NIS2: Cybersecurity is now a management task

THE NIS2 DIRECTIVE INTRODUCES MORE STRINGENT CYBERSECURITY REQUIREMENTS FOR COMPANIES AS WELL AS FAR-REACHING SANCTION MECHANISMS TO ENSURE COMPLIANCE.

Executive Summary

- Compared to the previous legislation, the NIS2 Directive broadens the scope of application considerably, with companies in 18 sectors now affected (compared to seven previously).
- Firstly, the companies concerned have to implement and document comprehensive technical, operational and organisational measures to counter cybersecurity risks. Secondly, they are also responsible for ensuring "supply chain security" by checking their existing contracts for NIS2 compliance and adapting them if necessary.
- Violations of the new catalogue of duties can be punished with substantial fines of up to 10 million euros. Managing directors may in some cases be held personally liable.
- Companies need to achieve NIS2 compliance by 17 October 2024 at the latest.

1. Introduction

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union ("**Network and Information Security Directive 2**"/"**NIS2 Directive**") entered into force on 16 January 2023. The Directive needs to be transposed into national law by **17 October 2024**; a second draft bill for the implementation of the NIS2 Directive is already available.

The aim of the Directive is to coordinate and further strengthen cybersecurity across the Union, both in the area of public administration and in private companies. This is because hacker attacks not only have the potential to cause significant damage, especially financial damage, for the individual company concerned, but can also damage the national economy and society as a whole if, for example, a central internet hub goes down due to a cyber attack, a traffic light system is attacked or a hospital's operations are disrupted. Last but not least, there are also risks in connection with (corporate) espionage if sensitive

information can be accessed – for example, due to insufficiently protected IT systems.

Although there are already – in some cases even EU-wide – regulations on cybersecurity with comparable objectives, these have been deemed insufficient, as they are essentially limited to critical infrastructure and digital services. Moreover, there are significant differences in the level of protection achieved across EU Member States to date.

Against this background, but also in light of the fact that the smooth functioning of IT systems has long since become a key foundation for social interaction and, above all, for the success of the EU Single Market, and that threats to these systems are constantly increasing, the EU felt compelled to make the existing regulations more stringent with a comprehensive catalogue of minimum security measures, as well as to significantly broaden the scope of application from the previous seven to 18 sectors.

2. Affected companies

All companies that meet the following criteria are affected by the NIS2 Directive and the corresponding implementation law:

- More than 50 employees and
- Annual turnover of more than 10 million euros and
- Active in one of the following sectors:
  - Banking and financial market infrastructures
  - Digital infrastructure
  - Digital providers (such as cloud services and online marketplaces)
  - Manufacturing (esp. machinery and equipment/ motor vehicles/IT/household appliances/consumer electronics)
  - Food (production, processing and distribution)
  - Energy
  - Chemicals (manufacture, production and distribution)
  - Transport
  - Health
  - ICT service management (B2B)
  - Postal and courier services
  - Research
  - Public administration
  - Drinking water, waste water and waste management
  - Space

Regardless of their size, companies are subject to the obligations of the Directive based solely on the work they perform or services they offer, such as certain IT service providers like DNS service providers or qualified trust services that provide digital signatures.

Furthermore, the Directive authorises EU Member States to expand the scope of application to include additional companies if there is reason to fear that a disruption of their services would have a significant impact on society or the economy as a whole.

3. Obligations of affected companies

All companies covered by the NIS2 Directive are required to **take technical, operational and organisational measures** to manage the security risks threatening their network and information systems and to prevent or minimise the impact of potential security incidents.

The determination of which measures need to be taken must take into account, firstly, the probability of a security incident occurring, and secondly, its potential impact on the company as well as on society and the economy as a whole. The greater this assessed risk and impact, the more extensive the measures must be. In any case, the measures must include the following:

- Policies on risk analysis and information system security;
- Incident handling;
- Business continuity, such as backup management and disaster recovery, and crisis management;
- Supply chain security, including security-related aspects concerning the relationships between each entity and their direct suppliers or service providers;

- Security in network and information system acquisition, development and maintenance, including vulnerability management and disclosure;
- Policies and procedures to assess the effectiveness of cybersecurity risk management measures;
- Basic cyber hygiene procedures and cybersecurity training;
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- Human resources security, access control policies and asset management;
- The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

In addition, companies must arrange for **regular training** of their employees to ensure that they have sufficient knowledge and skills to identify and address cybersecurity risks.

Furthermore, the precautions to be taken are paired with **comprehensive notification and reporting obligations**: As soon as a security incident occurs which has led or may lead to a serious operational disruption or financial loss for the company concerned, or which has caused or may cause damage to natural or legal persons, the company must report this to the competent authority within 24 hours and also inform the recipients of its services. This early warning must subsequently be confirmed and/or updated and evaluated, and a detailed final report must be submitted.

Companies which the Directive defines as **essential entities**, i.e. which are a part of critical infrastructure or which exceed the ceilings for medium-sized enterprises and belong to certain sensitive sectors, are also subject to a **proactive obligation to provide evidence** that the measures they have taken are sufficient. These companies can also be audited for NIS2 compliance by the competent authority on an ad hoc basis.

4. Sanctions and liability

Violations of the aforementioned obligations are subject to sanctions. Depending on whether the company is classified as an essential or important entity, fines of up to ten million euros or 2% of annual turnover (essential entities) or up to seven million euros or 1.4% of annual turnover (important entities) can be imposed – whichever amount is higher in each case.

In addition to the company, its management bodies may also be subject to liability. If they violate their – non-delegable – monitoring duties, they can be held personally liable by the company for the damage incurred.

The Directive also empowers the competent authorities to suspend the operating licence of essential entities and to demand the temporary removal of management staff if the entities have not complied with cybersecurity orders.

5. Relationship to the Digital Operational Resilience Act

With the Digital Operational Resilience Act (Regulation [EU] 2022/2554; "**DORA**"), the EU introduced another legal act as a **lex specialis** that is intended to increase digital resilience and harmonise it across the EU for almost all companies in the financial sector. According to the NIS2 Directive, the provisions relating to cybersecurity risk-management, reporting obligations, supervision and enforcement should not apply to these companies. Instead, the relevant – and stricter – provisions of DORA apply. According to the legislative drafts and discussion papers already available, it is also becoming apparent that the German legislator would like to completely exclude those companies in the financial sector that are already obliged by DORA from the scope of the NIS2 Implementation Act.

6. Consequences and outlook

The significance of the NIS2 Directive and its impact can hardly be underestimated. With managing directors being held personally liable, cybersecurity is now a management task; the measures to be taken are extensive and require a structured implementation of cybersecurity precautions and corresponding documentation. In addition to these technical, operational and organisational measures to be taken, contracts with business partners within a supply chain must also be checked for NIS2 compliance and adapted if necessary.

Although German lawmakers still have until **17 October 2024** to implement the Directive into national law, since the measures to be taken are so comprehensive, it would be wise for companies to get a head start on checking their own structures and contracts for NIS2 compliance and making any necessary adjustments. While this may incur considerable costs, any potential fines for a lack of NIS2 compliance, let alone the financial losses incurred from a "successful" attack on a company's network and information security, are likely to be even higher.

Dr Jörg Wünschel
Lawyer, Senior Associate
Berlin
Tel +49 30 2039070
joerg.wuenschel@gsk.de

Dr Jonathan Jung
Lawyer, Associate
Berlin
Tel +49 30 2039070
jonathan.jung@gsk.de

GSK
STOCKMANN

Disclaimer
This client briefing exclusively contains general information which is not suitable to be used in the specific circumstances of a certain situation. It is not the purpose of the client briefing to serve as the basis of a commercial or other decision of whatever nature. The client briefing does not qualify as advice or a binding offer to provide advice or information and it is not suitable as a substitute for personal advice. Any decision taken on the basis of the content of this client briefing or of parts thereof is at the exclusive risk of the user.

GSK Stockmann as well as the partners and employees mentioned in this client briefing do not give any guarantee nor do GSK Stockmann or any of its partners or employees assume any liability for whatever reason regarding the content of this client briefing. For that reason, we recommend you to request personal advice.

www.gsk.de

GSK Stockmann
Rechtsanwälte Steuerberater Partnerschaftsgesellschaft mbB

BERLIN
Mohrenstrasse 42
10117 Berlin
T +49 30 203907 - 0
F +49 30 203907 - 44
berlin@gsk.de

HEIDELBERG
Mittermaierstrasse 31
69115 Heidelberg
T +49 6221 4566 - 0
F +49 6221 4566 - 44
heidelberg@gsk.de

FRANKFURT/M.
Bockenheimer Landstr. 24
60323 Frankfurt am Main
T +49 69 710003 - 0
F +49 69 710003 - 144
frankfurt@gsk.de

MUNICH
Karl-Scharnagl-Ring 8
80539 Munich
T +49 89 288174 - 0
F +49 89 288174 - 44
muenchen@gsk.de

HAMBURG
Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBOURG
GSK Stockmann SA
44, Avenue John F. Kennedy
L - 1855 Luxembourg
T +352 271802 - 00
F +352 271802 - 11
luxembourg@gsk-lux.com

LONDON
GSK Stockmann International
Rechtsanwaltsgesellschaft mbH,
London branch
Queens House, 8-9 Queen Street
London EC4N 1SP
United Kingdom
T +44 20 4512687-0
london@gsk-uk.com

Registered office: Munich
Munich Local Court
HRB 281930
Managing directors:
Dr Mark Butt, Andreas Dimmling

YOUR PERSPECTIVE.
GSK.DE | GSK-LUX.COM