THE
NATIONAL LAW REVIEW

What You Need to Know About Germany's Cybersecurity Law

Monday, September 14, 2015

Whilst the discussions on the proposed ***Network and Information Security (NIS)*** Directive at European level are still ongoing (*see* Update on the Cybersecurity Directive – over to Luxembourg?), less has been said about Germany new national Act to Increase the Security of Information Technology Systems (the "IT Security Law"). The IT Security Law was published in the Federal Official Gazette on July 24, 2015 (*see* here) and entered into force the following day.

COVINGTON

Article By
Privacy and Data Security Practice Group
Covington & Burling LLPInside Privacy

Communications, Media & Internet
Election Law / Legislative News
Germany

Recognizing the importance of cybersecurity as a core element of security, the IT Security Law aims to improve the level of IT security of certain companies, and protect citizens online. The IT Security Law was been adopted with certain changes compared to the initial legislative proposal (see New Version of Draft German Cybersecurity Law Published). Most importantly, the IT Security Law now foresees the possibility of administrative fines (of up to Euro 100,000 in case of a serious violation). Moreover, certain provisions of the IT Security Law will be evaluated four years after the entry into force of the aforementioned secondary legislation.

Who is covered?

The IT Security Law defines **critical infrastructure** as equipment, plants or parts thereof which are of great importance for the functioning of the community, because their failure or impairment could lead to significant supply shortfalls or threats to the public safety. Infrastructure in the following **sectors** is covered:

- energy
- information technology
- telecommunications
- transport and traffic
- health
- water
- food
- finance
- insurance

The exact scope of application of the IT Security Law will be determined by secondary legislation. The German Interior Ministry is planning to adopt implementing legislation in spring 2016 for the information and telecommunication technology, energy, water and food sectors, and at the end of 2016 for the other sectors. The German Government expects that no more than 2,000 operators of critical infrastructure in the various sectors would be covered.

Certain providers have been exempted from some of the obligations under the IT Security Law, in particular the obligation to implement minimum IT security measures, to designate a contact point, and to report cybersecurity incidents. These include micro-enterprises (as defined in Commission Recommendation 2003/361/EC), but also operators of power grids and power plants, telecommunications providers and other operators which are already subject to comparable statutory requirements.

However, the IT Security Law has also amended several other laws, including the Telecommunications Act (TKG) and Telemedia Act (TMG). Importantly, as a result, since July 25, 2015 **telecommunications providers** and **providers of information society services** (essentially content and hosting providers [1].) are already subject to increased requirements under the amended TKG and TMG, respectively, regarding the protection of user data and of their IT systems. Telecommunications providers are also subject to extended notification obligations as a result.

What are the new obligations?

Operators of critical infrastructure must in particular:

- **implement appropriate organizational and technical safeguards** and other measures in accordance with the state of the art within two years after the entry into force of secondary legislation specifying those safeguards and measures. There is some room for self-regulation, as operators and associations of the respective industry sector can develop sector-specific standards to comply with the minimum IT security requirements, which the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – the "BSI"), upon application, can declare to be appropriate.

- **regularly** (but at least every two years) **prove that they fulfill the security requirements** (*e.g.*, by means of security audits, examinations or certifications); the operators must provide an overview of such audits, *etc*., to the BSI, including information on the security defects discovered. The BSI can request further information and that the security defects be remedied, and can also further specify the procedures to be taken for security audits, examinations and certifications;

- **designate a contact point** for the BSI;

- **notify the BSI immediately** of any significant disruptions of the availability, integrity, authenticity and confidentiality of their IT systems, components and processes which may result or have resulted in the failure or an impairment of the functioning of critical infrastructure operated by them. The BSI can ask the manufacturers of affected IT products and systems to cooperate with respect to the removal or avoidance of disruptions.

The new competences of the BSI; enforcement

The IT Security Law strengthens the BSI, which acts as a central point of contact, gathers and analyzes all relevant information, cooperates with other authorities, and provides information to operators of critical infrastructure and the public as well as advice and support. In order to fulfill its tasks, the BSI is empowered to issue warnings, to recommend security measures or the use of specific security products, and to examine IT products and systems. The BSI will also prepare minimum standards for the IT security of German federal infrastructure, which the German Federal Ministry of the Interior can adopt in form of administrative regulations.

The IT Security Law establishes administrative offences of up to Euro 50,000 and up to Euro 100,000 respectively in case of a violation of certain obligations thereunder.

[1] Under German/EU law, an "information society service" is any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services and includes, for instance, online banking and online shopping.