European Commission - Press release

New rules to boost cybersecurity of the EU institutions enter into force

Brussels, 8 January 2024

The new Cybersecurity Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union entered into force yesterday, 7 January 2024.

The Regulation lays down measures for the establishment of an internal cybersecurity risk management, governance and control framework for each Union entity, and sets up a new Interinstitutional Cybersecurity Board (IICB) to monitor and support its implementation by Union entities. It provides an extended mandate of the Computer Emergency Response Team for the EU institutions, bodies, offices and agencies (CERT-EU), as a threat intelligence, information exchange and incident response coordination hub, a central advisory body, and a service provider. In line with its mandate, CERT-EU is renamed to Cybersecurity Service for the Union institutions, bodies, offices and agencies, but it retains the short name "CERT-EU".

Next Steps

Following the timeline defined in the Regulation, the Union entities will establish internal cybersecurity governance processes and will progressively put in place specific cybersecurity risk management measures foreseen by the Regulation. The IICB will be set up and will become operational as soon as possible, with the objective to ensure the strategic steering to CERT-EU under its extended mandate, provide guidance and support to the Union entities and monitor the implementation of the Regulation.

Background

In its resolution from March 2021, the Council of the European Union stressed the importance of a robust and consistent security framework to protect all EU personnel, data, communication networks, information systems and decision-making processes. In this context, the Commission announced the proposal for the Cybersecurity Regulation in March 2022, and in June 2023 the European Parliament and Council reached a political agreement.

This Regulation aligns with the Commission's policy objectives as set by the EU Security Union Strategy and the EU Cybersecurity Strategy, and ensures consistency with other legislative initiatives in the area:

- The Directive on measures for a high common level of cybersecurity across the Union ('NIS 2'), with which this legislation is aligned in terms of principles and level of ambition, while respecting the specificities of Union entities;
- The Cybersecurity Act;
- The Commission Recommendation on coordinated response to large-scale cybersecurity incidents and crises.

The Cybersecurity Regulation was presented jointly with a proposal for an Information Security Regulation, setting minimum **information security rules** and standards for all EU institutions, bodies, offices and agencies. This proposal aims at a **secure exchange of information** across EU institutions, bodies, offices and agencies and with the Member States, based on standardised practices and measures to protect information flows. Negotiations between the co-legislators on this proposal have not yet started.

IP/23/6782

Quotes:

"As the cyber threats are becoming more pervasive and the cyber attackers more sophisticated, achieving a high common level of cybersecurity across Union entities is paramount to ensure an open, efficient, secure and resilient EU public administration. The Regulation strengthens Union entities' cybersecurity and aligns the EU administration with the standards imposed on Member States, such as the Directive on high common levels of cybersecurity across the Union, also known as NIS 2. The rapid adoption of the Regulation proves the commitment of the EU towards these objectives. Now I call upon the co-legislators to swiftly engage on negotiations for the parallel Information Security Regulation."
Johannes Hahn, Commissioner for Budget and Administration - 08/01/2024

Press contacts:

Johannes BAHRKE (+32 2 295 86 15)
Roberta VERBANAC (+32 2 298 24 98)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email