alliuris

ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS.

Cybersecurity and the EU's NIS 2 Directive

Sara Nesler, Mag. iur. (Torino), LL.M. (Münster)

August 2024

In 2023, a significant proportion of European businesses faced cyber-attacks, with around 32% of companies reporting a breach or security incident. Larger organisations were more likely to be targeted, with 37% of mid-sized companies and 59% of large companies experiencing cybercrime incidents (AAG-IT statistics). The consequences of such attacks range from business interruption, loss of revenue, data recovery costs and reputational damage to compensation claims from affected customers, which can quickly reach significant sums. When companies or institutions that play a particularly important role in society are affected, such as energy suppliers or pharmaceutical manufacturers, the consequences can be devastating.

Against this backdrop, the EU's NIS 2 Directive, also known as the *Network and Information Systems Security Directive*, came into force on 16 January 2023. It must be transposed into Member States' national law by 17 October 2024 and replaces the 2016 NIS Directive. The main changes relate in particular to the extension of the scope and the personal liability of management bodies.

Background

With the original NIS Directive, which came into force in 2016, the EU aimed to establish a high common level of security for network and information systems. It served as a basis for national cybersecurity strategies and the establishment of *Computer Security Incident Response Teams* (CSIRTs) and required certain service providers to report cybersecurity incidents. However, it soon became clear that the rapidly changing threat landscape required the Directive to be expanded. The NIS 2 Directive was developed to meet these new challenges. It aims to improve cyber security in the EU through a comprehensive and risk-based approach. Instead of focusing on individual critical infrastructures, the Directive looks at the security of an organisation as a whole. This comprehensive approach means that a wider range of companies will have to meet higher risk management requirements in order to comply.

Extension of the scope of application

Material scope of application

The old NIS Directive applied to operators in essential sectors (energy, transport, banking, financial infrastructure, healthcare and drinking water supply) and

to providers of digital services. The NIS 2 Directive distinguishes between 'essential' and 'important' organisations. All sectors covered by the NIS Directive are included in the list of essential organisations in the NIS 2 Directive. However, the scope of the new Directive is broader than that of the old Directive and covers a total of 18 sectors, of which 11 are essential and 7 are important (Art. 3 NIS 2 Directive and Annex 1). This means that about 25,000 additional companies are covered in Germany alone.

The list of key facilities has been extended to include the following sectors:

- Public administration
- Management of information and communication technology services (ICT services)
- Waste water management
- Aerospace

The list of important sectors now includes:

- Post and courier services
- Food distribution
- Waste Management
- Chemical industry
- Manufacture of pharmaceuticals and medical devices

It should be noted that the Member States can still extend the scope of the Directive when transposing it into national law. In the German draft bill for the *NIS 2 Implementation and Cyber Security Strengthening Act* (NIS2UmsuCG), for example, 'operators of critical facilities' are included in the material scope of application in addition to essential and important facilities.

Thresholds

The NIS 2 Directive only applies to companies and organisations that are classified as at least medium-sized. This is the case if they have 50 or more employees and an annual turnover of more than EUR 10 million. The distinction becomes difficult for companies whose main activity does not fall under one of the establishment categories, but where a secondary activity of the company could fall under this category. Furthermore, the applicability of the NIS 2 Directive to a subsidiary does not automatically mean that the whole group of companies (even outside the EU) falls within the scope of the Directive. However, the affiliated companies may have to be taken into account when calculating the threshold.

Irrespective of the size and turnover of a company, certain exemptions are provided for if the company carries out a critical activity, has an impact on public policy or if there are systemic risks or cross-border effects.

Territorial scope

Geographically, the NIS 2 Directive applies to companies providing services or otherwise operating in the EU, irrespective of their place of establishment (Art. 2 NIS 2 Directive). The applicable law is determined by the establishment of a company in the relevant Member State. If a company has no place of business in the EU but provides services or otherwise operates in the EU, it must appoint a representative in the EU. The law of the representative's place of business is then applicable.

Increased security requirements

The NIS 2 Directive places increased security requirements on the companies and organisations concerned, which are further specified by the implementing laws of the Member States. These include:

- The implementation of comprehensive risk management tailored to the specific threats and vulnerabilities of each sector;
- The development and implementation of effective measures to respond to security incidents (*incident response*);
- Conducting regular security reviews and audits to ensure compliance with the policy.

Supply chains

The innovations in the area of supply chains are particularly relevant for companies. As interfaces between several companies, these are particularly susceptible to data transfers and companies are therefore particularly vulnerable, the Commission considers it necessary to strengthen the protection of supply chains. The following criteria, among others, must be taken into account:

- The extent to which essential and important facilities depend on critical ICT services, systems or products;
- The importance of these critical ICT services, systems or products for the performance of critical or sensitive functions;
- The availability of alternative services, systems and products;
- The resilience of the entire supply chain to destabilising events.

Extended reporting obligations

The NIS 2 Directive also extends the reporting obligations for cyber security incidents. Companies and organisations are obliged to report any significant threat to their network and information systems to the competent authorities within a short period of time. A security incident is considered significant if it has caused or is likely to cause a serious impairment of the functioning of services or financial losses for the organisation concerned, or has caused or is likely to cause significant material or immaterial damage to other natural or legal persons.

Personal liability of directors

Another important change concerns liability for breaches of the Directive. According to Art. 20 para. 1 NIS 2 Directive, the management bodies, i.e. managing directors, board members, etc., are personally liable with their private assets. National liability rules in the public sector remain unaffected. In addition, the management bodies of significant and important organisations are obliged to take part in training and to provide regular training to all employees.

Penalties

The penalties for violations are substantial. For significant facilities, the maximum fine is EUR 10 million or 2% of the previous year's worldwide turnover (Art. 34 para. 4 NIS 2 Directive). For significant establishments, the maximum fine is EUR 7 million or 1.4% of the previous year's worldwide turnover (Art. 34 para. 5 NIS 2 Directive). As the Directive only provides for minimum harmonisation, fines may be even higher in individual Member States. In addition, the competent authorities have supervisory and enforcement powers.

Enhanced cooperation and coordination

The NIS 2 Directive emphasises the importance of cooperation and coordination between Member States and between public and private actors. This includes the establishment and strengthening of CSIRTs in all Member States and their cooperation at European level (CSIRT network), as well as the establishment of a cooperation group to promote strategic cooperation and exchange of information between Member States. It also provides for the establishment of an early warning system to inform Member States of potential threats and incidents at an early stage.

Relationship with other regulations

The General Data Protection Regulation is not affected by the new NIS 2 Directive. The competent authorities under the NIS 2 Directive must cooperate with the data protection authorities and report data protection breaches in accordance with Art. 33 GDPR.

The Critical Entities Resilience Directive (CER Directive) is another component of the EU's cybersecurity approach and must be implemented by the Member States by 17 October 2024.

Recommendation

Member States must transpose the NIS 2 Directive into national law by 17 October 2024. Affected companies should therefore familiarise themselves in good time with the NIS 2 Directive and the draft transposition laws of the respective Member States, as these fully specify the requirements of the Directive. This is likely to involve considerable effort, particularly for companies that have not previously fallen within the scope of the Directive. In Germany, for example, the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*) offers an NIS 2 impact assessment on its website for companies that are unsure whether they are affected by the Directive.

A comparison shows that the ISO 27001:2022 standard (Information Technology - IT Security Procedures - Information Security Management Systems Requirements) already meets many of the requirements of the NIS 2 Directive. There are also some similarities with ISO 27002:2022 (Information Technology IT Security Procedures Guide for Information Security Management). For example, the governance requirements of Art. 20 NIS 2 Directive can be found in Art. A.5 OF ISO 27001:2022.

A GAP analysis, which shows the deviation of the actual state from the target state, is useful. As a first step, the German Federal Office for Information Security recommends appointing a responsible person, assuming management responsibility, carrying out an initial inventory, improving information security and preparing for reporting obligations.

+ + +

The Alliuris Group

The Alliuris Group consists of 20 law firms and 400 business lawyers within Europe, Asia and America.

Contact	Ulrich Herfurth Alliuris Communication
Web	www.alliuris.law
Mail	info@alliuris.org
Fon	+49 511 307 56 20
Fax	+49 511 307 56 21

Alliuris in Germany

Firm	Herfurth & Partner Luisentraße 5, D-30159 Hanover
Web	www.herfurth.de
Fon	+ 49 511 30756 0
Fax	+ 49 511 30756 10
Mob	
Contact	Ulrich Herfurth, Partner
Language	German, English, French, Spanish, Portuguese, Russian, Mandarin, Czech, Polish
Mail	info@herfurth.de

IMPRINT

EDITORS: ALLIURIS A.S.B.L. ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS | BRUSSELS

MANAGEMENT: Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-20, Fax +49-511-307 56-21

BRUSSELS · PARIS · LONDON · AMERSFOORT · UTRECHT · KNOKKE · LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · SALZBURG · MOSCOW MINSK · ATHENS · ISTANBUL · BEIJING · SHANGHAI · GUANGZHOU NEW DELHI · MUMBAY · NEW YORK · MEXICO CITY SAO PAULO · RIO DE JANEIRO · BRASILIA · BUENOS AIRES · LIMA

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt