirements for critical infrastructure are set out in the IT Security Act (*IT-Sicherheitsgesetz*, or IT-SiG) and the BSI Criticality Ordinance (*BSI-Kritis-Verordnung*, or BSI-KritisV). The central provision for operators of critical infrastructure is Section 8a of the BSiG which defines the particular organisational and technical precautions KRITIS operators must take and implement appropriately to ensure the security of their IT and processes and provide evidence of this. It also regulates the obligation to report security incidents.

Many operators of critical infrastructure use industrial control systems (ICS) to comply with these special provisions. In contrast to traditional IT, ICS have different requirements for the protection goals of availability, integrity and confidentiality. This manifests itself, for example, in longer operating times and infrequent maintenance windows. The BSI has published an ICS security compendium which defines basic principles for IT security in ICS.

1.7 Key Developments

Implementation of the New Standard Contractual Clauses

Within the European Economic Area, data can be transferred freely as this transfer is subject to the GDPR. In countries outside the European Economic Area a level of data protection appropriate to the GDPR must be ensured by other means. Typically, this is done by concluding standard contractual clauses (SCC) pursuant to Article 46 paragraph 2(c) of the GDPR, which are provided by the European Commission in

the form of model contracts. With Implementing Decision 2021/914 of 4 June 2021, the Commission published new model contracts. The new templates are not only to be used for new contracts but all existing contracts must also be adjusted accordingly or replaced by 27 December 2022 at the latest.

Data Transfer to the USA

The SCC innovation described in the section above must also be taken into account when transferring data to the USA. However, additional action is required as the European Court of Justice ruled in its judgment of 16 July 2020 (Case C-311/18, Schrems II) that the conclusion of SCCs by itself is not sufficient to ensure an adequate level of data protection in the USA; in particular, the performance of a so-called "transfer impact assessment" is required. On 1 December 2021 (Az. 6 L 738/21), the Wiesbaden Administrative Court prohibited the use of a cookie banner, if there is a US connection.

The Telecommunications-Telemedia Data Protection Act

On 1 December 2021, the Telecommunications and Telemedia Data Protection Act (TTDSG) came into force, essentially combining the data protection provisions from the former versions of the TKG and TMG.

The TTDSG contains provisions for data privacy in telecommunications and telemedia. Adjustments required due to the GDPR and the E-Privacy Directive were implemented. Among other things, the TTDSG also contains new provisions on digital estate, privacy protection for terminal equipment, consent management and data protection supervision.

1.8 Significant Pending Changes, Hot Topics and Issues

The broad spectrum of applicable law closes many of the security gaps in cyberspace. But the growing number of cyber-attacks makes it clear that security standards must be continuously adapted to the changing risks. A further issue is that the rules on cybersecurity are not condensed into one cybersecurity act, but are spread among numerous different laws. This poses profound challenges for companies to determine which legal framework applies to them.

Ransomware

Ransomware is, nowadays, marketed by cybercriminals in a manner similar to the marketing of regular software and they have thus created a business model. Ransomware can be purchased for licence fees, even including technical support. This market is likely to continue to grow. In order to address such increased risk, companies must respond proactively and invest more in training and awareness for their employees and in securing their technical infrastructure.

Supply Chain Vulnerabilities

Cybercriminals are increasingly targeting large companies in ransomware attacks: in particular, those that produce particularly sought-after and rare goods in the global supply chain crisis.

The case of the American IT service provider Kaseya also shows how hackers are trying to expand the power of their attacks. The criminals had gained access to a program offered by Kaseya, which is used by companies to manage and roll out their software updates. In this way, they managed to encrypt the systems of over a thousand companies in order to extort a ransom.

Impact of the SolarWind Hack in Germany
In December 2020, a US-based tech company was the victim of a sophisticated large-scale cyber-attack. The attack had far-reaching implications on international users of the company's software. This included multiple German ministries and federal offices that used or had used the software. The hack clearly revealed the prevalence of security gaps and insufficient attention to IT security.

Due to the complexity of modern IT systems and the comparatively low cost of carrying out attacks of this nature, the threat of vector attacks on software supply chains is expected to gain importance in the coming years. Furthermore, traditional security mechanisms will need to be supplemented with more refined policies for detection of malicious changes in code.

2. Key Laws and Regulators at National and Subnational Levels

2.1 Key Laws

The key cybersecurity laws, as opposed to the cybersecurity-related provisions of general criminal law, are:

- the BDSG provides cybersecurity requirements and sanctions when personal data is involved;
- EU Directive 2016/1148 of 6 July 2016 provides specific requirements for networks and information systems for operators of essential services and digital service providers; Germany implemented the directive by amending the BSIG and the EnWG;
- the Cybersecurity Act provides requirements for European cybersecurity certification schemes with respect to ICT products, ICT services and ICT processes in the EU;
- EU Directive 2015/2366 of 25 November 2015 on Payment Services 2 (PSD2) sets out provisions for information systems of payment service providers (PSPs);
- EU Regulation 2017/745 applies to medical devices that include software components;
- the German IT Security Act provides certain security standards and reporting requirements for the operators of critical infrastructures; and
- the TKG regulates the protection of personal data and privacy in electronic communications; however, it will be replaced by the E-Privacy Regulation.

German Criminal Act (StGB)
Any unlawful alteration, deletion, suppression or rendering unusable of external data fulfils the facts of the case according to Section 303a of the StGB (data alteration). In particularly serious cases, this is also punishable under Section 303b I No 1 of the StGB ("computer sabotage") and is punishable by imprisonment of up to five years or a fine. Since 2007, distributed denial-of-service (DDoS) attacks have also constituted computer sabotage; the same applies to any action that causes damage to an information system that is essential to another.

Spying on data (Section 202a, StGB) – ie, gaining access to external data that is specially protected against this – is punishable with a prison sentence of up to three years or a fine. Intercepting foreign data in networks or from electromagnetic radiation has also been a punishable offence since 2007. In contrast to Section 202a of the StGB, no special access protection is required here. Procuring, creating, distributing, making publicly accessible, etc, so-called hacker tools has also been a punishable offence since 2007, if a criminal offence is prepared with them (Section 202c, StGB).

According to Section 202a paragraph 2 in conjunction with paragraph 1 of the StGB, data is only protected from being spied on if it is "specially secured" in order to prevent the offence from escalating. This means that only in case users protect their data by technical means do they enjoy protection under criminal law. The earlier debate as to whether "hacking" without retrieving data is punishable under criminal law is no longer relevant since the wording of Section 202a paragraph 1 of the StGB was changed in 2007 in such a way that criminal liability begins as soon as access to data is gained. It is also disputed whether encryption is part of special security. Although it is very effective, it is argued that the data is not secured, but is only available in an "incomprehensible" or simply "different" form.

Computer fraud is punishable under Section 263a of the StGB with a fine or imprisonment for up to five years if data processing operations are manipulated to obtain financial gain. Even the creation, procurement, offering, safekeeping or transfer of suitable computer programs is punishable.

2.2 Regulators

Please see **1.2 Regulators**.

2.3 Over-Arching Cybersecurity Agency

ENISA

The European Network and Information Security Agency (ENISA) was created in 2004. The objective of ENISA is to serve as a contact point and centre of expertise for the member states and the institutions of the European Union on issues related to network and information security. Its activity consists of:

- anticipating future network and information security challenges and assisting the European Union in responding to them, by collecting, compiling, analysing and publishing relevant information and expertise on crucial issues regarding network and information security, taking into account the developments in the digital environment;
- supporting EU member states and EU institutions in developing and implementing the strategies necessary to meet the legal and regulatory requirements for national information security and thereby promoting the significance and need for network and information security;
- supporting the EU in building and developing state-of-the-art network and information security capacities and in its continuous adaptation to the latest trends; and
- strengthening the co-operation between EU member states and between national institutions to ensure network and information security.

ENISA also publishes reports and studies on cybersecurity: for example, on privacy, cloud security or the detection of cyber-attacks.

ENISA's main target groups are public sector organisations, in particular:

- the governments of the EU member states; and
- the institutions of the EU.

The Agency also provides support to:

- the ICT industries (telecommunications, internet service providers and IT companies);
- enterprises in general, especially small enterprises;
- network and information security professionals (eg, IT emergency teams);
- academic circles; and

• the public at large.

The European ENISA Regulation 2019/881 (Cybersecurity Act), adopted on 17 April 2019, grants a permanent mandate to ENISA and broadens its powers. ENISA has been made responsible for drafting the European Certification Schemes for Cybersecurity. These are to serve as a basis for the certification of products, processes and services that support the provision of the digital single market.

The BSI

The BSI acts in an advisory capacity to the business community and supports companies of all sizes and from all industries in questions of IT and information security. The objective of the BSI is the preventative promotion of information and cybersecurity in order to enable and promote the secure use of information and communication technology in the state, economy and society.

At federal level, the BSI is also responsible for the protection of critical information infrastructures (KRITIS).

In addition to its advisory function, the BSI cooperates with the business community in a variety of ways. For example, co-operation in the area of certification has long been established. Through the independent testing of IT products and services, the BSI offers manufacturers an opportunity to ensure transparency and more trust in the IT security features of their products and services.

The tasks of the BSI also include:

- protection of federal networks, detection and defence of attacks on government networks;
- testing, certification and accreditation of IT products and services;
- warning of malware or security gaps in IT products and services;
- IT security consulting for the federal administration and other target groups;
- information and awareness raising of citizens on IT and internet security;
- development of uniform and binding IT security standards; and
- development of cryptosystems for federal IT.

2.4 Data Protection Authorities or Privacy Regulators

Please see **1.2 Regulators**.

2.5 Financial or Other Sectoral Regulators

Aspects of cybersecurity are handled by the authorities listed under **1.2 Regulators**. Additionally, the Federal Institute for Financial Institutions and Insurances (*Bundesanstalt für Finanz- und Versicherungsaufsicht*, or BaFin) publishes the MA-Risk, which contains procedural and security requirements to be considered by banks, payment service providers and insurers.

2.6 Other Relevant Regulators and Agencies

TeleTrusT

The Federal Association for IT Security (TeleTrusT) is a competence network comprising of domestic and foreign members from industry, administration, consulting and science as well as thematically related partner organisations. Due to the broadly diversified membership and the partner organisations, TeleTrusT embodies the largest competence network for IT security in Germany and Europe. TeleTrusT offers forums for experts, organises events or participations in events and gives its opinion on current issues of IT security.

For additional information, please see **1.2 Regulators**.

3. Key Frameworks

3.1 De Jure or De Facto Standards

In Germany, the operators of critical infrastructures are obliged by the IT Security Act to comply with certain security standards and reporting requirements. This law was modified to comply with the requirements of the Directive (EU) 2016/1148 (the "NIS Directive"). On 16 January 2023, the Directive (EU) 2022/2555 (the "NIS 2 Directive") came into force. As a result, the IT Security Act has to be amended to comply with the NIS 2 Directive by 17 October 2024.

However, many companies have chosen to voluntarily comply with the ISO/IEC 27001 and ISO/IEC 27018 standards, as this is a good way to improve cybersecurity. The Federal Network Agency (*Bundesnetzagentur*, or BNetzA) even explicitly ordered ISO 27001 certification for electricity and gas network operators in its IT security catalogue by 2018. Furthermore, BaFin also refers to common IT standards such as ISO 27001 or the BSI basic protection catalogues in its minimum requirements for risk management.

Further, on 8 February 2023 the International Organization for Standardization (ISO) adopted ISO 31700, which relates to privacy-by-design principles. The new standard does not require conformity immediately. Instead, the standard features 30 requirements and guidance on privacy-by-design principles to enable consumers to "enforce their privacy rights, assigning relevant roles and authorities, providing privacy information to consumers, conducting privacy risk assessments, establishing and documenting requirements for privacy controls, how to design privacy controls, lifecycle data management, and preparing for and managing a data breach." It can therefore safely be assumed that ISO 31700 will set the benchmark for privacy by design across the globe.

As part of its IT Basic Protection Compendium, the BSI offers guidance on the creation of systematic policies for dealing with security breaches in the section entitled "Detection and Reaction". These steps walk companies through the task of preparing their own incident information security management policies and establishing minimum requirements, including for (i) determining responsibilities and contact persons, (ii) setting minimum standards for internal and external communication relating to security incidents, (iii) remedying security breaches and (iv) re-establishing the operating environment post-breach. Additionally, the BSI guidance provides an overview of what it considers to be the best practice when responding to security breaches.

In addition to the BSI standards and recommended practices, international norms such as ISO/IEC 27001:2013 represent recognised standards for IT security management systems. The more recent ISO/IEC 27035:2016, which builds upon both the former version and on ISO/IEC 27002:2013, also provides a structured standard that is specifically tailored for responses to cybersecurity incidents.

The Federal Crime Office also provides a series of recommendations for companies in a leaflet entitled "Cybercrime: Recommended actions for businesses", which similarly recommends employee training courses and the establishment of internal procedures prior to breaches, as well as the documentation and collection of information after being the subject of a cybercrime to aid with the investigation. Further exam-

ples of measures recommended by the Federal Crime Office include the installation of a filter to prevent DDoS attacks and the isolation of network areas that are the subject of attacks.

Nevertheless, it is usually helpful to develop a framework specifically tailored to the company. For this purpose, sources such as COBIT, NIST and SANS20 should be consulted. These current frameworks for cybersecurity can therefore serve other companies as "idea generators" for the design of internal processes. As an "ISMS-light approach", small and medium-sized companies can be recommended to use, for example, the "VdS 3473", which usually represents a preliminary stage for a possible ISO/IEC 27001 and BSI IT-basic-protection certification.

3.2 Consensus or Commonly Applied Framework

Please see **3.1 De Jure or De Facto Standards**.

3.3 Legal Requirements and Specific Required Security Practices

The Control and Transparency Act

Pursuant to the Control and Transparency Act (*Gesetz zur Kontrolle und Transparenz im Unternehmensbereich*, KonTraG), which came into force on 27 April 1998, the management of a company is obliged to implement a system for the early identification of developments and risks threatening the continued existence of the company.

The Stock Corporation Act

The German Stock Corporation Act (*Gesetz betreffend die Gesellschaften mit beschränkter Haftung*, GmbHG) stipulates that the management board shall be personally liable if it fails to monitor developments that could pose a risk to the company in the future by means of risk management and take appropriate measures to prevent them (Section 91(2) and Section 93(2) of the German Stock Corporation Act). Virtually the same requirements apply in the following cases.

- The managing director of a GmbH must exercise the diligence of a prudent businessman in the affairs of the company (Section 43 paragraph 1, GmbHG); this admittedly rather ambiguous stipulation contains in legal practice very similar consequences for risk management as for executive board members according to the German Stock Corporation Act.
- Other types of corporate entities, such as the general partnership or the limited partnership, are in fact on an equal footing with corporations with regard to the legal obligations for IT security if they do not have a natural person as a personally liable partner (the "Corporations and Co-Directives Act" (*Kapitalgesellschaften- und Co- Richtlinie- Gesetz*, or KapCoRiLiG)).
- If the management or the management board – as the person responsible – does not comply with the above-described risk provisioning obligation and if the company suffers financial damage as a result, this can lead to personal liability of the members of the management board and the management, and possibly also of the members of the Supervisory Board (Section 116, AktG).
- If the management of a company does not undertake the technical and organisational measures necessary to implement and maintain an appropriate level of IT security (eg, information security plans or programmes and business continuity plans), then in view of the expected damages, which could potentially even trigger an insolvency of the company, there is a high risk that such behaviour will result in a personal liability of the management of the company.

- Article 33 of the GDPR provides that, in the event of a breach of the protection of personal data, the controller must notify the competent supervisory authority without delay and, if possible, within 72 hours; to facilitate notification, the supervisory authorities have set up extensive input masks that can be processed online.
- Notification may only be dispensed with if the violation "is not likely to pose a risk to the rights and freedoms of natural persons". However, when processing data on behalf of a contractor, the contractor must immediately inform the responsible party ("controller") about the data breach and support the responsible party in reporting the data breach by providing the responsible party with the information available to him (Article 28 paragraph 3(f), GDPR).
- Where the breach of the protection of personal data is likely to present a high risk to the personal rights and freedoms of natural persons, the controller shall notify the data subject of the breach without delay (Article 34 paragraph 1, GDPR).
- In the event of a data breach, each party involved must know who to contact for rapid action and the controller must know exactly what needs to be done in which case; in this regard, it is advisable to compile a crisis document and keep it up to date. This should contain:
  (a) examples of possible data breaches, sorted by severity;
  (b) necessary next steps, short and concise procedure;
  (c) tasks of the responsible employees;
  (d) contact details of the competent supervisory authority and contact person; and
  (e) text modules for information to the persons concerned or necessary places.

Data Protection Officers

The GDPR establishes the concept of the data protection officer (DPO) at European level. The obligation to appoint a data protection officer affects companies according to their core activities: ie, activities that are essential for achieving the company's objectives. If these include the processing of sensitive personal data on a large scale or a form of data processing that has particularly far-reaching consequences for the rights of the data subjects, a DPO must be appointed.

There are two ways for groups and companies to fulfil their obligation to appoint a DPO. Either they appoint an employee as internal DPO or an external DPO is appointed.

The tasks of the data protection officer include:

- ensuring compliance with all relevant data protection regulations;
- the monitoring of certain processes, such as a data protection impact assessment; and
- raising awareness and training of staff and co-operation with the supervisory authority.

Nevertheless, the company itself remains responsible for compliance with data protection regulations. Failure to appoint a company DPO constitutes an administrative offence subject to a fine.

As stated above, the management of a company is obliged to implement a system for the early identification of developments and risks threatening the continued existence of the company; this includes measures such as internal risk assessments, vulnerability scanning and penetration tests.

Privacy Impact Assessments
Furthermore, Article 35 of the GDPR introduced the instrument of a privacy impact assessment (PIA) or data protection impact assessment (DPIA). A PIA or DPIA must always be conducted when the processing could result in a high risk to the rights and freedoms of natural persons. The Article 29 Working Party published a list of ten criteria that indicate that the processing bears a high risk to the rights and freedoms of a natural person.

In the course of a PIA or DPIA, the effects of data processing on data subjects must be evaluated and effective IT security measures established. Operators of critical infrastructures even have to implement preventative protection measures according to the "state of the art" in order to protect the critical infrastructure from a cyber-attack.

3.4 Key Multinational Relationships
ENISA provides practical advice and solutions to the public and private sector institutions of member states and to EU institutions. Please see **2.3 Over-Arching Cybersecurity Agency** for additional information.

4. Key Affirmative Security Requirements

4.1 Personal Data
Article 32 of the GDPR provides security requirements for the processing of personal data. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In this process they shall take into account various aspects, such as: the state of the art; the costs of implementation; the nature, scope, context and purposes of processing; as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The technical and organisational measures may include pseudonymisation and encryption or regular testing, assessments and evaluations of the effectiveness of the technical and organisational measures. What constitutes an appropriate level of protection arises, inter alia, from the risks represented by the processing, in particular by destruction, loss or alteration, whether accidental or unlawful, or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

For additional information, please see **3.3 Legal Requirements and Specific Required Security Practices**.

4.2 Material Business Data and Material Non-public Information
Please see **3.1 De Jure or De Facto Standards** and **3.3 Legal Requirements and Specific Required Security Practices**.

4.3 Critical Infrastructure, Networks, Systems
Pursuant to Section 8 of the BSIG, operators of critical infrastructures must implement IT security in accordance with the "state of the art" and regularly demonstrate compliance with it to the BSI. They are obliged to take appropriate organisational and technical precautions to avoid disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes that are essential for the functionality of the critical infrastructures they operate.

If security deficiencies are discovered, the BSI may order their elimination in agreement with the supervisory authorities. In addition, according to

Section 8b of the BSIG, the BSI becomes the central reporting office for IT security of critical infrastructures. Operators must report significant faults in their IT to the BSI if such faults could have an impact on the availability of critical services. If reportable faults occur at a critical information infrastructure (KRITIS) operator, the BSI may, if necessary, also require the manufacturers of the corresponding IT products and systems to co-operate. Furthermore, according to Section 7a of the BSIG, the BSI is granted the authority to examine IT products for their security in order to perform its tasks.

For additional information, please see **3.1 De Jure or De Facto Standards** and **3.3 Legal Requirements and Specific Required Security Practices**.

4.4 Denial of Service Attacks

Please see **3.1 De Jure or De Facto Standards** and **3.3 Legal Requirements and Specific Required Security Practices**.

4.5 Internet of Things (IoT), Software, Supply Chain, Other Data or Systems

Please see **3.1 De Jure or De Facto Standards** and **3.3 Legal Requirements and Specific Required Security Practices**.

In relation to the manner in which data and IT security is regulated within an IoT platform, there is no IoT platform-specific regulatory framework that has been enacted in Germany. However, the prevalent data privacy and IT security regulations cover aspects of the IoT industry and supply chain landscape. There are also certain technical regulations that govern the same.

With regard to the collection and use of personal data, which is often done by consumer IoT devices (eg, location data), the GDPR applies, along with federal data protection rules. Depending upon the industry sector, there may be additional sector-specific rules to be adhered to (eg, telecommunications sector). Article 32(1) of the GDPR lists certain technical and organisational measures (TOMs) to be taken by the controller to protect personal data. Furthermore, and technologically upstream of the TOMs, Article 25(1) of the GDPR stipulates the principle of data protection by design. According to this principle, the data controller is obliged to take into account the protection of personal data during the development of a product. However, it must be noted that the requirements posed by the GDPR are technologically neutral and Article 32(1) only lists a few possible measures as examples. Nevertheless, the required security level is high and could result in a significant improvement in IT security to the IoT if properly implemented.

Since the introduction of the GDPR, however, there has been no noticeable improvement in IT security in the area of the IoT in practice. The enforcement of the GDPR is even more complicated with regards to the supply chain of IoT devices, since measures under the GDPR may only be directed against the controller. This means that data protection authorities cannot take action against manufacturers, suppliers, importers or sellers, even if the controller evades access by the authorities.

The German IT Security Act 2015 focuses on telecommunications and media companies, as well as service providers operating in “critical infrastructure”. Such infrastructure relates to telecommunications, technology, health and water. Any such market player is obliged to take effective measures in order to prevent IT security issues.

Article 1(1) of the EU Cybersecurity Act (the "Act") defines a framework for the establishment of a European cybersecurity certification for ICT products, ICT services and ICT processes. The Act could be applicable to IoT devices if they represent ICT products. However, it must be noted that the Act does not impose any binding requirements on the IT security of IoT devices in general. Instead, Articles 46 et seq of the Act provide only a voluntary certification framework, which does not create any obligations for the manufacturers to carry out certification or even third-party scrutiny procedures.

Since 1994, the BSI has published an annual catalogue detailing over 1,600 best practices and recommendations on how to secure IT infrastructure (the *Grundschutz Kompendium*). Upon demonstrating compliance with the *Grundschutz Kompendium*, organisations may obtain certification under BSI Standards 200-1 to 200-3. One of the chapters relates explicitly to IoT devices. Even though they are not legally binding, the *Grundschutz Kompendium* recommendations have gained considerable relevance since a number of statutory provisions refer to its content and thresholds.

In May 2019, the German Institute of Standardisation published a new standard called Information Technology – IoT capable devices – Minimum Requirements for Information Security (ie, the DIN SPEC 27072). It provides for the requirements to change the standard password after initial use, authentication requirements, establishment of dedicated update mechanisms, etc. However, the scope of DIN SPEC 27072 is limited to IT security in relation to consumer IoT devices.

4.6 Ransomware

There are no special requirements applicable to ransomware attacks besides the general ones that apply to other data breach and cybersecurity incidents. Government authorities strongly advise against paying the ransom. If a company pays the ransom, it is likely to become a target for other ransomware attacks. Additional risk exists due to the identity and location of the recipient of the ransom being unknown. The anonymity of the ransomware attacker may lead to a situation wherein the recipient or its country is listed on sanctions lists or is embargoed, for example by the USA, EU, UN or Germany. In that case, the paying company could be prosecuted for paying the ransom.

5. Data Breach or Cybersecurity Event Reporting and Notification

5.1 Definition of Data Security Incident, Breach or Cybersecurity Event

The GDPR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The BSIG uses the word "malfunction" or "disruption" rather than data breach or incident. Relevant is a malfunction to the availability, integrity, authenticity and confidentiality of information technology systems, components or processes that (can) lead to a malfunction or significant impairment of the functionality of the critical infrastructures.

For additional information, see **1.1 Laws** and **1.3 Administration and Enforcement Process**.

5.2 Data Elements Covered
Any data that is personal data according to Article 4 No 1 of the GDPR is covered.

5.3 Systems Covered
All systems that are used to process personal data are covered.

5.4 Security Requirements for Medical Devices
Pursuant to EU Regulation 2017/745, medical devices are subject to cybersecurity requirements when they include software components. However, in the wake of the COVID-19 pandemic, the entry into force of the regulation was postponed to 26 May 2021.

5.5 Security Requirements for Industrial Control Systems (and SCADA)
There are no special or additional legal requirements concerning industrial control systems. However, whenever there is processing of personal data, the GDPR is applicable.

5.6 Security Requirements for IoT
There are no special or additional legal requirements concerning the internet of things. However, whenever there is processing of personal data, the GDPR is applicable.

ENISA has published a list of good practices with respect to security of the internet of things in the context of smart manufacturing and developed an interactive web-based online tool aimed at guiding IoT operators and smart infrastructure firms when conducting risk assessments.

5.7 Requirements for Secure Software Development
There are no special or additional legal requirements concerning the development of secure software. However, whenever there is processing of personal data, the GDPR is applicable.

Every year, the BSI publishes the Basic IT Security Compendium (*IT-Grundschutz-Kompendium*), the fundamental guideline on basic IT security. The Basic IT Security Compendium focuses on the so-called Basic IT Security Building Blocks (*IT-Grundschutz-Bausteine*). These modules include software development, patch management and change management.

5.8 Reporting Triggers
Article 33 of the GDPR provides that in the event of a breach of the protection of personal data, the controller must notify the competent supervisory authority without delay and, if possible, within 72 hours. To facilitate notification, the supervisory authorities have set up extensive input masks that can be processed online.

Notification may only be dispensed with if the violation "is not likely to pose a risk to the rights and freedoms of natural persons". However, when processing data on behalf of a contractor, the contractor must immediately inform the responsible party ("controller") about the data breach and support the responsible party in reporting the data breach by providing the responsible party with the information available to them (Article 28 paragraph 3(f), GDPR). Where the breach of the protection of personal data is likely to present a high risk to the personal rights and freedoms of natural persons, the controller shall notify the data subject of the breach without delay (Article 34 paragraph 1, GDPR).

Pursuant to Section 8b of the BSIG, operators of critical infrastructures must immediately report to the BSI any disruption to the availability, integrity, authenticity and confidentiality of their information technology systems, components or

processes that (can) lead to a failure or significant impairment of the functionality.

5.9 "Risk of Harm" Thresholds or Standards

The body of the independent federal and state data protection authorities (*Datenschutzkonferenz*, or DSK) has published a short paper that serves as a first orientation (especially for the private sector) to the manner in which to conduct a risk assessment. According to this, the risk assessment should be done in the following phases.

Risk Identification

In order to identify data protection risks, the following questions can be used as a starting point.

- What damage can be caused to natural persons on the basis of the data being processed?
- What causes the damage: ie, what events can cause it?
- What actions and circumstances can cause these events to occur?

Estimation of the Probability of Occurrence and Severity of Possible Damage

The probability of occurrence and severity are estimated for each potential loss. In general, they cannot be mathematically summarised or calculated. One way of measuring a risk is to show a gradation of the severity and probability of occurrence of a possible loss on a scale, with four values: slight/low, manageable, substantial and big/high.

Allocation to Risk Grades

Once the probability of occurrence and the severity of possible losses have been determined, they must be assigned to the risk categories "low risk", "risk" and "high risk". If the potential damage is large and the probability of occurrence is high, there is a high risk. If, on the other hand, the possible damage is small and the probability of occurrence low, there is a low risk.

Sector-Specific Risk Management

Pursuant to Section 8b of the BSIG, operators of critical infrastructures must immediately report to the Federal Office for Information Security any disruption to the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes. However, a notification is not required if the disturbance does not and/or cannot lead to a significant impairment of the operability of the operated critical system.

According to the minimum requirements for risk management in banks and financial service providers (MaRisk) issued by BaFin, the following risks are to be classified as material:

- counterparty default risks (including country risks);
- market price risks;
- liquidity risks; and
- operational risks.

The institution must set up appropriate risk management and risk controlling processes that ensure the identification, assessment, management, monitoring and communication of the main risks and associated risk concentrations.

GDPR Considerations

Furthermore, GDPR Recitals 75 and 76 require that, when assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. It further states that risk should be evaluated on the basis of objective assessment. Article 29 of

the Working Party Guidelines recommend that controllers consider the following specific criteria when assessing the risk of harm:

- type of breach;
- nature, sensitivity, and volume of personal data;
- ease of identification of individuals;
- special characteristics of individual (ie, children, vulnerable individuals, etc); and
- number of affected individuals.

Lastly, ENISA has produced recommendations for assessing the severity of a potential breach.

6. Ability to Monitor Networks for Cybersecurity

6.1 Cybersecurity Defensive Measures

The BSI recommends the following basic measures for cybersecurity:

- determination of the threat level of an institution's own infrastructure and the transparency of the institution towards attackers;
- identification and protection of all network transitions;
- effective prevention of infection with malicious programs;
- inventory of the IT systems and testing for security controllability;
- avoidance of open security gaps on IT systems;
- interaction with the internet only via secure components;
- central collection and evaluation of log data;
- providing your own organisation with all necessary information;
- the organisation is prepared for the management of security incidents;
- authentication mechanisms to prevent misuse by third parties;
- sufficient internal resources are available, external service providers are integrated;
- qualify and sensitise own personnel in questions of cybersecurity;
- enforcement of user-oriented segregation measures;
- the organisation and its members move safely in social networks;
- in the case of higher protection requirements, confidentiality, availability and integrity are ensured by effective measures and penetration tests are carried out; and
- supporting protective measures are taken to defend against targeted attacks.

6.2 Intersection of Cybersecurity and Privacy or Data Protection

Any conflict or issue with cybersecurity will most likely involve personal data. In that case, the GDPR and the BDSG will be applicable. This underlines the strong connection between cybersecurity, privacy and data protection.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information

Under Article 33 of the GDPR, in the case of a personal data breach, the controller shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory data protection authority. This includes information about:

- the nature of the personal data breach, including the categories and approximate number of data subjects concerned and the

categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the personal data breach; and
- the measures taken or proposed to be taken by the controller to address the personal data breach.

Pursuant to Section 8b of the BSIG, operators of critical infrastructures must immediately report to the BIS any disruption to the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes that (can) lead to a failure or significant impairment of the functionality.

The notification shall contain information on the failure, on possible cross-border effects and on the technical conditions, in particular the presumed or actual cause, the information technology affected, the type of facility or installation affected, the critical service provided and the impact of the failure on that service.

7.2 Voluntary Information Sharing Opportunities

The BSI founded the Alliance for Cybersecurity in order to strengthen Germany's resistance to cyber-attacks. Participants in the Alliance for Cybersecurity will have access to an extended range of services, in particular information on the cybersecurity situation, alerts and further background information. Due to the partially confidential nature of this information, the sharing of this content must be restricted and is subject to restrictions under the Traffic Light Protocol (TLP).

Currently, 4,178 companies and institutions are members of the initiative – and more are joining every day. IT service and consulting companies and IT manufacturers are equally represented in the network as user companies of all sizes and from all sectors. This diversity is an important guarantee for a rich exchange of IT expertise and application experience, from which all participants benefit.

8. Significant Cybersecurity and Data Breach Regulatory Enforcement and Litigation

8.1 Regulatory Enforcement or Litigation

The web-based online service Knuddels, which essentially offers a chat service for people aged 14 and over, was fined EUR20,000 because the user passwords were stored without encryption. The website was hacked, which is why the infringement was discovered. Knuddels therefore co-operated with the supervisory authority, which is an important factor in the fine remaining modest.

The highest fine imposed by German data protection authorities is EUR14.6 million. The real estate company Deutsche Wohnen SE stored personal data of its tenants without checking whether this was lawful and necessary. Despite a previous request in 2017 to remedy the deficiencies in data protection, no improvement was achieved. Deutsche Wohnen SE has announced that it will take action against the fine.

The Berlin-based company Delivery Hero was fined almost EUR200,000 for not deleting customer data records and for sending illegal advertising emails.

These fines are all based upon violations of the GDPR. As yet, the BSI has not exercised the right to impose a fine for violations of the BSIG.

8.2 Significant Audits, Investigations or Penalties

Please see **8.1 Regulatory Enforcement or Litigation**.

8.3 Applicable Legal Standards

The applicable legal standards are provided by the GDPR, the BDSG, the TKG, the BSIG, the EnWG and the EU Cybersecurity Act.

8.4 Significant Private Litigation

There are no known major private enforcement cases yet.

8.5 Class Actions

In Germany, class actions are generally not permitted, as German law does not allow for group actions. In general, each plaintiff must present and prove their individual affectedness, individual damage and the causal link between the two.

The Model Declaratory Action

However, in 2018, the model declaratory action was introduced. This enables claims of a large number of consumers who have suffered similar damage to be efficiently enforced. Registered consumer protection associations have the option to establish factual and legal prerequisites for the existence or non-existence of claims or legal relationships determined in favour of at least ten affected consumers. The model declaratory action is conducted exclusively between the plaintiff, the consumer protection association and the defendant. The affected consumers can register their claims in a register of actions and thus achieve the suspension of the limitation period of their possible claims. The ruling on the model declaratory action has a binding impact on the subsequent actions of the consumers. It is to be expected that this instrument will be used for damage claims according to Article 82 of the GDPR. So far this has not been the case, though.

A few model declaratory actions have been brought in Germany since 2018. It seems that German courts are carefully considering whether or not those bringing the claims fulfil the requirements of a "qualified institution". Where the courts are not satisfied that the claimant associations pursue the rights of consumers, but instead forward their own financial interests, the action is terminated.

The Volkswagen model declaratory action revealed that it took the courts almost one year to hold the first oral hearing. This was because claimants actively encouraged individuals to deregister and pursue their claims individually. The reason behind this is that consumers are often under the impression that stand-alone claims will arrive at a quicker solution. In cases of less complexity, judgments can be expected fairly quickly.

9. Cybersecurity Governance, Assessment and Resiliency

9.1 Corporate Governance Requirements

The management of a company has a general duty of care from company and commercial law, especially within the scope of the AktG, GmbHG and HGB. Pursuant to the KonTraG, this obligation includes the recognition and management of cybersecurity risks. Management may be liable for violations. These general cybersecurity obligations of the board of directors include risk identification, risk management, implementation of preventative security measures and information obligations. There are no specific requirements for specified board expertise or training requirements.

There is no legal obligation to appoint a Chief Information Security Officer (CISO) but it is highly recommended as they have the expertise to implement and control an effective cybersecurity concept. Those concepts are required to be certified, for example after ISO 27001.

After a cyber-attack, there may be reporting and notification requirements as described in **5. Data Breach or Cybersecurity Event Reporting and Notification**. Standards for the recovery and resiliency of business operations are described in ISO 27001 and in BSI-Standard 100-4.

BSI-Standard 200-3 sets standards for risk assessment regarding cybersecurity. For risk assessments regarding the processing of personal data pursuant to the GDPR, see **3.3 Legal Requirements and Specific Required Security Practices**.

10. Due Diligence

10.1 Processes and Issues

The GDPR provides for draconian penalties for violations. For this reason and because of the reputational and business risks involved, cybersecurity has become a crucial component of due diligence in the mergers and acquisitions sector. The due diligence process shall at least encompass an analysis of the applicable legal requirements regarding cybersecurity, an analysis of cybersecurity practices and, where appropriate, questions to the management department. Share purchase agreements may include guarantees or safeguards of cybersecurity policies and practices, where appropriate.

10.2 Public Disclosure

There is no regulation requiring disclosure for cybersecurity risk profile or experience.

11. Insurance and Other Cybersecurity Issues

11.1 Further Considerations Regarding Cybersecurity Regulation

All significant cybersecurity issues in Germany have already been addressed in this chapter.

It should also be noted that the importance of cyber insurance is likely to increase in the future. At present, it is mainly of interest for large companies and corporations, as these are usually the primary target of cyber-attacks. However, the threat to small and medium-sized enterprises (SMEs) continues to grow. Cyber-insurance can therefore make sense, especially for SMEs, to cushion the financial losses from a cyber-attack and a resulting loss of business.

Heuking Kühn Lüer Wojtek is one of Germany's major commercial law firms, with more than 400 lawyers in nine offices across Germany and in Zurich offering service at the highest level. The lawyers in the firm's data protection, privacy and cybersecurity group are leaders in their fields and help clients develop global privacy and data security strategies for today's digital economy. They advise clients on, inter alia, data processing agreements; international data flows within groups of companies and binding corporate rules; development of compliance programmes (including GDPR compliance); technology-related data usages; the setting up and operation of customer relationship management, personnel or other databases involving personal identifiable information; as well as the setting up of whistle-blowing and other reporting schemes. Furthermore, they represent clients before administrative authorities and in legal disputes related to (alleged) data protection and data security breaches.

Authors

Thomas Jansen is a partner in Heuking Kühn Lüer Wojtek's Munich office and a member of the IP, media and technology practice group. Thomas has over 26 years of experience as a technology transactions lawyer. He advises German and international corporate clients across diverse industries on all kinds of technology-related matters, with a focus on providing strategic guidance in the creation, acquisition, use and commercial exploitation of technology. He also counsels clients on the intellectual property aspects of mergers, acquisitions and financings, and advises clients on privacy and data protection and cybersecurity-related issues. Thomas is a frequent speaker and is also author of numerous articles on technology and privacy-related topics.

Philip Kempermann is a managing partner of Heuking Kühn Lüer Wojtek based in Düsseldorf. He focuses on IT and data protection and is a member of the firm's IP, media and technology and antitrust practice groups. He advises and represents several large national and international corporations with their IT projects, operations and data protection matters. Additionally, Philip Kempermann assists clients with IoT strategies and provides several international organisations with GDPR compliance advice. Philip Kempermann is an active member of the International Technology Law Association (ITechLaw) as well as the German Association of Law and Informatics (DGRI).

Heuking Kühn Lüer Wojtek

Prinzregentenstraße 48
80538 Munich
Germany

Tel: +49 89 540 31 160
Fax: +49 89 540 31 540
Email: t.jansen@heuking.de
Web: www.heuking.de

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com