Information security in the institutions, bodies, offices and agencies of the Union

2022/0084(COD) - 22/03/2022 - Legislative proposal

PURPOSE: to establish rules with a view to achieving a common high level of security for EU classified information and for non-classified information handled and stored by the EU institutions and bodies.

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: given the ever-increasing volumes of non-classified sensitive information and EU classified information (EUCI) that the EU institutions and bodies have to share, and due to the dramatically evolving threats, the **EU administration is exposed to attacks** in all its areas of activity. The information handled by the EU institutions and bodies is of great interest to malicious actors and needs to be properly protected, which requires swift action to improve its protection.

Currently, the EU institutions and bodies either have their own rules on information security, based on their Rules of Procedure or their founding acts, or they have no rules at all. **The lack of a common approach** hinders the deployment of common tools building on an agreed set of rules depending on the security needs of the information to be protected.

Therefore, and in order to increase the protection of the information handled by the European administration, this initiative aims to **streamline the different legal frameworks of the Union institutions and bodies** in the field by:

- establishing harmonised and comprehensive categories of information, as well as common handling rules for all Union institutions and bodies,

- setting up a lean cooperation scheme on information security between Union institutions and bodies able to foster a coherent information security culture across the European administration,

- modernising the information security policies at all levels of classification/categorisation, for all Union institutions and bodies, taking into account the digital transformation and the development of teleworking as a structural practice.

This initiative is part of the EU strategy for the Security Union adopted by the Commission on 24 July 2020 and is part of a broad set of EU policies in the field of security and information security.

CONTENT: the proposed Regulation is intended to **create a minimum set of rules on information security** applicable to all EU institutions and bodies. It applies to all information handled and stored by the Union institutions and bodies, including information related to the European Atomic Energy Community activities, other than Euratom classified information. The Regulation covers both non-classified information and EUCI.

Security governance and organisation

The proposal foresees the creation of an **inter-institutional information security coordination group** in which the security authorities of all EU institutions and bodies would be represented. The coordination group would have the task of **defining the common policy** of these institutions and bodies in the field of information security. It should enhance the coherence of policies in the field of information security and contribute to the harmonisation of information security procedures and tools across the Union institutions and bodies.

The coordination group should draft guidance documents and create platforms for sharing best practices and knowledge on common issues relevant to information security and for providing assistance in case of information security incidents. It would regularly exchange with the national security authorities of the Member States, gathered in an **Information Security Committee**.

Five sub-groups of experts representing different institutions and bodies would be set up to streamline procedures and other practical aspects of information security.

Each EU institution or body would be required to designate a **security authority**, responsible for the definition and implementation of internal information security policies.

Information assurance and communication and information systems

The proposed Regulation establishes a **sub-group** on information assurance with the objective of enhancing the coherence across the Union institutions and bodies between the information security rules and the cybersecurity baseline as defined by the Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

Non-classified information

The Regulation provides for **three categories** of non-classified information: (1) information for public use, (2) normal information and (3) sensitive non-classified information. All categories are defined, while markings and handling conditions are stipulated for protecting such information.

With a view to coordinating the work on equivalence between particular categories established by some Union institutions and bodies and common categories provided by the Regulation, the proposal sets up a sub-group on non-classified information.

Classified information (EUCI)

The section on general provisions provides for **four levels of EUCI**: (1) TRES SECRET UE/EU TOP SECRET, (2) SECRET UE/EU SECRET, (3) CONFIDENTIEL UE/EU CONFIDENTIAL, (4) RESTREINT UE/EU RESTRICTED. It also provides for an obligation of Union institutions and bodies to take the necessary security measures in accordance with the results of an information security risk management process.

The proposal also covers aspects of personnel security, physical security, EUCI management, protection in information and communication systems, industrial security, EUCI sharing and exchange of classified information.

The proposed regulation establishes sub-groups on information assurance, on non-classified information, on physical security, on accreditation of communication and information systems handling and storing EUCI and on EUCI sharing and exchange of classified information.