The Legislative Framework Governing Cybersecurity in Germany and the European Union

12 November 2020

The subject of cybersecurity has gained in importance within Germany and the European Union. There is a growing need to protect the digital market, and players' IT systems therein, against cybersecurity threats. In the last two years, 68% of enterprises have registered cybersecurity attacks against them. According to the President of the German Federal Office for Information Security (*Bundesamt für Informationstechnologie* or *BSI*), the number of malware programs that we currently know of in Germany (roughly 800 million) grows each day by 390,000. Consequently, European and German legislators have taken measures in order to strengthen cybersecurity, thereby imposing a multitude of new obligations on EU Member States and enterprises. This briefing aims to provide an overview of the most relevant cybersecurity legislation and the requirements affected parties must meet.

The existing legislation regarding cybersecurity can be roughly divided in two categories: Some legislative acts are directly aimed at the improvement of cybersecurity, notably the EU Cybersecurity Regulation that came into force in summer 2019. Other legislation, such as the General Data Protection Regulation (*GDPR*) touches upon questions of cybersecurity incidentally.

Legislation directly aimed at the improvement of cybersecurity

Directive 2009/140/EC (*Framework Directive*) and Directive 2002/58/EC (*ePrivacy Directive*) – transposed into German law into the Telecommunications Act (*Telekommunikationsgesetz* or *TKG*) – are directed at the operators of public telecommunications networks and providers of publicly available electronic telecommunications services. With the adoption of Directive (EU) 2016/1148 (*NIS-Directive*), 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 (*Gesetz über die Elektrizitäts- und Gasversorgung* or *EnWG*) were amended. These latter cybersecurity regulations are directed at: the Federal Office for Information Security itself; at the operators of critical infrastructure (organizations and facilities highly important to the functioning of the community, since their failure or impairment would lead to dramatic repercussions); and at digital service providers (online marketplaces, online search engines and cloud computing services). Small suppliers are excluded from the scope of application of these laws.

These cybersecurity laws primarily set standards for minimum-security requirements and reporting obligations:

Minimum-Security Requirements

The above laws require relevant operators to set in place technical and organisational measures to protect their networks and IT-systems against potential threats in order to avoid security breaches or at least kept them to a minimum. References to EU directives and soft law specify the respective security requirements for certain industries.

Operators of public telecommunications networks and providers of publicly accessible electronic telecommunications services must appoint a security officer and draw up a security concept based on requirements set out in the Federal Network Agency's security catalogue. This security concept must be submitted to the Federal Network Agency immediately after network operation has commenced. As for digital service providers, the security standards are specified in the EU Commission's Implementing Regulation (EU) 2018/151. Operators of energy supply networks must comply with a catalogue of security requirements set out by the Federal Network Agency. A corresponding catalogue exists for operators of power plants that also qualify as critical infrastructure. All other operators of critical infrastructure may propose industry-specific safety standards to the BSI for evaluation and adoption. They must provide proof of compliance with these safety requirements at least every two years.

Reporting Obligations

The reporting obligations that the aforementioned laws prescribe are of great importance in practice. Operators of public communications networks and providers of publicly accessible electronic communications services must immediately notify the Federal Network Agency and the BSI of significant impairments to their networks and services (Article 109 (5) TKG). In such an event, operators of critical infrastructure must report to the BSI immediately via their contact point all disruptions that caused system failures as well as all other significant disruptions that may in the future lead to system failures (Article 8b (4) BSIG). Furthermore, providers of digital services must immediately report to the BSI any incidents that have a significant impact on the provision of a digital service they provide within the European Union.

Guidelines as to what may qualify as an incident of significant impact are set out in the BSIG. Relevant factors may include the number of users and the geographical area affected, as well as the duration and the extent of the disruption.

In turn, the BSI must immediately inform the responsible Federal State (*Bundesland*), supervisory authorities and the operators of critical infrastructure that a cybersecurity attack was attempted or took place, and about the security vulnerabilities they were made aware of.

Fines

Should operators of public telecommunications networks fail to submit a security concept to the Federal Network the TKG provides for fines of up to EUR 100,000. Further, violations of the reporting obligations carry fines of up to EUR 50,000. Under the Energy Industry Act, operators face penalties of up to EUR 100,000 for non-compliance with security standards and failure to fulfil the reporting obligations. The BSIG provides for fines of up to EUR 50,000 for these breaches of law.

Other laws that Contain Provisions on Cybersecurity

Provisions on cybersecurity may be found in several other laws. Regulation (EU) 2016/679 (*GDPR*) and the **Federal Data Protection Act** prescribe concrete measures to achieve a level of security appropriate for the handling of personal data. These precautions include encryption techniques and pseudonymisation. The data protection officer responsible must report any breach of the data protection rules to the competent supervisory authority without undue delay, ideally within 72 hours. Where there is a high risk that the rights of the affected data owner have been violated by the breach, they are to be informed as well. The GDPR specifies fines of up to EUR 10 million for non-compliance with protection standards and violations of reporting duties.

Under the **Banking Act**, financial institutions and the Federal Financial Supervisory Authority are obliged to take measures to ensure data protection and data security. According to the **Act to Improve Enforcement of Law in Social Networks** (*Network Enforcement Act*), providers of social networks that receive more than 100 complaints about illegal content within a calendar year must publish a report on their handling of complaints on their website and in the Federal Gazette. Failure to comply with this obligation can result in fines of up to EUR 5 million.

EU Cybersecurity Regulation

On June 27, 2019, the EU Cybersecurity Regulation came into force. This legal act creates a permanent mandate for the European Union Agency for Cybersecurity (*ENISA*), which has been strengthened in terms of personnel and financial resources. In addition, the regulation introduces a European framework for the cyber security certification of information technology products, processes and services. Security features in IT products and services are verified by an independent body, allowing users to determine how trustworthy the IT products and services they purchase are. The regulation also provides for security features to be built into IT products and services at an early stage of their technical design and development to prevent subsequent security breaches ("security by design").

Regulatory Outlook

The wide range of legislation enacted has improved the detection and remedy of cybersecurity vulnerabilities. However, the high number of cybersecurity attacks shows a need to continuously adapt security standards to the evolving risks. Furthermore, the fragmentation of cybersecurity regulations can be profoundly challenging for companies as they might have to go to great length to determine the legal framework applicable to them.

The coalition treaty between Christian Democratic Union and Social Democrat Party envisages for an IT security law 2.0. On May 7, 2020, the Federal Ministry of the Interior (*BMI*) specified this intention by means of a second draft bill. According to this draft bill, the special obligations currently applicable to critical infrastructure are to be extended to "companies in the special public interest" (Section 2 para. 14 BSIG-E). These include not only defence, space, chemical and IT security companies but also companies of "special economic importance". An additional ordinance is to further precise the definition of these categories.

In addition, the BMI is to be entitled to prohibit the use of critical components from untrustworthy manufacturers by operators of critical infrastructures (Section 9b BSIG-E). This is intended to prevent improper access to hardware and software for sabotage and espionage purposes in the context of the deployment of 5G. Importantly, the obligations of telecommunications and telemedia providers to cooperate in cyber defence are to be tightened. For example, the draft bill gives the BSI the power to order cyber defence measures against telecommunications providers (Section 109a (8) TKG-E). Also, the fines for non-compliance and the violation of reporting duties are to be aligned with the fines set out in the GDPR and thus drastically increased. In conclusion, the development of a regulatory framework to improve cybersecurity in public and private spaces is not yet complete.

Should you have any questions concerning the impact the cybersecurity regulation may have on your company now or in the future, Roland M. Stein and Christopher Wolters are happy to provide assistance.