

NEW CYBERSECURITY REGULATIONS IN GERMANY—REGISTRATION REQUIREMENT EXPIRES ON 6 MARCH 2026

Date: 5 March 2026

EU Corporate and Policy and Regulatory Alert

By: Dr. Thomas Nietsch, Dr. Ulrike Elteste

After a delay of more than a year, the German implementation law for the [NIS2 Directive](#) (Directive (EU) 2022/2555) came into force in December 2025 ([Law on the Implementation of the NIS 2 Directive and on the Regulation of Essential Features of Information Security Management in the Federal Administration](#)). The law provides for significant changes and revisions to various cybersecurity laws, in particular the BSI Act.

Many more companies than before now fall within the scope of the BSI Act. Previously, the BSI Act only regulated traditional critical infrastructure such as transport and traffic, energy, finance, health, research, and the telecommunications industry. Now, the digital sector is also covered, in particular cloud computing services, data center operators, managed (security) service providers, and providers of online marketplaces, online search engines, and social networks. The production and trade of chemical substances, the production, processing, and distribution of food, and various areas of the manufacturing industry (production of goods) are also affected. Lists of the sectors and activities covered are available [here](#) and [here](#). The BSI offers an [impact assessment](#) on its website.

Although not provided for in the directive, the German implementation law provides for a *de minimis* exemption if an activity that is generally covered is negligible in relation to the overall activity of a company. In these cases, the requirements of the BSI law do not apply.

Covered entities must register on the [platform](#) provided by the BSI by 6 March 2026. This requires an ELSTER organization certificate.

Violations are punishable by a fine of up to EUR€500,000. Regardless of this, however, companies should thoroughly check whether they fall within the scope of the law and what obligations this entails for them.

Other obligations of covered companies include, in particular:

- Taking appropriate measures to prevent and remedy disruptions to the availability, integrity, and confidentiality of their information technology systems;
- Immediately reporting significant security incidents to a single reporting center;
- Training obligations

Management is liable to their company for damages in the event of violations of these obligations.

KEY CONTACTS



DR. THOMAS NIETSCH
PARTNER

BERLIN
+49.30.220.029.408
THOMAS.NIETSCH@KLGATES.COM



DR. ULRIKE ELTESTE
COUNSEL

FRANKFURT
+49.69.945.196.416
ULRIKE.ELTESTE@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.