ALSTON&BIRD

CYBER ALERT

A Publication of the Cybersecurity Preparedness & Response Team

WWW.ALSTONPRIVACY.COM JANUARY 13, 2016

Global Cybersecurity Spotlight: Germany

Following nearly two years of negotiations, the European Parliament and European Council finally reached agreement on the Network and Information Security Directive ("NIS Directive") in December 2015.[1] The Directive will require certain operators of "essential services" and "digital services providers" (e.g., online marketplaces, search engines and cloud computing services) to implement cybersecurity controls and report significant security breaches to the appropriate national authority. EU member states will be required to implement the NIS Directive at the national level within 21 months and will have an additional six months to identify in-scope entities. It is therefore possible that we will not see the real-world impacts of the Directive until 2017 or 2018. The fact that the imposition of minimum cybersecurity requirements on critical infrastructure owners is still merely on the horizon has not, however, prevented EU member states from moving ahead with legislation of their own in the meantime.

While discussions on the NIS Directive were ongoing, Germany passed its own domestic cybersecurity law in 2015 aimed at safeguarding IT systems in companies essential to national interests. The "Act to Increase the Security of Information Technology Systems" (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme* (text in German)) (referred to as the "IT Security Act") is Germany's first comprehensive legislative scheme passed for the purpose of establishing a minimum level of cybersecurity in critical infrastructure, as defined by the law.

Passage of the Act was only the first in a two-step lawmaking process. Later this year, Germany's Interior Ministry will be issuing regulations that identify companies subject to the Act and set its compliance obligations into force. Some commentators have estimated that approximately 2,000 providers of essential services could fall under the combined provisions of the IT Security Act and its accompanying regulations. The German agency responsible for IT security at the national level is known as the *Bundesamt für Sicherheit in der Informationstechnik* (Federal Office for IT Security), or the BSI. Most of the IT Security Act's provisions affect or are overseen by the BSI.

---

1 *See* Delphine Charlot, "EU Institutions Adopt First Pan-European Legislation on Cybersecurity," Alston & Bird Privacy & Data Security Blog, Dec. 11, 2015.

Companies Covered by the IT Security Act

The IT Security Act sets forth new cybersecurity compliance obligations for operators of "critical infrastructure." For the purposes of the Act, critical infrastructure is generally defined as the following industries: energy, IT, telecommunications, transportation, health care, water, food and finance and insurance. This definition, however, is preliminary and will soon be rounded out by detailed regulations issued by Germany's Interior Ministry throughout 2016.

Currently, the Interior Ministry is working through the components of these industries to determine what parts of each industry will be designated critical infrastructure for cybersecurity purposes. The Ministry will make this determination by reviewing each industry on a progressive sector-process-facility basis to identify segments and asset classes that should be deemed critical, such as in the following example from the energy industry:

Industry	Energy
Sector	Electricity
Process	Power production
Facility	Power plants
Critical threshold value	[x] gWh per year

In spring 2016, the Ministry plans to issue regulations designating the critical components of the energy, IT, telecom, water and food sectors. By the end of 2016, regulations identifying the in-scope portions of the remaining critical infrastructure industries are expected to be issued and binding regulations identifying all German critical infrastructure subject to the IT Security Act's compliance obligations should be in place.

Compliance Duties Under the Act

The IT Security Act imposes numerous new compliance obligations on "operators of critical infrastructure" ("CI operators"). The most salient obligations are:

- ***Duty to Implement Appropriate Cybersecurity Measures:*** The Act requires CI operators to implement "appropriate organizational and technical measures," in accordance with the state of the art, that safeguard against "disturbances to the availability, integrity, authenticity and confidentiality" of their IT processes and systems.
- ***Standard Setting:*** Despite the regulatory nature of this new cybersecurity requirement, the process of standard-setting may be more collaborative than adversarial. Article 1 of the IT Security Act implements a self-regulatory approach by permitting industries to band together to suggest industry-wide security standards to the BSI for approval. The BSI appears to be amenable to working with industry groups to develop industry- or sector-wide cybersecurity standards, as indicated in public presentations.[2]

---

[2] *See, e.g.*, Bundesministerium des Innern [Ministry of the Interior], Das IT-Sicherheitsgesetz: Welche Anforderungen kommen auf die Branche zu? [The IT Security Act: What Requirements Should Industry Expect?], Sept. 30, 2015.

- ***Biannual Testing and Reporting Obligations:*** Every two years, CI operators must file a report with the BSI proving—via security audits, tests, or certifications—that they are in compliance with their duty to implement appropriate cybersecurity measures. The report must (1) provide an overview of all audits, tests or certifications conducted; and (2) identify any cybersecurity defects discovered during testing. The BSI can then request further information and can require the CI operator to eliminate any cybersecurity defects.

- ***Ad Hoc Duty to Report Security Incidents:*** The IT Security Act requires CI operators to "immediately" report to the BSI any "significant disturbances in the availability, integrity, authenticity, or confidentiality of their IT systems" that have led or *could lead* to a failure or an impairment of their critical infrastructure. In other words, the *potential* for a security breach gives rise to a duty to report, as would a significant outage or software issue that is not caused by an intrusion but affects the availability or integrity of IT systems. As a compromise, however, the report for a potential incident need only contain the technical details and the "branch" of the affected CI operator[3]—only in cases of an *actual* incident does the CI operator need to be identified. Upon receiving an incident notice, the BSI can require the manufacturer of the affected IT product or system to cooperate in removing or remedying the disruption.

- ***Duty to Designate a Point of Contact:*** Every CI operator must designate a contact point who can be reached by the BSI at any time. However, each industry or branch thereof may designate an industry- or branch-wide "single point of contact" (SPOC) and, if it does, the entire information exchange between the BSI and that industry or branch runs through the SPOC. The BSI hopes that industries will designate industry-wide SPOCs so that the BSI can profit from industry know-how in incident reporting and the BSI can quickly disseminate vital information to entire industries.

- ***BSI's Duties:*** For its part, the BSI must maintain an up-to-date status report on cybersecurity threats and must share any information it receives with any CI operator (or industry SPOC) that could be affected by it.

Generally, these compliance duties will come into force two years after the Interior Ministry issues its regulations setting forth which industry components constitute critical infrastructure subject to the IT Security Act. The exceptions to this are power plant and power grid operators, who must install appropriate cybersecurity measures immediately, as well as telecom and web companies, which must immediately begin reporting security breaches.

Notably, several types of entities will be exempt from certain aspects of the IT Security Act by law. These include micro-enterprises[4] and operators of critical infrastructure already subject to comparable requirements (such as via network security requirements already implemented under the EU's e-Privacy Directive[5] for telecommunications operators).[6]

---

3 The term "branch" is not defined in the Act.

4 *See* Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

5 *See* Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

6 The German law implementing, *inter alia*, the e-Privacy Directive is the Telecommunications Act (*Telekommunikationsgesetz*). The Telecommunications Act already contained a comparable duty to implement network security standards, but did not contain a comparable breach-notification requirement. Instead, Article 5 of the IT Security Act introduced such a requirement as the new § 109(5) of the Telecommunications Act.

BSI's Powers and Fines for Noncompliance

The IT Security Act beefs up the authority of the BSI so that it can ensure that reasonable cybersecurity levels are being maintained throughout Germany's critical industries. The BSI is now, by law, CI operators' central point of contact for cybersecurity issues. It can conduct investigations into IT products and systems, collect and analyze information about cybersecurity threats, issue warnings, recommend security measures or specific security products and liaise with other German agencies as appropriate.

Moreover, the BSI can fine any company that "intentionally or negligently" violates its compliance duties. In general, fines are limited to €50,000. However, if the BSI orders a company to eliminate a cybersecurity defect and the company fails to do so, the fine can increase to €100,000.

German Data Protection Law Remains Unaffected

The IT Security Act permits CI operators to process and use personal data only to the extent that is necessary to comply with their cybersecurity and reporting obligations under the Act. Otherwise, the Act expressly states that CI operators must abide by the Federal Data Protection Act (*Bundesdatenschutzgesetz*), i.e., they must comply with generally-applicable data-protection law. No provisions of the IT Security Act, however, permit the BSI to fine a CI operator for violating data-protection law; that responsibility appears to remain with Germany's 17 Data Protection Authorities.

Interactions with Other EU Legislation on Cybersecurity

The IT Security Act appears to overlap to a large degree with the NIS Directive, and in light of the similarity in aims between the Act and the Directive as well as the discretion Article 3a of the NIS Directive grants member states in identifying operators of essential services, the Act and its regulations could well end up serving as a portion of Germany's implementing legislation for the NIS Directive.

Entities subject to the IT Security Act will also be subject to the new EU General Data Protection Regulation (GDPR) once it becomes effective, which contains its own set of data security requirements.[7] While the IT Security Act and NIS Directive primarily focus on business continuity and network security, the GDPR's emphasis is on the protection of "personal data against accidental or unlawful destruction or accidental loss" and the prevention of "any unlawful forms of processing, in particular any unauthorized disclosure, dissemination or access or alteration of personal data."

Alston and Bird is closely following the implementation of the IT Security Act as well as the Interior Ministry's forthcoming regulations. Further, although the final text of the NIS Directive is not yet available, we will soon release a preliminary analysis of the most recent draft as well as an analysis of the dual breach notification requirements of the NIS Directive and GDPR.

---

7 *See* Jan Dhont, Delphine Charlot and Jon Filipek, "The EU General Data Protection Regulation – Europe Adopts Single Set of Privacy Rules," Alston & Bird Privacy & Data Security Blog, Dec. 16, 2015.

If you have any questions or would like additional information, please contact Kimberly Peretti, Daniel Felz or Jason Wool.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ■ 18th Floor ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ■ Suite 400 ■ Durham, North Carolina, USA, 27703-85802 ■ 919.862.2200 ■ Fax: 919.862.2260
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, California, USA, 94303-2282 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333