High common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

2022/0085(COD) - 21/11/2023 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 557 votes to 0, with 27 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

The European Parliament adopted its position at first reading under the ordinary legislative procedure.

Subject matter

This Regulation lays down measures that aim to **achieve a high common level of cybersecurity** within Union entities with regard to:

- the establishment by each Union entity of an internal cybersecurity risk-management, governance and control framework;

- cybersecurity risk management, reporting and information sharing;

- the organisation, functioning and operation of the Interinstitutional Cybersecurity Board as well as the organisation, functioning and operation of the Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU);

- the monitoring of the implementation of this Regulation.

Cybersecurity risk-management, governance and control framework

Each Union entity should, after carrying out an initial cybersecurity review, such as an audit, establish an internal cybersecurity risk-management, governance and control framework. The establishment of the Framework should be **overseen by and under the responsibility of the Union entity's highest level of management**. The Framework should be based on an all-hazards approach. It should ensure a high level of cybersecurity and be reviewed on a regular basis, in light of the changing cybersecurity risks, and at least every four years.

Each Union entity should appoint a **local cybersecurity officer** or an equivalent function who should act as its single point of contact regarding all aspects of cybersecurity. The local cybersecurity officer should facilitate the implementation of this Regulation and report directly to the highest level of management on a regular basis on the state of the implementation.

Cybersecurity risk-management measures

Without undue delay and in any event by 20 months from the date of entry into force of this Regulation, each Union entity should, under the oversight of its highest level of management, take appropriate and proportionate technical, operational and organisational measures to manage the cybersecurity risks identified under the Framework, and to prevent or minimise the impact of incidents. Those measures should ensure a level of security of network and information systems across the entirety of the ICT

environment commensurate to the cybersecurity risks posed. When assessing the proportionality of those measures, due account should be taken of the degree of the Union entity's exposure to cybersecurity risks, its size and the likelihood of occurrence of incidents and their severity, including their societal, economic and interinstitutional impact.

Cybersecurity plans

Following the conclusion of the cybersecurity maturity assessment carried out pursuant to the Regulation and taking into account the assets and cybersecurity risks identified in the Framework, as well as the cybersecurity risk-management measures, the highest level of management of each Union entity should approve a cybersecurity plan without undue delay and in any event by 24 months from the date of entry into force of this Regulation.

Interinstitutional Cyber Security Board

The Regulation establishes the Interinstitutional Cyber Security Board (IICB), with a view to facilitating the establishment of a common high level of cyber security among EU entities. The IICB will play an exclusive role in monitoring and supporting the implementation of the Regulation by EU entities, overseeing the implementation of the overall priorities and objectives of the EU-CERT and providing strategic direction to the EU-CERT.

In order to support Union entities, the IICB should provide guidance to the Head of CERT-EU, adopt a multiannual strategy on raising the level of cybersecurity in the Union entities, establish the methodology for and other aspects of voluntary peer reviews, and facilitate the establishment of an informal group of local cybersecurity officers, supported by the European Union Agency for Cybersecurity (ENISA), with the aim of exchanging best practices and information in relation to the implementation of this Regulation.

CERT-EU should **collect, manage, analyse and share information** with the Union entities on cyber threats, vulnerabilities and incidents in unclassified ICT infrastructure. It should coordinate responses to incidents at interinstitutional and Union entity level, including by providing or coordinating the provision of specialised operational assistance.

Reporting obligations

This Regulation lays down a multiple-stage approach to the reporting of significant incidents. All EU entities will have to **inform CERT-EU of any incident** with a significant impact. An incident should be considered to be significant if: (a) it has caused or is capable of causing severe operational disruption to the functioning of, or financial loss to, the Union entity concerned; (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Union entities should submit to CERT-EU:

- without undue delay and in any event within **24 hours** of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate that the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-entity or a cross-border impact;

- without undue delay and in any event within **72 hours** of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

- a final report **not later than one month** after the submission of the incident notification, including the following: (i) a detailed description of the incident, including its severity and impact; (ii) the type of threat

or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures; (iv) where applicable, the cross-border or cross-entity impact of the incident.

A Union entity should, without undue delay and in any event **within 24 hours** of becoming aware of a significant incident, inform any relevant Member State counterparts in the Member State where it is located that a significant incident has occurred.

The amended text specifies that the processing, by CERT-EU, the Interinstitutional Cyber Security Council and Union entities, of personal data under the Regulation must be carried out in accordance with Regulation (EU) 2018/1725 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.