Measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

2023/0109(COD) - 15/01/2025 - Final act

PURPOSE: to strengthen EU's solidarity and capacities to detect, prepare for and respond to cybersecurity threats and incidents.

LEGISLATIVE ACT: Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act).

CONTENT: this regulation is part of the Cybersecurity legislative package which also includes a targeted amendment to the Cybersecurity Regulation.

The regulation down measures to strengthen capacities in the Union to detect, prepare for and respond to cyber threats and incidents. It pursues the general objectives of reinforcing the competitive position of industry and services in the Union across the digital economy, including microenterprises and small and medium-sized enterprises as well as start-ups, and of contributing to the **Union's technological sovereignty** and open strategic autonomy in the area of cybersecurity, including by boosting innovation in the Digital Single Market.

The regulation establishes:

(1) Cybersecurity Alert System

A cyber security alert system is established to support the development of advanced capabilities for the Union to enhance detection, analysis and data processing capabilities in relation to cyber threats and the prevention of incidents in the Union. It is a **pan-European network of infrastructures** composed of national cyber hubs and cross-border cyber hubs adhering to it on a voluntary basis. These entities will be responsible for sharing information and detecting and responding to cyber threats. The cyber hubs will use state-of-the-art technology, such as artificial intelligence (AI) and advanced data analytics, to detect and share timely warnings on cyber threats and incidents across borders. They will strengthen the existing European framework and, in turn, authorities and relevant entities will be able to respond more efficiently and effectively to cybersecurity incidents.

(2) Cybersecurity Emergency Mechanism

This emergency mechanism is established to support the improvement of the Union's resilience to cyber threats and the preparation for and mitigation of, in a spirit of solidarity, the short-term impact of significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents.

The cybersecurity emergency mechanism will support the following:

- **preparedness actions**, including testing entities in highly critical sectors (healthcare, transport, energy, etc.) for potential vulnerabilities, based on common risk scenarios and methodologies;

- a new **EU Cybersecurity Reserve** composed of incident response services provided by the private sector and ready to intervene, at the request of a Member State or EU institutions, bodies and agencies and associated third countries, in the event of a significant or large-scale cybersecurity incident. To benefit from support from the EU Cybersecurity Reserve, users must take all appropriate measures to mitigate the effects of the incident for which they are requesting support. Requests for support must be reviewed by the contracting authority. A response must be provided to users without delay and in any case no later than 48 hours after the submission of the request to ensure the effectiveness of the support;

- a **new EU cybersecurity reserve** consisting of incident response services from the private sector ready to intervene at the request of a member state or EU institutions, bodies, and agencies, as well as associated third countries, in case of a significant or large-scale cybersecurity incident;

- technical **mutual assistance**.

(3) A cybersecurity incident review mechanism

In order to support the objectives of promoting shared situational awareness and enabling effective response to significant cybersecurity incidents and large-scale cybersecurity incidents, the Commission or the European cyber crisis liaison organisation network (EU-CyCLONe) will be able to request ENISA, with the support of the CSIRTs network and with the approval of the Member States concerned, to review and assess cyber threats, known exploitable vulnerabilities and mitigation actions with respect to a specific significant cybersecurity incident or large-scale cybersecurity incident.

Following the completion of a review and assessment of an incident, ENISA will prepare an **incident review report**, in collaboration with the Member State concerned, relevant stakeholders, including representatives from the private sector, the Commission and other relevant Union institutions, bodies, offices and agencies. Building on the collaboration with stakeholders, including from the private sector, the review report on specific incidents should aim to assess the causes, impact and mitigation of an incident, after it has occurred.

ENTRY INTO FORCE: 4.2.2025.