Procedure file

Basic information

COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	2022/0085(COD)
High common level of cybersecurity at the institutions, bodies, offices and agencies of the Union	Procedure completed

Subject
2.80 Cooperation between administrations
3.30.06 Information and communication technologies, digital technologies
3.30.07 Cybersecurity, cyberspace policy
3.30.25 International information networks and society, internet
8.40 Institutions of the Union
8.40.08 Agencies and bodies of the EU

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
ITRE Industry, Research and Energy		18/05/2022
	VIRKKUNEN Henna	
	Shadow rapporteur	
	KUMPULA-NATRI Miapetra	
	BILBAO BARANDICA Izaskun	
	PEKSA Mikuláš	
	BUCHHEIT Markus	
	TOŠENOVSKÝ Evžen	
	BOTENGA Marc	

Committee for opinion	Rapporteur for opinion	Appointed
BUDG Budgets		22/04/2022
	UŠAKOVS Nils	
LIBE Civil Liberties, Justice and Home Affairs (Associated committee)		12/12/2022
	TOBÉ Tomas	
AFCO Constitutional Affairs		20/06/2022
	GREGOROVÁ Markéta	

Council of the European Union European Commission	Commission DG Informatics	Commissioner HAHN Johannes

Key events

22/03/2022	Legislative proposal published	COM(2022)0122	Summary
04/04/2022	Committee referral announced in Parliament, 1st reading		
15/09/2022	Referral to associated committees announced in Parliament		
09/03/2023	Vote in committee, 1st reading		
09/03/2023	Committee decision to open interinstitutional negotiations with report adopted in committee		
10/03/2023	Committee report tabled for plenary, 1st reading	A9-0064/2023	Summary
13/03/2023	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 71)		
15/03/2023	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 71)		
19/09/2023	Approval in committee of the text agreed at 1st reading interinstitutional negotiations	PE753.446 GEDA/A/(2023)005465	
21/11/2023	Results of vote in Parliament		
21/11/2023	Decision by Parliament, 1st reading	T9-0398/2023	Summary
08/12/2023	Act adopted by Council after Parliament's 1st reading		
13/12/2023	Final act signed		
18/12/2023	Final act published in Official Journal		

Technical information

Procedure reference	2022/0085(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
Legal basis	Treaty on the Functioning of the EU TFEU 298-p2; Rules of Procedure EP 57; Euratom Treaty A 106a-pa
Other legal basis	Rules of Procedure EP 159
Stage reached in procedure	Procedure completed
Committee dossier	ITRE/9/08708

Documentation gateway

Legislative proposal		COM(2022)0122	22/03/2022	EC	Summary
Document attached to the procedure		SWD(2022)0067	22/03/2022	EC	
Document attached to the procedure		SWD(2022)0068	22/03/2022	EC	
Document attached to the procedure		N9-0039/2022 OJ C 258 05.07.2022, p. 0010	17/05/2022	EDPS	
Committee opinion	BUDG	PE732.682	13/07/2022	EP	
Committee draft report		PE737.231	07/10/2022	EP	
Amendments tabled in committee		PE738.403	27/10/2022	EP	
Committee opinion	AFCO	PE730.184	01/02/2023	EP	
Committee opinion	LIBE	PE739.801	01/03/2023	EP	
Committee report tabled for plenary, 1st reading/single reading		A9-0064/2023	10/03/2023	EP	Summary
Coreper letter confirming interinstitutional agreement		GEDA/A/(2023)005465	15/09/2023	CSL	
Text agreed during interinstitutional negotiations		PE753.446	15/09/2023	EP	
Text adopted by Parliament, 1st reading/single reading		T9-0398/2023	21/11/2023	EP	Summary
Draft final act		00057/2023/LEX	13/12/2023	CSL	
Commission response to text adopted in plenary		SP(2024)109	23/02/2024	EC	

Additional information

Research document	Briefing	02/09/2022

Final act

Regulation 2023/2841
OJ L 000 18.12.2023, p. 0000

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

PURPOSE: to establish measures to ensure a high common level of cybersecurity in the Union institutions, bodies and agencies.

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: evolving technology and increased complexity and interconnectedness of digital systems amplify cybersecurity risks making the Union administration more vulnerable to cyber threats and incidents.

From 2019 to 2021, the number of significant incidents affecting Union institutions, bodies and agencies, authored by advanced persistent threat actors, has surged dramatically. The first half of 2021 saw the equivalent in significant incidents as in the whole of 2020.

The Centre for Cybersecurity of the EU Institutions, Bodies and Agencies (CERT-EU) has assessed the main cyber threats to which the EU institutions, bodies and agencies are currently exposed or are likely to be exposed in the foreseeable future. The analysis examined the influence of major ongoing shifts affecting the ways in which the EU institutions manage and use their IT infrastructures and services. These shifts include the increase in teleworking, the migration of systems to the cloud and the increased outsourcing of IT services.

The analysis of the 20 Union institutions, bodies and agencies shows that their governance, cyber-hygiene, overall capability and maturity vary over a broad spectrum. Therefore, requiring all Union institutions, bodies and agencies to implement a baseline of cybersecurity measures is

instrumental to address this disparity in maturity and to bring all Union institutions, bodies and agencies to a high common level of cybersecurity.

This proposal builds on the EU Strategy for the Security Union and the EUs Cybersecurity Strategy for the Digital Decade.

CONTENT: this proposal establishes a framework to ensure common rules and measures on cybersecurity within the Union institutions, bodies, offices and agencies to enable them to perform their respective tasks in an open, efficient and independent manner. It aims to improve all entities resilience and incident response capacities.

The proposed Regulation:

- obliges the Union institutions, bodies, offices and agencies to (i) establish an internal framework for the management, governance and control of cybersecurity risks, ensuring effective and prudent management of all such risks, (ii) adopt a cybersecurity baseline to address the risks identified through this framework, (iii) carry out a cybersecurity maturity assessment covering all elements of its IT environment at least every three years, and (iv) adopt a cyber security plan;

- establishes an inter-institutional cybersecurity board to monitor the implementation of this Regulation by the Union institutions, bodies, offices and agencies, as well to supervise the implementation of general priorities and objectives by CERT-EU and providing strategic direction to CERT-EU;

- defines the task and missions of CERT-EU as an autonomous inter-institutional cybersecurity centre at the service of all EU institutions, bodies, offices and agencies. CERT-EU will contribute to the security of the unclassified IT environment of all Union institutions, bodies and agencies by advising them on cybersecurity, by helping them to prevent, detect, mitigate and respond to incidents and by acting as their cybersecurity information exchange and incident response coordination hub;

- ensures cooperation and the exchange of information among CERT-EU, and the Union institutions, bodies and agencies to develop trust and confidence. To this end CERT-EU may request Union institutions, bodies and agencies to provide it with relevant information and CERT-EU may exchange incident-specific information with Union institutions, bodies and agencies to facilitate detection of similar cyber threats or incidents without the consent of the affected constituent. CERT-EU may only exchange incident-specific information which reveals the identity of the target of the cybersecurity incident with the consent of the affected constituent;

- obliges all EU institutions, bodies, offices and agencies to notify CERT-EU of significant cyber threats, significant vulnerabilities and significant incidents without undue delay and in any event no later than 24 hours after becoming aware of them.

Budgetary implications

According to studies, direct cybersecurity spending has tended to vary between 4 and 7% of the aggregated IT expenditures of organisations. However, the threat analysis undertaken by CERT-EU in support of this legislative proposal indicates that international bodies and political organisations face increased risks and therefore a level of 10% of IT spending on cybersecurity would seem a more adequate target.

The exact cost of such efforts cannot be determined due to the lack of detailed information on IT expenditure of the Union institutions, bodies and agencies and the relevant share of cybersecurity spending.

CERT-EU will require additional resources to fulfil its expanded role and these resources should be reallocated from the Union institutions, bodies and agencies benefitting from CERT-EUs services.

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

The Committee on Industry, Research and Energy adopted the report by Henna VIRKUNEN (EPP, FI) 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 committee responsible recommended that the European Parliament's position adopted at first reading under the ordinary legislative procedure should amend the proposal as follows:

Subject-matter

This Regulation lays down measures that aim to achieve a high common level of cybersecurity in Union entities. To that end, this Regulation lays down:

- obligations that require Union entities to establish a cybersecurity risk management, handling of incidents, governance and control framework;

- cybersecurity risk management and reporting obligations for Union entities;

- rules underpinning information sharing obligations and the facilitation of voluntary information sharing arrangements with regard to Union entities;

- rules on the organisation, tasks and operation of the Cybersecurity Centre for the Union entities (CERT-EU) and on the functioning, organisation and operation of the Interinstitutional Cybersecurity Board (IICB).

Risk management, handling of incidents, governance and control framework

On the basis of a full cybersecurity audit, each Union entity should establish its own cybersecurity risk management, handling of incidents, governance and control framework. The establishment of the framework should be overseen by the Union entitys highest level of management .

The risk management framework should (i) define the strategic objectives to ensure a high level of cybersecurity in the Union entities; (ii) lay down cybersecurity policies for the security of network and information systems encompassing the entirety of the ICT environment, and define the roles and responsibilities of staff of the Union entities tasked with ensuring the effective implementation of this Regulation; (iii) include the key performance indicators (KPIs).

The framework should be reviewed regularly and at least every three years.

Cybersecurity risk management measures

Risk management measures should ensure a level of security for networks and information systems across the ICT environment that is appropriate to the risks identified in the risk management framework, taking into account the state of the art and, where appropriate, applicable European and international standards or available European cybersecurity certificates.

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

The Interinstitutional Cybersecurity Board

The IICB aims to support entities in elevating their respective cybersecurity postures by implementing this Regulation. In order to support Union entities, the IICB should: (i) adopt guidance and recommendations required for Union entities cybersecurity maturity assessments and cybersecurity plans, (ii) review possible interconnections between Union entities ICT environments and (iii) support the establishment of a Cybersecurity Officers Group under ENISA, comprising the Local Cybersecurity Officers of all Union entities with an aim to facilitate the sharing of best practices and experiences gained from the implementation of this Regulation.

Where the IICB finds that a Union entity has not effectively applied or implemented this Regulation, it could, without prejudice to the internal procedures of the Union entity concerned: (i) request relevant and available documentation relating to the effective implementation of the provisions of this Regulation, (ii) communicate a reasoned opinion with observed gaps in the implementation of this Regulation, (iii) invite the Union entity concerned to provide a self-assessment on its reasoned opinion and (iv) issue, in cooperation with CERT-EU, guidance to bring its respective risk management, governance and control framework, cybersecurity risk-management measures, cybersecurity plans and reporting obligations.

CERT-EU mission and tasks

The mission of CERT-EU, the autonomous interinstitutional Cybersecurity Centre for all Union entities, should be to contribute to the security of the unclassified environment of all Union entities and providing for them services that are analogous to CSIRTs established by the Member Sates, in particular by advising them on cybersecurity, by helping them to prevent, detect, handle, mitigate, respond to and recover from incidents. CERT-EU is an autonomous interinstitutional service provider for all Union entities, integrated into the administrative structure of a Commission Directorate-General in order to benefit from the Commission's administrative, financial, management and accounting support structures.

Reporting obligations

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

The Union entities should notify, inter alia, any information enabling the CERT-EU to determine any cross-entities impact, impact on the hosting Member State or cross border impact following a significant incident. All 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, should indicate whether 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 report.

CERT-EU should coordinate among the Union entities the handling of major incidents.

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

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 entitys 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 entitys 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.

Transparency

VIRKKUNEN Henna	Rapporteur	ITRE	25/01/2023	European Central Bank
GREGOROVÁ Markéta	Rapporteur	AFCO	07/12/2022	Representatives of Nemec+Chvatal representatives of S.ICZ
VIRKKUNEN Henna	Rapporteur	ITRE	29/09/2022	Finnish Transport and Communications Agency Traficom Finnish Ministry of Transport and Communications
VIRKKUNEN Henna	Rapporteur	ITRE	22/09/2022	European Central Bank

VIRKKUNEN Henna	Rapporteur	ITRE	12/09/2022	ECSO Policy Task Force
VIRKKUNEN Henna	Rapporteur	ITRE	07/09/2022	Finnish Ministry of Transport and Communications