October 2022

EEA's position on the revision of the Network and Information Security (NIS2) Directive and Implementation

Introduction

The Network and Information Security (NIS) Directive was a landmark piece of EU legislation that improved and harmonized Europe's cybersecurity preparedness at national and Union level. It is a major step in making Europe more resilient and ensuring a strong response to current and emerging cyber threats to vital sectors of the EU economy.

The EEA supports the goal of raising the level of cyber-resilience by introducing a renewed NIS 2 Directive, but it has to be done in a way that ensures coherent implementation across the Member States, especially from a point of view of companies that have cross-border or even international operations such as the members of the EEA.

Key priorities for the implementation of the NIS 2 directive

In view of the upcoming national implementation process, we would like to put forward the following recommendations:

A. Cybersecurity risk management measures based on international standards

The EEA welcomes that the cybersecurity risk management measures laid out in the NIS2 directive shall be appropriate to the risk presented and having regards to the state of the art and relevant European and international standards, as well as the cost of implementation. Such existing international standards should form the basis of any effort to lay down technical and methodological specifications for the risk management measures that companies must undertake. This helps to provide a high degree of legal certainty for the now covered important entities, by avoiding the emergence of contradicting regulatory requirements, and also supports a harmonized European wide implementation. Member States should refer to this in their implementation in order to make the new requirements practicable for the newly affected sectors.

Fragmentation amongst Member State approaches should be reduced. Therefore, the European Commission should provide guidance to support Member States in implementing the provisions on the scope and evaluating the proportionality of the measures to be taken pursuant to this Directive, in particular as regards entities in newly added sectors.

B. Incident reporting obligations

The EEA believes that the now decided timeframe for reporting is overly ambitious. In many cases, companies may not have enough information to understand how significant an incident is, nor indeed whether it was caused by an unlawful or malicious actor, within 24 hours. It is still unclear what the added value of receiving an initial report within 24 hours would be for a competent authority, when this report may not contain any valuable information due to the fact that the relevant entity did not have enough time at its disposal to determine the scope and source of the incident. The EEA support efforts from the Cooperation Group and ENISA to develop standardized incident reporting forms common notification templates in English language to reduce the administrative burden of companies operating across Europe while strengthening harmonized implementation.

C. Responsibilities of management bodies

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).

D. Supervision on important entities

The EEA agrees with the directive to allow the Member States to prioritise supervision following a risk-based approach.

Conclusion and next steps

The EEA stands ready to work with EU and national policymakers to deliver a functioning and proportionate Directive that also works for companies such as the EEA Members that have a global business model and therefore a global IT infrastructure. This shall be considered during the implementation of the directive.

Member States will have 21 months from the entry into force of the revised NIS 2 directive to transpose the new directive into national law. The new directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the EU. Until now, the publication is still pending.

***

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.