A high common level of cybersecurity

2020/0359(COD) - 10/11/2022 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 577 votes to 6 with 31 abstentions a legislative resolution on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

The European Parliament's first reading position under the ordinary legislative procedure amends the proposal as follows:

Strengthening EU-wide cybersecurity and resilience

This 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 and to further improve the resilience and incident response capacities of both the public and private sector and the EU as a whole.

To that end, this Directive lays down:

- obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);

- cybersecurity risk management measures and reporting obligations for entities in ‘critical’ sectors such as 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;

- **rules and obligations** on cybersecurity information sharing;

- **supervisory and enforcement obligations** on Member States.

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 cyber security.

Scope of application

All **medium and large entities** operating in the sectors covered by the Directive or providing services falling within its scope will fall within its scope.

As **public administrations** are often the target of cyber-attacks, 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 as well as 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 field 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 includes additional provisions to ensure **proportionality**, a higher level of risk management and clear criteria on the **criticality of entities** to determine which ones are covered.

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

Peer reviews should be introduced to help learn from shared experiences, **build mutual trust** and achieve a common high level of cyber security. The Cooperation Group should establish, no later than 2 years after the date of entry into force of the Directive, with the assistance of the Commission and ENISA and, where appropriate, the CSIRT network, the methodology and organisational aspects of peer reviews. Participation in peer reviews should be voluntary.

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 should 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.