A high common level of cybersecurity

2020/0359(COD) - 27/12/2022 - Final act

PURPOSE: to strengthen cybersecurity and resilience across the EU.

LEGISLATIVE ACT: Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910 /2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

CONTENT: the Directive establishes measures that aim to achieve a **common high level of cybersecurity** across the Union with a view to further improving the resilience and incident response capabilities of both the public and private sectors and the EU as a whole. The new Directive, called 'NIS 2', will replace the current Network and Information Security Directive (NIS Directive).

Objective

The revised Directive aims to **harmonise cybersecurity requirements** and implementation of cybersecurity measures in different Member States. To achieve this, it sets out minimum rules for a regulatory framework and lays down mechanisms for effective cooperation among relevant authorities in each Member State.

The NIS2 Directive will form the basis for **cybersecurity risk management** measures and **reporting obligations** in all key sectors covered by the Directive, namely energy, transport, banking, financial market infrastructure, health, drinking water, digital infrastructure, public administrations and the space sector, as well as in important sectors such as postal services, waste management, chemicals, food, medical device manufacturing, electronics, machinery, vehicle engines and digital suppliers.

Scope

The new NIS2 Directive introduces a **size-cap rule** as a general rule for identification of regulated entities. This means that all medium and large entities operating in the sectors covered by the Directive or providing services within its scope will fall within its scope.

The Directive will apply to public administration entities at central and regional level. In addition, Member States may decide to apply it also to such entities at local level and to educational institutions, in particular where they carry out critical research activities.

The Directive will not apply to public administration entities carrying out activities in the fields of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences. Parliaments and central banks are also excluded from the scope.

The Directive lays down minimum rules for a regulatory framework and does not prevent Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity.

While the revised directive maintains this general rule, its text includes additional provisions to ensure **proportionality**, a higher level of risk management and clear-cut criticality criteria for allowing national authorities to determine further entities covered.

Coordinated cyber security frameworks

The Directive sets out obligations for Member States to adopt **national cybersecurity strategies**, designate or establish competent authorities, cyber crisis management authorities, single cyber security contact points and computer security incident response centres (CSIRTs).

Cooperation at EU level

The Directive sets out mechanisms for effective cooperation between the competent authorities of each Member State. It establishes a **Cooperation Group** to support and facilitate strategic cooperation and information exchange between Member States and to build confidence. A **network of national CSIRTs** is established to contribute to confidence building and to promote swift and effective operational cooperation between Member States.

The Directive also formally establishes the European cyber crisis liaison organisation network (EU-CyCLONe), which will support the coordinated management of large-scale cyber security incidents.

Voluntary peer learning mechanism

A voluntary peer learning mechanism will enhance mutual trust and learning from good practices and experiences in the Union, thereby contributing to a common high level of cyber security.

The Cooperation Group will establish, by 17 January 2025, with the assistance of the Commission and ENISA and, where appropriate, the CSIRT network, the methodology and organisational aspects of peer reviews with a view to learning from shared experiences, building mutual trust, achieving a common high level of cybersecurity, as well as strengthening Member States' cybersecurity capacities and policies necessary for the implementation of the Directive.

Simplification of reporting obligations

The Directive streamlines the reporting obligations to avoid over-reporting and creating an excessive burden for the entities concerned.

In order to simplify the reporting of information required under the Directive and to reduce the administrative burden on entities, Member States will provide technical means, such as a single entry point, automated systems, online forms, user-friendly interfaces, templates and dedicated platforms for the use of entities, irrespective of whether they fall within the scope of the Directive, for the submission of the relevant information to be reported.

Lastly, the Directive provides for **remedies and penalties** to ensure compliance with the legislation.

ENTRY INTO FORCE: 16.1.2023

TRANSPOSITION: no later than 17.10.2024. The provisions will apply from 18.10.2024.