FRANZ
RECHTSANWÄLTE

AUGUST 2015

NEWSFLASH

IT Security

» A new German IT Security Act came into force on July 25, 2015.

Minimum standards are established and obligations to report cyber attacks are introduced for companies which operate so-called “Critical Infrastructures”.

Obligations in the area of IT security for companies operating commercial websites are extended. «

FRANZ RECHTSANWÄLTE Partnerschaftsgesellschaft mbB | Düsseldorf – Basel | www.franzlegal.com
Kaistraße 16A | 40221 Düsseldorf | Deutschland | Tel +49 (0)211 157676-0 | Fax +49 (0)211 157676-76
Gerbergasse 1 | 4001 Basel | Schweiz | Tel +41 (0)61 26120-48 | Fax +41 (0)61 26120-49

Summary

In view of the growing threat by cyber attacks, the German Federal Parliament has passed a new law in order to increase the security of information technology systems, the so-called **IT Security Act**, which **came into force on July 25, 2015**. At the center of the discussion of the draft law were obligations for companies operating so-called "Critical Infrastructures". However, the IT Security Act also tightens the obligations for all providers of commercial websites.

Operators of **nuclear power plants** and **telecommunications providers** have to report cyber attacks already as of July 25, 2015. For example, telecommunication companies have to inform their customers, if their data-processing systems cause violations to IT security. Affected customers have to be informed about how to solve these problems. For operators of other "***Critical Infrastructures***" the corresponding obligations will **not** apply **before a legislative decree will come into force.** Such decree is yet to be passed and a draft is currently being prepared by the Federal Ministry of the Interior. Therefore, the companies concerned still have the opportunity to adapt to the changes and to test the changeover of their IT processes.

Already the IT Security Act brings along **changes**, which are relevant to **nearly each operator of a commercial website**, e.g online shops or websites with user accounts. As of now, increased requirements for the protection of customer data as well as of the own IT systems apply. Service providers are obligated to take technical and organizational measures for the protection against unauthorized access to personal data and against malfunctions. Thereby the distribution of malicious software via the internet shall be curbed as well as attacks and malfunctions through third party content shall be prevented. Therefore, service providers should update the technological level of their services. The measures taken should be documented and contract partners should become obligated to take the corresponding protective measures.

I. Extension of the obligations for operators of "Critical Infrastructures"

Companies from system-critical areas now are obligated to observe a minimum level of IT security and to report cyber attacks. Through amendments of the Telecommunications Act as well as the Atomic Energy Act increased requirements already apply with the coming into force of the IT Security Act. For the operators of further so-called **"*Critical Infrastructures*" similar obligations** do not apply **before the adoption of a more detailed legislative decree**. This becomes relevant to companies from certain branches which are significant for the functioning of the community and for the securing of people's basic needs. According to the explanatory memorandum of the IT Security Act, in particular services in the branches **power supply, natural gas** and **mineral oil supply, telecommunications** and **information technology, transport services providers in the fields of aviation, inland navigation** and **ocean shipping, rail** and **road transport, medical care, laboratories, pharmaceuticals** and **vaccines, public water** and **wastewater supply, food industry** and **grocery business, banking, stock exchanges, insurance companies** as well as **financial service providers** and **payment service providers are considered as critical infrastructures**. Therefore, the term "Critical Infrastructures" probably will include a rather broad spectrum.

The companies which operate "Critical Infrastructures" are, among other things, obligated to take appropriate organizational and technical precautions, which may include infrastructural and personnel-related measures in order to improve the security of their IT systems. Also measures for tracing and remedy of malfunctions are required. Precise security standards shall be determined in the regulation, but they may also specifically be proposed by the concerned companies or inter-trade organizations themselves.

Considerable malfunctions of IT-systems, components or processes which may lead to a breakdown or impairment of the functioning of Critical Infrastructures have to be reported to the Federal Office for Information Security. In case such breakdown or impairment actually occurred, the name of the company concerned also has to be disclosed.

Intentional or negligent violations of the requirements of the IT Security Act may be punished by a fine of up to 100,000 Euros.

II. Additional obligations for each operator of a commercial website

The IT Security Act introduces additional obligations and requirements for operators of commercially offered websites by the amendment of the Telemedia Act ("*Telemediengesetz*"). Therefore, the rather broad scope includes all commercial websites, online shops as well as websites that are financed by advertising.

The objective of the new act is to prevent unauthorized accesses to the technical systems used for telemedia offerings (i.a. websites). Moreover, commercial websites shall be protected against unauthorized access to personal data and malfunctions, in particular if they are caused by external attacks. The companies which run commercial websites have to take technical and organizational precautions as far as – in each individual case – technically possible and economically reasonable, in order to prevent such accesses. In this context, it is also necessary to repel attacks from third parties, on which the service provider possibly has not direct technical influence, e.g. in case of compromised advertisement banners as a "gateway" for malware.

Violations against these obligations may be punished by penalties in the amount of up to 50,000 Euros.

Even though the amendment does not directly introduce new, additional claims for damages, it cannot be outruled that general claims under civil law will be enforced more easily due to the increased obligations and requirements. The risk which may occur through the use of (e.g.) unencrypted websites (e.g. by phishing or infection with malicious software) may represent a violation of property rights or of the general right of personality in particular cases. The provider of the commercial website might be liable for these violations, if he failed to take the appropriate measures resulting from the new IT Security Act amendment and thereby, possibly violates his general legal duty to maintain safety. It is quite conceivable that the requirements established by the IT Security Act may be classified as a so-called "protective law", which may more easily open the way for a general tortious claim for damages.

Therefore, companies operating commercial websites should **check the security of their websites and update them regularly**. State-of-the-art encrypting methods as well as a secure authentication process appropriate to the security requirements have to be used, in particular when using personal data in online shops with user accounts. **Contracts with service providers and contract partners** to which the provider offers (e.g.) advertising space on a website, **should be checked and – if required – be modified** in a way that the corresponding obligations as well as possible claims for damages can be passed on to these contract partners. All measures should be documented in a legally consistent way in order to be able to respond to possible accusations effectively.

We want our clients to be able to keep up to date with the legal developments and the technical progress. In this context, we advise our clients in all IT-related issues. We represent domestic and foreign IT companies as well as software developers in preparing and executing IT projects, we advise companies in IT-related M&A projects and support our clients up to and including court litigation.

Contact persons:

Axel Staudt, LL.M.
Attorney-at-law and Partner
staudt@franzlegal.com
Practice Group
Mergers & Acquisitions

Karsten Korrat
Attorney-at-law and Partner
korrat@franzlegal.com
Practice Group
Commercial /
Outsourced Legal Department