Security of network and information systems (NIS 2 Directive): simplification and alignment with the Cybersecurity Act 2

2026/0012(COD) - 14/01/2026 - Legislative proposal

PURPOSE: to simplify the implementation of measures for a high common level of cybersecurity across the EU.

PROPOSED ACT: Directive of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market. Since the entry into force of Directive (EU) 2022/2555, progress has been made in increasing the Union's level of cyber resilience. At the same time, certain challenges have arisen during the implementation by Member States including in relation to the scope of the Directive, the implementation of the cybersecurity risk-management and incident reporting obligations and the supervision of cross-border entities.

Building on the proposal for the Cybersecurity Act 2, targeted amendments should be made to Directive (EU) 2022/2555 to address those challenges, by simplifying specific aspects in order to increase legal certainty and ensure uniform implementation of Directive (EU) 2022/2555.

This proposal is part of a package of measures that aims at aligning the Union's cybersecurity framework with the needs of stakeholders in an increasingly sophisticated cyber threat landscape and complex geopolitical reality.

CONTENT: the proposed Directive amends Directive (EU) 2022/2555 (the NIS 2 Directive) in order to simplify its implementation and ensure coherence with the forthcoming revised Cybersecurity Act (Cybersecurity Act 2). It responds to concerns raised by Member States and stakeholders regarding administrative complexity, overlaps between EU cybersecurity frameworks, and the need for greater legal clarity. It will amend the existing NIS 2 Directive and further streamline the obligations imposed on businesses, therefore ensure a higher level of harmonisation across the Union.

The objective of the proposed Directive should be considered as part of the overarching goals of the Cybersecurity Act revision package involving the proposal for a Regulation by the European Parliament and the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881.

The main targeted amendments to the NIS2 directive aim to:

- **facilitate compliance with the NIS 2 directive by entities and suppliers**: entities governed by the NIS 2 directive will be able to obtain certificates within the framework of the organisational cybersecurity certification schemes developed within the framework of the ECCF (European Cybersecurity Certification Framework);

- **further facilitate compliance with cybersecurity risk management measures for multinational entities subject to the supervision of the competent authorities of several Member States**: ENISA would be given a new role of supporting Member States in the supervision of these entities, facilitating mutual assistance and creating a better overview of entities covered by the NIS 2 Directive.

Other targeted include:

- clarifications of the **scope and definitions**. Certain scope-related provisions concerning healthcare providers, electricity producers, hydrogen undertakings and entities in the chemical sector should be clarified to ensure legal certainty and reduce compliance burden for both entities and national authorities;

- removal of micro- and small-sized DNS service providers from the scope;

- introduction of **maximum harmonisation for implementing acts** (specifying cybersecurity risk-management measures) to facilitate compliance for entities and supervision for authorities;

- introduction of a **new category of small mid-caps,** entities qualifying as small mid-caps are to be designated as important entities, reducing their compliance burden and the supervision burden on competent authorities;

- the requirement for Member States to adopt policies for the **migration to postquantum cryptography** (PQC) as part of their national cybersecurity strategy; and

- introduction of a harmonised **collection of data on ransomware attacks**.

Lastly, the proposal envisages that the Commission adopts guidelines on the application of supply chain security requirements that entities in scope of the NIS 2 Directive pass on to their suppliers, in order to ensure legal certainty and prevent the undue passing on of obligations on entities not in scope of the NIS 2 Directive.