By PwC Deutschland | 02. September 2026

NIS2 - Network Information Service and what came about

NIS2 is the European Union’s second directive on network and information system security aimed at strengthening cybersecurity across critical sectors and digital infrastructure. It is much more than just an update to the cybersecurity requirements. Its implementation is not merely an IT project.

Against the backdrop of growing dependence on digital technologies, the COVID-19 pandemic highlighted how vulnerable digitalized societies can be to unexpected risks. In light of this, the European Commission reviewed the existing NIS Directive and identified various areas for improvement:

After several rounds of negotiations, the final NIS 2 Directive was adopted by the European Commission in December 2022.

NIS2 is far more than just an update to the cybersecurity requirements for operators of critical infrastructure. The directive significantly expands the scope of affected companies compared to NIS1, tightens the requirements for governance and risk management, and interacts with other regulations such as DORA, CRA, the AI Act, and the GDPR. For companies, this translates into one thing: Implementation is not merely an IT project.

For many companies, NIS2 starts with a very practical question: Are we even covered by it? In Germany, this question is addressed in the BSIG (i, e., the Federal Act on Information Security) which covers not only KRITIS providers but also companies in defined sectors that exceed a certain size. CRITIS refers to critical infrastructure in Germany, which are essential systems that support societal functions, health, security, and economic well-being. These infrastructures are crucial for maintaining the availability and integrity of services, and their failure can lead to significant disruptions. The transposition of the directive into the national laws of EU member states has led to variations in the scope of application from one member state to another.

This is precisely where legal departments come into play.

The NIS2 Directive’s list of duties includes appropriate, proportionate, and effective technical and organizational cybersecurity measures. These include, among other things, risk analysis, incident response, business continuity, supply chain security, cybersecurity hygiene, and training. In this process, the legal department takes the lead to interpret, coordinate and harmonize the internal regulatory framework.

The effectiveness of governance becomes apparent when an incident occurs: The legal department would be well advised to ensure that procedures for handling an incident are rehearsed with stakeholders. After all, a security incident is never merely a technical event. It also triggers

reporting obligations, communication requirements, and the need for coordination with authorities, insurance companies, business partners, and other stakeholders.

NIS2 clearly makes the supply chain an integral part of risk management. Security requirements must be communicated to service providers and set forth in contracts. In this context, existing contracts and new contracts must be reviewed for security standards, control mechanisms, liability, contractual penalties, and termination rights.

With NIS2, management is also increasingly involved. The legal department should therefore provide early advice on risks, recourse options, and appropriate mitigation measures.t

Note: This post is in part a free translation of the article published on 31 August 2026 in the German **Blog *Steuern & Recht***.

Schlagwörter

Digital Operational Resilience Act (DORA), networking