14 October 2025

Position of the European Express Association (EEA)

The Digital Omnibus – Focus: Network & Information Security Directive 2 (NIS 2)

Introduction

The **European Express Association (EEA)** is pleased to provide its feedback to the **European Commission's Call for Evidence on the Digital Omnibus Package**. The EEA welcomes the Commission's continued commitment to simplifying and streamlining the EU's digital regulatory landscape, which plays a central role in enabling innovation, competitiveness, and efficiency across the European economy.

The express delivery sector, as an essential enabler of trade, operates at the intersection of logistics, technology, and cybersecurity. The EEA therefore strongly supports the Commission's efforts to **identify and reduce unnecessary administrative burdens, eliminate regulatory overlaps, and foster a coherent, predictable, and innovation-friendly framework for businesses and public authorities alike**.

The **Digital Omnibus** comes at a **crucial moment**. It provides an opportunity to **simplify and rationalize existing digital legislation** on **cybersecurity,** while ensuring that the rules remain **effective, proportionate, and future-proof**. By enhancing clarity and alignment across the EU, the initiative can help **national authorities and Member States** achieve greater **harmonization** in **implementation**, thereby supporting the integrity of the Single Market.

In this context, the EEA particularly welcomes the focus on **cybersecurity and incident reporting obligations**, as these are areas where fragmented national implementation continues to pose challenges for cross-border operators like the EEA Members operating in all Member States which leads to language and procedural challenges. At the same time, EEA maintains the importance of a level playing field for all market players; the same rules shall apply, as harmonized as possible. **Entered into force in January 2023, the Network and Information Security (NIS2) Directive** is the EU's main legislative instrument for cybersecurity. We support NIS2 as **vital for protecting European businesses and supply chains**; we are **promoting a smooth and harmonized roll-out of NIS2** across the Union.

We encourage the European Commission to **pursue simplification of several aspects and support Member States** in the implementation **through targeted guidance** and coordination. A more consistent approach will ensure that cybersecurity regulation remains **effective, proportionate, and**

innovation-driven, supporting **business resilience**. We have invested and continue to invest in technology security initiatives, information technology risk management and disaster recovery plans.

In more detail: Cybersecurity & NIS 2 (2022/255)

In view of the upcoming digital omnibus framework, we would like to put forward the following recommendations:

EU-wide harmonization of implementation

Status quo:

Since the co-legislators agreed on the regulatory measure of a "Directive" when developing the NIS 2, the regulatory requirements are implemented differently across the EU's 27 Member States. For example, Member States are adopting varying approaches in terms of incident notification processes, entity classification (ranging from single-tier to three-tier systems), sector coverage (with some states expanding scope), and size-cap thresholds. This regulatory fragmentation means organizations may face different compliance and international operational requirements across jurisdictions, even when providing identical services. For instance, up to 27 separate incident notifications across 27 different jurisdictions may be triggered for only one single incident. Therefore, a company's NIS2 compliance in one country does not necessarily imply compliance and operational alignment in another.

Proposed simplification:

To reduce the implementation efforts for companies and to ensure the risk adequate level of cyber-resilience across the Union, the Commission should drive uniform national implementation of NIS2 and issue central guidance for a pragmatic, harmonized interpretation of key terms, including "significant incident" and "establishment/main establishment" as well as unique reporting templates. For highly interconnected, cross-border sectors such as transport and logistics, a "main establishment" concept should allow single registration and coordination for groups operating in multiple Member States, avoiding duplicative registrations and divergent local add-ons. In the next review, the EU should consider moving from a directive to a regulation to secure full harmonization of scope, timelines and obligations.

Reporting obligations (Article 23)

Status quo:

Article 23 of the NIS 2 Directive requires all essential and important entities to report every cybersecurity incident which has significant implications for their services. In case of a significant cyber security incident, companies must fulfil three to five reporting obligations. In many cases, companies may not have enough information to understand how significant an incident is, nor whether it was caused by an unlawful or malicious actor, within 24 hours, with a second report to follow within 72 hours. Upon request of a CSIRT or, where appropriate, the competent authority, can request an interim report on relevant status updates. Moreover, companies must submit a final report no later than one month after the submission of the notification of the incident. In case of an ongoing security incident at the time of submission of the final report, the organization concerned must submit a progress report at that time and a final report within one month of the handling of the security incident. There is also a different approach among the Member States about what a "significant incident" entails.

Proposed simplification:

Harmonized three stage incident reporting

The EEA urges the European co-legislators to harmonize the scope and definitions of reportable incidents across all 27 Member States and to align the initial notification timeline with the one required by the GDPR. Specifically, the initial report should be submitted without undue delay and, in any event, within 72 hours of becoming aware of a significant incident (replacing the current 24-hour requirement to reduce false positives and enable accurate triage; a 48 hour target may be used where feasible). The second (interim) report should be due 14 days after the initial report, and the final report should be due one month after incident closure, where necessary (i.e., unless already covered in the interim report). This calibrated timeline gives entities sufficient time to determine scope, root cause, and impact.

In addition, the EEA underlines the importance of harmonising reporting deadlines across related regulatory domains. In particular, there should be greater alignment between the timelines for cybersecurity incident reporting under NIS 2 and those applicable to **aviation security (AVSEC) occurrence reporting**. Harmonising these reporting deadlines would simplify compliance for operators active in both areas, reduce duplication of effort, and promote a coherent and efficient approach to incident notification across the Union.

Aligned definitions and templates
To ensure consistency, the definition of a "significant incident" should reference the ENISA definition[1] (Document C(2024)7151, page 10) and be used consistently across all relevant EU legislation. The EEA also recommends standardized, English language reporting templates and common data formats to reduce administrative burden for cross border operators and support harmonized implementation.

One stop shop reporting
Enable a single submission for NIS2 / CRA / DORA / GDPR/ EU AI Act through an ENISA operated EU hub, which would disseminate notifications to national CSIRTs/NCAs. This should include:

- Acceptance of one report for cross border incidents,
- Avoidance of duplicate sanctions, and
- A single, aligned timeline capped at the three reports (initial, interim, final).

Support secure authentication, e.g., via EUDI Wallet. Until the EU hub is operational, require national one stop shops with a single endpoint at least for NIS2 and CRA submissions.
Procedure:

Critical components & certificates (Article 24(2))
Status quo:
In case of insufficient levels of cybersecurity, under NIS 2 Article 24 paragraph 2, the European Commission is empowered to adopt delegated acts, in accordance with Article 38, to supplement the NIS 2 Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881. This could lead to overlaps with the horizontal requirements under the CRA.

Proposed simplification:
Recognise CRA CE-marking as sufficient for ICT products and services under NIS2 Article 24(2) to prevent duplicate certification.

[1] EUR-Lex - C(2024)7151 - EN - EUR-Lex

Responsibilities of management bodies

Status quo:

The Directive provides that the management bodies of the essential and important entities shall be held liable for non-compliance of the cybersecurity management measures taken by these entities, and that they shall follow specific training to ensure that they are able to assess and apprehend these measures and practices. While this term is still unspecific, in the context of information security, the main governance function is usually assigned to a Chief Information Security Officer (CISO) and the respective security organization. EEA believes that this aspect should be taken into account by the Member States in the national implementation.

It is overall necessary to guarantee that provisions involving personal accountability for non-compliance are proportionate to the specific risks entailed. High disproportionality would not contribute to an equal and trustworthy relationship between essential and important entities and National Competent Authorities (NCAs).

Proposed simplification:

To ensure proportionality and clarity, Member States should **define "management body"** in a uniform and narrow way, limited to individuals with executive responsibility for the company's strategic direction, risk decisions, and internal governance. Training requirements should enable board level oversight without shifting operational accountability away from security functions, i.e. the Chief Information Security Officer (CISO) and the respective security experts within the organization.

Scope

Status quo: the no exemption for services within an organization

Subsidiaries in which the central IT operations of a group of companies are organized should generally be regarded as Managed Services Providers (MSP) or Managed Security Service Providers (MSSP).

Proposed simplification

Where services that would otherwise fall under NIS2 are provided exclusively intra-group, the providing entity should be out of scope of NIS2 and of Implementing Regulation (EU) 2024/2690; the regulatory obligations should instead attach to the in-scope operating entities that consume those services, managed through their supply-chain controls and consolidated accountability. NIS2's sectoral scope (Annex I/II) and the EU-level Implementing Regulation 2024/2690 target digital infrastructure and ICT service management providers such as data center service providers, managed service providers (MSPs) and managed security service providers-a taxonomy framed around B2B market supply. Intra-group units with no external customers are qualitatively different: they are not "providers" competing on the market but internal functions of a single economic undertaking. Carving them out aligns the rule set with its market-facing orientation (while keeping the consuming entities fully regulated).

Conclusion

The EEA reiterates its strong support for a simplified, harmonized, and proportionate cybersecurity framework under NIS2 that fosters resilience while avoiding regulatory duplication. Achieving consistency in definitions, reporting obligations, and certification requirements across the EU is essential to ensuring that businesses, especially those operating cross-border, can maintain high cybersecurity standards without unnecessary administrative complexity.

The EEA believes that a single, coherent approach to implementation, supported by clear Commission guidance and coordination among Member States, will deliver greater predictability, cost-efficiency,

and security across the Single Market. Harmonization will also ensure that the objectives of the NIS2 Directive, enhancing the overall level of cybersecurity and strengthening the internal market-are effectively met in practice.

We remain available to address any open questions and stand ready to continue the dialogue with the European Commission and Member States. We are committed to supporting the development of a practical, innovation-friendly, and risk-based framework that secures Europe's digital infrastructure while enabling competitiveness and growth.

***

About the European Express Association

The European Express Association (EEA) represents the interests of the express industry in Europe. The express industry provides door-to-door transport and delivery of next-day or time-definite shipments, throughout Europe and the world. According to a 2020 Oxford Economics study on the impact of the express industry on the EU economy, the European express industry directly supported 330,000 jobs and an estimated 1.1 million indirect jobs in the EU in 2018, while generating €24 billion in tax revenues for EU Member States' governments that same year. EEA's EU Transparency Register number is 1894704851- 83.