Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2026

Definitive global law guides offering comparative analysis from top-ranked lawyers

Belgium: Trends and Developments

Stéphanie De Smedt
Loyens & Loeff

BELGIUM

Trends and Developments

Contributed by:
Stéphanie De Smedt
Loyens & Loeff

Loyens & Loeff is a leading law and tax firm, and the trusted partner for businesses in the Netherlands, Belgium, Luxembourg and Switzerland. With more than 1,000 advisers across Benelux and Swiss offices and key financial centres worldwide, it delivers integrated legal and tax solutions tailored to clients' needs. The firm's multidisciplinary approach combines deep sector knowledge with pragmatic, business-oriented advice. It is recognised for excellence in corporate, M&A, tax, dispute resolution and regulatory matters, and for its niche expertise in privacy, cybersecurity and technology law. Clients value the firm's responsiveness, technical strength and ability to handle complex cross-border issues efficiently. Loyens & Loeff invests in innovation and client-focused solutions, ensuring compliance and risk management in a rapidly evolving legal landscape.

Author

Stéphanie De Smedt is a partner in Loyens & Loeff's Brussels office and leads the firm's privacy and cybersecurity team. She has extensive experience in guiding clients through complex regulatory landscapes (GDPR, NIS2, AI Act, etc) and assists clients in setting up compliance frameworks, performing regulatory risk assessments, and drafting and negotiating commercial and technology agreements. She also advises on pre-litigious matters and represents clients in regulatory audits and enforcement proceedings. With a broad background in commercial contracts and IP/ICT law (including technology transfers, e-commerce and software/IT contracting), Stéphanie is the go-to person for clients active in the technology industry.

Loyens & Loeff

Avenue de Tervueren 2
1440 Etterbeek
Belgium

Tel: +32 773 2377
Email: Stephanie.de.smedt@loyensloeff.com
Web: www.loyensloeff.com

Contributed by: Stéphanie De Smedt, **Loyens & Loeff**

Introduction

Cybercrime has significantly increased in recent years, with a growing number of ransomware attacks, increasingly sophisticated phishing campaigns, and major data breaches affecting both private companies and public institutions. As a result, cybersecurity has become a key strategic concern in Belgium for both the public and private sectors.

The regulatory landscape in this area remains under construction, with certain legislation already in force and other requirements set to apply in the coming years, as follows.

- Following the transposition of EU Directive 2022/2555 (the "NIS 2 Directive") into Belgian law at the end of 2024, many entities are still investing considerable resources to achieve NIS 2 compliance. From 2026, entities that have opted for the "Basic" or "Important" frameworks will be required to have their initial self-assessments verified by a "Trusted NIS Provider" and approved by the Centre for Cybersecurity Belgium (CCB).
- Belgium is expected to transpose EU Directive 2022/2555 (the "CER Directive") in 2026 – a process that should have been completed by October 2024.
- While EU Regulation 2024/2847 (the "Cyber Resilience Act", or CRA) will generally apply from 11 December 2027, its Article 14 will become applicable as of 11 September 2026, and its Chapter IV (Articles 35 to 51) shall apply from 11 June 2026.

An analysis of some of these topics and developments follows.

CCB Publishes Second Version of the NIS 2 FAQ

In 2025, the CCB released a second version of its FAQ, clarifying several key aspects of the Belgian NIS 2 implementation act (the "NIS 2 Law").

The main points clarified by the CCB include the following.

- Ancillary activities may trigger NIS 2 applicability: a company whose principal activity falls outside the scope of the (exhaustively listed) NIS 2 sectors but that engages, even marginally, in activities listed in the annexes to the NIS 2 Law will be considered "in-scope". The primary or ancillary nature of the activities do not, as such, matter for NIS 2 applicability to be triggered. In such cases, the size calculations for the applicability assessment will encompass the entire entity, and not merely the activities deemed to be "in-scope".
- Application of NIS 2 to groups of companies: the size thresholds for determining NIS 2 applicability are to be calculated on a group level, taking into account the employees and financials of partnered and linked enterprises. Conversely, the relevant in-scope activities should be assessed for each legal entity individually. When assessing the scope of NIS 2 within a group of companies, every legal entity must analyse, on its own, whether its activities and services bring it within the scope of NIS 2. The mere sharing of data, networks or information systems within a corporate group does not, in itself, determine or alter the applicability of NIS 2. However, it is possible for a NIS 2 entity to be subject to several pieces of transposition legislation and competent supervisory authorities throughout the EU. This is the case when, within the same group, entities are established in multiple EU member states and are not subject to the main establishment criteria (which apply only to certain entities providing digital services).
- Intra-group provision of managed IT services or cloud services: although highly criticised for this position, the CCB takes the view that entities providing IT management or cloud services to affiliates (ie, in a purely intra-group situation) fall within the scope of activities covered by NIS 2 (provided that the size thresholds are also met at group level). Even where the main operational activities of a group have no relation at all to NIS 2 in-scope activities, NIS 2 applicability may therefore be triggered purely by the way in which a group is structured internally (namely by centralising intra-group IT management within one entity). Conversely, the CCB notes that the situation differs when multiple organisations within the same group share data, networks or systems and distribute costs, without any entity actually acting as a managed service provider for the others. The same reasoning applies if an entity enters into a contract with a NIS 2 service provider and allows this contract/service

to be used by its affiliates. In such case, the NIS 2 services continue to be provided by the NIS 2 service provider and not by the contracting entity. The scope of "managed IT services" activities and their application in an intra-group context therefore remains a delicate and debated topic in Belgium in 2026.

- NIS 2 in M&A: NIS 2 has become an important point of attention in M&A transactions in Belgium, notably as the NIS 2 qualification of an entity that undergoes a change of control may change. While NIS 2 applicability does not automatically transfer to the acquirer of an in-scope entity, both the calculation of size thresholds and the identification of in-scope activities may change after an acquisition. For example, depending on the service provided by the NIS 2 entity, an increase in size (because the acquiring group is much larger than the seller group) may trigger a post-closing qualification as an "Essential" rather than "Important" entity. Intra-group IT arrangements (see "managed IT services", as discussed above) may trigger (or "de-trigger") NIS 2 applicability. A re-assessment of NIS 2 applicability post-M&A (and, even better, as part of due diligence in order to assess potential additional cost/financial implications) is therefore highly advisable.
- Civil and criminal liability of the management board: Article 31, Section 1 of the NIS 2 Law provides that management bodies are liable for breaches of cybersecurity measures. The CCB refers to the general principles of liability under Belgian law. The liability of legal entities is, in principle, engaged through the actions of their representative organs, as provided by Article 2:49 of the Companies and Associations Code. In addition, civil liability of members of management or supervisory bodies may also be engaged under the theory of cumulative liability, pursuant to Articles 2:56 to 2:58 of the Companies and Associations Code, where the fault is tortious and clearly exceeds what a prudent and diligent director would have done under the same circumstances. Regarding criminal liability, the CCB explicitly notes that the NIS 2 Law does not exclude criminal liability of either legal or natural persons.
- Content of management training: while the NIS 2 Law requires members of management bodies to receive cybersecurity training, the CCB has clarified in interviews that there are no mandatory training centres, certificates or prescribed content or methods for the delivery of such training. The CCB's FAQ, however, does specify the objective of such training: "*The purpose of training members of the management body is to enable them to properly perform the duties assigned to them under the law, ie, to approve cybersecurity risk-management measures and to supervise their implementation. There is no prescribed content or duration; both are left to the discretion of the entity." The CCB further distinguishes between "Important"* and "Essential" entities, implying that training expectations may vary depending on the entity's NIS 2 classification. Accordingly, each organisation is responsible for determining the scope, format and duration of the management training, ensuring that members of management are adequately equipped to fulfil their supervisory and decision-making responsibilities under NIS 2.

Cybersecurity Measures to Gain a Competitive Edge in the Supply Chain

Cybersecurity is no longer evaluated solely within the boundaries of an organisation's own systems: it is assessed across the entire value chain. Indeed, supply chains have become one of the most common vectors for cyber incidents, and the NIS 2 Directive requires in-scope entities to implement specific cybersecurity measures to manage their supply chains. As a result, in-scope organisations impose obligations on their suppliers, including those not directly subject to NIS 2, which are now increasingly indirectly impacted by this legislation.

Many suppliers have understood that they can gain a strategic advantage by embedding cybersecurity into their operations. By adopting robust security practices, they strengthen client and partner trust, increase operational resilience, and position themselves as more competitive players in the market. This trust translates into tangible commercial value. Customers are more likely to work with suppliers who can demonstrate effective management of third-party risks, particularly when services are business-critical or involve sensitive data. In competitive tenders, credible cybersecurity governance can serve as a clear differentia-

tor, especially where price or functionality alone would not suffice. What was once a distinguishing feature of the most security-conscious organisations is rapidly becoming a baseline expectation across the market.

CyFun® 2025 as a Major Framework in Belgium

Since the entry into force of the NIS 2 Directive in Belgium, many organisations have adopted the Belgian CyFun® framework.

CyFun® is a structured framework providing:

- a standardised approach for risk assessment and cybersecurity controls aligned with Belgian and EU legal requirements;
- modular frameworks ("Basic", "Important", "Essential") allowing organisations to calibrate security measures according to size, criticality and sector; and
- a documentation and verification process facilitating audits by "Trusted NIS Providers" and approval by the CCB.

The key advantage of CyFun® lies in providing a common language for authorities, auditors and organisations, reducing ambiguity about what constitutes satisfactory NIS 2 compliance. It is designed to:

- systematically assess vulnerabilities and risks in information systems;
- define corrective and preventative action plans for identified weaknesses; and
- provide clear, traceable reporting for regulatory inspections and audits.

It is important to note that CyFun® certification also grants a legal presumption of compliance with the Belgian NIS 2 Law.

Although developed at a national level in Belgium, CyFun® is designed for recognition and use at a broader EU level. Romania has already officially adopted the framework, and several other EU member states, including France, acknowledge CyFun®'s value and are exploring integration or full adoption.

Transposition of CER Directive into Belgian Law

The law transposing the Critical Entities Resilience Directive into Belgian law is expected in 2026. This represents a significant step toward completing the long-overdue transposition, which was initially required by 17 October 2024. This new legislation will replace the Critical Infrastructures Directive (2008/114/EC) and its 2011 Belgian transposition law.

The sectors covered by the CER Directive are similar to NIS 2, although the list is not identical:

- energy;
- transport;
- banking;
- financial market infrastructures;
- digital infrastructures;
- drinking water;
- wastewater management;
- central public administration;
- space; and
- food.

Whereas NIS 2 focuses on the cybersecurity of networks, information systems and data, the CER Directive adopts a broader approach aimed at the overall resilience of critical entities. It addresses all risks (physical, natural, human or cyber) that could disrupt the provision of essential services.

The two laws are thus complementary: NIS 2 governs digital security, while CER ensures the operational continuity and robustness of critical infrastructures. Entities designated as "critical" under CER will generally also be considered "essential" under NIS 2.

For sectors subject to detailed European regulatory regimes (notably banking, financial market infrastructures and digital infrastructures), certain CER provisions may not apply when equivalent sector-specific obligations exist.

Companies' principal obligations under the CER Directive are as follows.

- Threat and risk assessment: critical entities are required to carry out a comprehensive risk assessment within nine months of being designated,

and subsequently at least every four years. These assessments should consider interdependencies and relevant national and EU evaluations.
- Resilience measures and planning: entities must develop, maintain and execute a resilience plan, incorporating technical, organisational and security measures that are proportionate to the risks identified.
- Reporting of incidents: significant incidents should be reported to the relevant authorities within 24 hours, with a detailed follow-up report submitted within a month if applicable.
- Co-operation and information exchange: the CER Directive encourages close collaboration with competent authorities and requires the sharing of essential information to align internal resilience efforts with external protective measures.
- Personnel screening: in compliance with national legislation and data protection requirements, entities may perform background checks on specific categories of personnel.
- Continuity and staff security: operational continuity measures, personnel security and training are typically included as part of the entity's overall resilience strategy.

Entities providing essential services in six or more EU member states are subject to special compliance procedures due to their European significance.

In accordance with the draft CER implementation law, a number of additional provisions will apply in Belgium compared to the general framework set out in the CER Directive.

- Resilience exercises and plan updates: critical entities are required to periodically carry out exercises to evaluate their resilience plans and update them based on lessons learned. Royal or ministerial decrees may set sector-specific schedules for these exercises, and define the participation of relevant government bodies.
- Sector-specific plan content and reporting: authorities in each sector may specify mandatory elements of resilience plans and require additional reporting or information from critical entities.
- Enhanced co-operation principle: a general expectation of collaboration between critical entities and competent authorities to align internal resilience efforts with broader external protection measures.
- Sanctions framework:
  (a) Administrative sanctions: fines range from EUR500 to EUR125,000, doubling if a second offence occurs within three years of a prior final sanction. Suspensions of payment may be permitted under certain conditions.
  (b) Criminal sanctions: penalties include imprisonment from eight days up to one year and/or fines of between EUR26 and EUR10,000 (to be multiplied with an indexation factor of eight), with harsher consequences for repeat offenders.
- Governance and compliance deadlines: enforcement is primarily managed by sectoral authorities, in contrast to the more centralised approach under NIS 2 (led by the CCB). Critical entities are expected to meet their initial obligations within six months of their explicit designation under the CER law.

Conclusion – Key Points to Keep in Mind

Belgium is rapidly advancing its cybersecurity and critical infrastructure regulatory framework, aligning closely with EU directives.

Organisations must recognise that compliance is not optional; it is a strategic necessity affecting internal operations as well as supply chain relationships and market competitiveness.

The CCB's latest NIS 2 FAQ provides useful clarifications.

The CyFun® framework has emerged as a major tool in Belgium (as well as in certain other EU jurisdictions) for achieving structured, auditable and EU-recognised compliance. Its adoption helps organisations demonstrate adherence to NIS 2 standards while also facilitating cross-border recognition and audit processes.

The CER Directive is expected to be transposed in Belgium in 2026, and requires organisations to prepare for sector-specific obligations, resilience planning, reporting and co-operation with authorities. The introduction of sanctions underscores the importance of proactive compliance.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com