EUROPEAN
COMMISSION

Brussels, 22.3.2022
SWD(2022) 65 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ANALYSIS REPORT

Accompanying the document

Proposal for a Regulation of the European Parliament and of the Council

on information security in the institutions, bodies, offices and agencies of the Union

{COM(2022) 119 final} - {SWD(2022) 66 final}

Executive Summary Sheet

Impact analysis on information security in the institutions, bodies, offices and agencies of the Union

A. Political context

The European Council's Strategic Agenda for 2019-2024 calls on the Institutions to protect the EU's information and communication networks and its decision-making processes from malicious activities of all kinds, including cyber and hybrid threats. Consequently, the General Affairs Council in December 2019 concluded that EU institutions and bodies should develop and implement a comprehensive set of measures to ensure their information security.

In July 2020, the Commission adopted its EU Security Union Strategy, by which it committed to complement the national efforts in the area of security. As part of this strategy, the Commission proposed to create a minimum set of rules on information security and cybersecurity across all Union institutions and bodies (UIBs).

B. What is the problem?

The main problems are: i) significant difference between the level of security of UIBs depending on their internal information security rules and ii) lack of coordination between the Union institutions and bodies in performing their security tasks.

Union institutions and bodies currently have their own information security rules or have not adopted such rules at all. The fragmentation of the applicable legal framework led to different categories of non-classified information, different markings and handling instructions across the board. For what concerns the EU classified information, the interoperability of the relevant systems remains limited, preventing a seamless transfer of information between institutions and bodies and with the Member States.

This situation increases the risks of attackers creating a security breach in the weakest link and use that as a starting point for further attacks on other institutions or bodies.

C. What should be achieved?

The general objective of the initiative is to create information security rules for all Union institutions and bodies with the aim to ensuring an enhanced and consistent protection against the evolving threats to their information.

The general objective is translated into four specific objectives:

- Establish harmonised and comprehensive categories of information
- Identify security gaps and implement measures required
- Establish a lean cooperation on information security between the Union institutions and bodies
- Modernise the information security policies, taking account of digital transformation and teleworking

D. What are different stakeholders' views?

The stakeholders consulted (Union institutions and bodies, Member States National Security Authorities

and research experts from JRC) agreed on the need of Information security common standards to all Union institutions and bodies, with a focus on the following points:

- The diversity and the different business environment of each UIB should be taken into account and local solution should be allowed;
- While the majority of institutions and bodies are ready to cooperate with their counterparts in common bodies for information security purposes, they are not willing to delegate their decision making powers;
- The draft Regulation should be drafted in respect of the Intergovernmental agreement[1] of the Member States on the protection of classified information.

E. What is the impact of the proposal?

Benefits

By creating a baseline of information security rules across Union institutions and bodies, the draft Regulation will increase the overall levels of information security while reducing the current discrepancies. It should also help to eliminate potential weak links while protecting the information shared within the European administration.

From an efficiency point of view, the draft Regulation should lead to gains from the coordinated performance of common information security tasks (e.g. clearances, accreditation of Communication and Information Systems) and the creation of common governance bodies (e.g. the Inter-institutional Coordination Group, the technical sub-groups).

Economic impact

For the Union institutions and bodies, the efforts required to implement the new legislation are expected to be compensated by the gains in efficiency while additional costs can be covered under the existing information security improvement programmes of each organisation. In the long term, they will gain from the coherent approach in addressing the ever evolving threats to information security.

The European Commission should ensure the permanent Secretariat of the Inter-institutional Coordination Group and allocate human resources for this task (one AD official and one AST official).

No economic impacts are expected at the level of Member States administrations and private sector.

F. Follow up

When will the policy be reviewed?

A full evaluation will be conducted every 5 years after the date of application in order to assess impacts and implementation of the draft Regulation. Commission shall present a report with its findings and submit it to the European Parliament and the Council.

[1] Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union, 2011/C202/05