# Trends and Developments

**Contributed by:**
Stéphanie De Smedt, Virginie de France, Bram Goetry and Olivier Verhasselt
**Loyens & Loeff**

**Loyens & Loeff** is a leading law and tax firm, and the logical choice for businesses in the Netherlands, Belgium, Luxembourg and Switzerland (its four home markets). With over 1,000 advisers in its Benelux and Swiss offices and key financial centres worldwide, Loyens & Loeff offers customised, innovative advice. The firm's cybersecurity team excels in identifying, assessing and mitigating risks through pragmatic expert advice, both in a transactional and a litigation context. Loyens & Loeff develop and implement policies and contractual frameworks, manage regulatory reporting and investigations and advise on compliance with laws like the GDPR, the NIS2 Directive and the Cyber Resilience Act. The firm's services also include compliance audits, due diligence assessments and tailored training for board members, general counsels and employees on cybersecurity risks, regulations and best practices.

## Authors

**Stéphanie De Smedt** is a partner in the Brussels office of Loyens & Loeff. She is an expert in commercial and IP/ICT law, and is the go-to person for clients active in the digital economy and tech sector. Developments such as artificial intelligence and the regulation of new technologies in general are among Stéphanie's core focus areas. She has developed recognised expertise with respect to regulatory compliance – more specifically as a CIPP/E-certified expert – in relation to the protection of personal data, cybersecurity and life sciences. Stéphanie is a member of the International Association of Privacy Professionals (IAPP) and of iTechLaw.

**Virginie de France** mainly focuses on ICT law, more specifically data protection law and cybersecurity. In her position as lawyer and professional support lawyer at Loyens & Loeff, she oversees and manages all aspects of the team's know-how, but also advises and represents clients in her fields of expertise. Virginie is a member of the Brussels Bar.

**Bram Goetry** is an associate at the Brussels office of Loyens & Loeff. He focuses on data protection law and cybersecurity, and general commercial and intellectual property law, and he advises and represents clients in both litigious and non-litigious matters in these fields of expertise. Bram is a member of the Brussels Bar.

**Olivier Verhasselt** is an associate at the Brussels office of Loyens & Loeff. Olivier mainly focuses on data protection law and privacy, but also has broader expertise in all areas of IP/IT law and general commercial law. He advises and represents clients in both litigious and non-litigious matters in these fields of expertise. Olivier is a member of the Brussels Bar.

## Loyens & Loeff

Tervurenlaan 2
1040 Brussels
Belgium

Tel: +32 2743 4343
Fax: +32 2743 4310
Email: Info.brussels@loyensloeff.com
Web: www.loyensloeff.com

LOYENS & LOEFF
Law & Tax

**Contributed by:** Stéphanie De Smedt, Virginie de France, Bram Goetry and Olivier Verhasselt, **Loyens & Loeff**

## Introduction

As digital transformation accelerates and cyberspace becomes increasingly complex, cybersecurity has emerged as a critical concern for organisations. The deep interconnectivity of the cyber-ecosystem means that a breach in a single entity can trigger a chain reaction, compromising entire networks with far-reaching consequences. Even the smallest vulnerabilities in digital systems can lead to significant disruptions, from financial losses to reputational damage.

For many organisations, cybersecurity is no longer merely an operational concern – it is also a legal imperative. In 2024, Belgium was the first EU member state to transpose Directive (EU) 2022/2555 (the "NIS2 Directive") into national law (the "NIS2 Law"). As a direct consequence thereof, 2025 is set to be an intense year as this landmark legislation is expected to impact over 2,500 entities across a wide range of sectors. In addition to implementing risk management measures, organisations will need to review their contracts with suppliers and subcontractors and ensure that future agreements explicitly include cybersecurity warranties. Management bodies will also be heavily involved, as the law imposes numerous obligations and responsibilities on them. Compliance with the NIS2 Law is overseen and enforced in Belgium by the Centre for Cyber Security (the CCB).

Below is an overview of the main cybersecurity trends the authors see for 2025.

## CyberFundamentals as a Cybersecurity Framework Originating in Belgium, but Potentially With Much Broader Recognition

Under the NIS2 legislation, certain entities are required to undergo periodic compliance assessments, which result in certification. In Belgium, only two certifications are recognised by law:

- the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 certification; and
- the Belgium-specific CyberFundamentals ("CyFun") certification scheme.

The latter is a certification granted by a conformity assessment body approved by the CCB. The framework is based on commonly used cybersecurity frameworks, namely the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), ISO 27001/ISO 27002, Center for Internet Security (CIS) Controls and IEC 62443. To address the varying levels of risk organisations face, the framework offers four assurance levels: small, basic, important and essential. The CyFun framework is generally deemed to be less burdensome (and less expensive) to implement than ISO certification, and the CCB has also published a multitude of online guidance notes and tools to aid implementation thereof by Belgian companies.

Interestingly, Romania has already implemented the NIS2 Directive, and has explicitly recognised the Belgian CyFun certification scheme as a valid compliance framework under its local law.

Following the Romanian example, CyFun, although initially a local Belgian initiative, could receive broader international recognition, with more countries expected to follow Romania's lead.

## Cybersecurity Clauses as a "Must Have" for Both Current and Future Contracts

In cases where IT services are outsourced, the legal responsibility under cybersecurity legislation (eg, NIS2 and DORA) remains with the in-scope organisation itself. Therefore, it is crucial for these organisations to properly map the various contactors, suppliers, service provid-

ers, etc, that have access to their IT systems, provide cloud-based software solutions or may otherwise impact the organisation's cybersecurity risk profile.

In Belgium, the authors are seeing a clear trend towards companies requesting additional cybersecurity-related guarantees and certifications from their suppliers. Since past cyber-attacks have highlighted the intrinsic link with various ecosystems, cybersecurity clauses are becoming a key concern in supply chain risk management.

More specifically, the authors see an increased focus on the following types of clauses in various types of commercial (supply/services) contracts, not only in the IT sector:

- clauses setting minimum standards and obligations of result in relation to cybersecurity (obtaining and maintaining certifications, annexes with detailed lists of technical and organisational measures to implement, etc) for the supplier;
- clauses ensuring swift incident reporting by suppliers, in order for the client – which may be a regulated entity under NIS2 or the Digital Operational Resilience Act (DORA) – to meet its own legal reporting obligations, often detailing reporting deadlines, mandatory information to be provided and co-operation obligations;
- clauses providing extensive cybersecurity audit rights for the client;
- liability and exoneration clauses (a higher or no liability cap for cyber-incidents, indemnification obligations for third-party claims, etc); and
- termination clauses in case of serious cyber-incidents or material non-compliance, etc.

While the arrangements for cybersecurity are in some cases set out in a lot of detail in the legislation itself (see DORA), this is not always the case (see NIS2), which leaves a lot of room for diverging practices and tough negotiations. In 2025, the authors expect more common practices and standards to develop in this respect – as it did for data processing agreements under the General Data Protection Regulation (GDPR), for example.

The focus on supply chain risk management will in any event remain in 2025. Noteworthy in this respect is the finding that, of all large organisations, 54% identified supply chain challenges as the biggest barrier to achieving cyber-resilience. The increasing complexity of supply chains, coupled with a lack of visibility and oversight regarding the security levels of suppliers, has emerged as the leading cybersecurity risk for organisations. Key concerns include software vulnerabilities introduced by third parties and the propagation of cyber-attacks throughout the ecosystem, as noted in the World Economic Forum's Global Cybersecurity Outlook 2025.

### Leaders Must Adopt a "Security-First" Mindset

The NIS2 legislation requires management bodies to play an active role in cybersecurity, making their involvement not only beneficial but also legally mandatory. The authors expect this to become a board-level priority in 2025.

More specifically, management bodies of NIS2-in-scope entities must:

- approve risk management measures related to cybersecurity and oversee their implementation;
- complete training to ensure they possess the necessary knowledge and skills to identify risks, assess cybersecurity risk management

practices and understand their impact on the services provided by their organisation (this entails an obligation for management to follow regular cybersecurity awareness trainings); and
- ensure the organisation's compliance with the law.

As the concept of "management body" is not defined in the NIS2 Directive, the explanatory memorandum to the Belgian NIS2 Law defines a "member of a management body" as "Any natural or legal person who:

1. exercises a function within or in relation to an entity which authorises him or her (a) to administer and represent the entity in question or (b) to take decisions in the name and on behalf of the entity which are legally binding on it or to participate, within a body of that entity, in the taking of such decisions, or
2. has control over the entity, meaning the power, in law or in fact, to exercise decisive influence over the appointment of the majority of the entity's directors or managers or over the direction of the entity's management".

Where the entity is a company governed by Belgian law, this control is determined in accordance with Articles 1:14 to 1:18 of the Belgian Code of Companies and Associations.

Moreover, if an organisation that is in-scope of NIS2 fails to comply with the NIS2 Law, then its management body may be held accountable and face not only director's liability, but also a temporary ban from holding executive responsibilities within the organisation. It remains to be seen how this liability will be assessed in practice, and in which situations (likely only very extreme ones) the CCB would impose such a temporary ban.

While 2025 will likely still be a year of transition, enforcement of the NIS2 Law by the CCB is expected to gradually increase, especially in case of major cybersecurity incidents in critical or public sectors.

### The Role of the CCB and the Data Protection Authority in Cybersecurity Compliance

The CCB has been designated by the NIS2 Law as the national authority responsible for the monitoring, supervision and enforcement of the NIS2 Law on Belgian territory. However, entities may also have to face another authority in the context of cybersecurity: the Belgian Data Protection Authority (DPA), which oversees the enforcement of the GDPR and national legislation concerning personal data protection. Indeed, the DPA is often called upon to examine IT systems and their use within companies, particularly due to the risks of personal data breaches, becoming a valuable asset in the event of cybersecurity incidents. The NIS2 Directive itself acknowledges in its recitals that personal data protection and cybersecurity are closely linked.

As a result, when a company suffers a cyberattack leading to a personal data breach – a common occurrence – it often finds itself engaging with multiple authorities, sometimes including sectoral regulators, while also adhering to tight deadlines and different formal requirements. Firstly, companies subject to the NIS2 Law must notify significant incidents to the CCB without undue delay, at the latest within 24 hours of becoming aware of the incident. Additionally, these companies must also notify the DPA if the incident constitutes a personal data breach under data protection law, and this must

be done no later than 72 hours after becoming aware of the breach.

The NIS2 Law does not provide amendments or exemptions to the GDPR in this regard. For initial notification, many companies will therefore first notify the CCB and then prepare their notification to the DPA. A late notification can lead to sanctions for non-compliance, as well as a broader investigation by the relevant regulatory authority.

The only exemption to the obligation to notify in the case of a personal data breach is provided by Article 74 of the NIS2 Law. According to this article, the data controller may be exempted from notifying a personal data breach to certain affected individuals, as provided in Article 34 of the GDPR. This exemption is possible subject to the CCB's approval, where such individual notification could jeopardise the control and supervision of the entities, as well as the preparation, organisation, management and follow-up of administrative measures and fines. However, it is important to note that this exemption only applies to the obligation to notify the affected individuals, not the authorities.

Therefore, it is essential that entities systematically notify incidents involving personal data to both relevant authorities, in accordance with the requirements and procedures of both pieces of legislation. This approach also aligns with the "cyber incident response plan" model published by the CCB, which explicitly mentions the CCB and the DPA among the entities that should receive a report.

The next natural question is whether, following a notification and any subsequent investigation by the CCB and the DPA, a company could face two fines, one under the NIS2 Law and another under the GDPR. The fourth Title of the NIS2 Law states that the CCB or any competent sectoral authority will not impose an administrative fine for an infraction resulting from the same behaviour for which an administrative fine has already been imposed by the DPA. Instead, they may decide to impose alternative sanctions for the same actions (eg, requiring the entities involved to make certain aspects of the violations public). However, neither the NIS2 Law nor the GDPR or its implementing legislation provide a solution where the CCB first imposes an administrative fine, and the DPA then decides to do the same. However, it is reasonable to expect that a similar approach will be applied in such a case, by analogy with the criminal law principle of non bis in idem.

### Ethical Hacking in Belgium Is Legal, Under Certain Conditions

Since 15 February 2023, in the context of the entry into force of a new whistle-blower law, the Belgian legislator has legalised "ethical hacking". Under certain conditions, ethical hackers are protected against criminal liability, even where the hacked organisation did not consent to being subject to such "testing" of their cybersecurity standards.

Traditionally, the term "hacker" evokes individuals who exploit security flaws in IT systems for malicious purposes, such as extortion, sabotage or data theft. However, there are also hackers with good intentions, known as "ethical hackers". "Ethical hacking" refers to the practice of testing an organisation's systems and networks to identify and fix potential vulnerabilities without any fraudulent intent.

Until 18 October 2024, any natural or legal person was allowed to search for and report security vulnerabilities, even outside a co-ordinated

vulnerability disclosure policy, without risking criminal prosecution, provided that they comply with certain conditions:

- there is no intent to cause harm or to obtain illegitimate benefits (eg, they cannot request payment, unless this has been agreed upon in advance, such as in the context of bug bounty programmes);
- the vulnerabilities they discover must be reported to the CCB without delay, as well as to the organisation they "hacked" – to gain some control over this process and safeguard both confidentiality and a streamlined notification process, several companies have already set up ethical hacking policies and dedicated communication channels;
- the hacker cannot do anything that goes beyond what is necessary and proportionate in order to uncover a cybersecurity vulnerability; and
- the hacker is prohibited from publicly disclosing the discovered vulnerabilities without prior authorisation to do so from the CCB.

However, in 2024, the NIS2 Law narrowed the previous general liability exemption for ethical hacking to a specific list of defined offences:

- interception of private communications (Article 314bis of the Criminal Code);
- violation of professional secrecy (Article 458 of the Criminal Code);
- hacking (Article 550bis of the Criminal Code);
- IT sabotage (Article 550ter of the Criminal Code); and
- offences related to telecommunications legislation.

Other offences, such as breaking and entering, are not included.

In other words, ethical hacking is now only permitted for conventional cyber-attacks involving remote access to IT systems. Physical attacks on these systems are no longer legally protected and require prior authorisation from the competent authorities. Otherwise, perpetrators face criminal prosecution, including charges of breaking and entering.

Furthermore, the four conditions established in 2023 remain in effect and are further clarified by the NIS2 Law, which entered into force on 18 October 2024.

- Proportionality and necessity: The hackers must limit themselves to the actions strictly necessary to demonstrate the existence of a vulnerability, without exceeding what is needed to prove the security flaw. This also means they are prohibited from disrupting the target organisation's services, even if an investigation is ongoing.
- No harm or blackmail: The hacker must never intend to cause harm or obtain sensitive information from the targeted company. Any form of blackmail, such as threatening to disclose vulnerabilities in exchange for benefits, is strictly prohibited.
- Reporting vulnerabilities: The hacker must promptly submit a simplified notification that includes the identification of the affected system and a brief description of the potential vulnerability, no later than 24 hours after its discovery, to both the organisation responsible for the system and the CCB. The hacker must submit a complete notification, without delay and no later than 72 hours after its discovery, to both the organisation responsible for the system (if applicable, in accordance with the reporting procedures established by that organisation) and the CCB. It is also important to note that disclosing information

publicly without prior consent from the CCB is strictly forbidden.
- Legal responsibility: The legislation on ethical hacking does not protect against potential violations or prosecutions under foreign laws. Hackers can still face legal action based on the legislation of other countries.

With the Belgian NIS2 Law reinforcing the legal framework for ethical hacking and the 2025–29 federal coalition agreement of the new Belgian government granting law enforcement agencies the authority to collaborate with ethical hackers, organisations are advised to be aware of the applicable legal requirements to protect themselves against potential abuse.