Basic information

2023/0109(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	Procedure completed
Measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents **Subject** 3.30.06 Information and communication technologies, digital technologies 3.30.07 Cybersecurity, cyberspace policy 3.30.25 International information networks and society, internet	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
ITRE Industry, Research and Energy	GÁLVEZ Lina (S&D)	02/05/2023
	Shadow rapporteur NIEBLER Angelika (EPP) GROOTHUIS Bart (Renew) NIINISTÖ Ville (Greens/EFA) TOŠENOVSKÝ Evžen (ECR)	

Committee for opinion	Rapporteur for opinion	Appointed
AFET Foreign Affairs	TUDORACHE Dragoş (Renew)	16/06/2023
BUDG Budgets	The committee decided not to give an opinion.	
CONT Budgetary Control	The committee decided not to give an opinion.	
IMCO Internal Market and Consumer Protection	The committee decided not to give an opinion.	
TRAN Transport and Tourism	FALCĂ Gheorghe (EPP)	07/07/2023
LIBE Civil Liberties, Justice and Home Affairs	The committee decided not to give an opinion.	

Council of the European Union	

Council configuration	Meetings	Date
Employment, Social Policy, Health and Consumer Affairs	4064	2024-12-02

European Commission	

Commission DG	Commissioner
Communications Networks, Content and Technology	BRETON Thierry

European Economic and Social Committee

Key events

Date	Event	Reference	Summary
18/04/2023	Legislative proposal published	COM(2023)0209	Summary
01/06/2023	Committee referral announced in Parliament, 1st reading		
07/12/2023	Vote in committee, 1st reading		
07/12/2023	Committee decision to open interinstitutional negotiations with report adopted in committee		
08/12/2023	Committee report tabled for plenary, 1st reading	A9-0426/2023	Summary
11/12/2023	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 71)		
13/12/2023	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 71)		
20/03/2024	Approval in committee of the text agreed at 1st reading interinstitutional negotiations	GEDA/A/(2024)001689 PE760.882	
24/04/2024	Decision by Parliament, 1st reading	T9-0355/2024	Summary
24/04/2024	Results of vote in Parliament		
02/12/2024	Act adopted by Council after Parliament's 1st reading		
19/12/2024	Final act signed		
15/01/2025	Final act published in Official Journal		

Technical information

Procedure reference	2023/0109(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 322-p1 Treaty on the Functioning of the EU TFEU 173-p3
Mandatory consultation of other institutions	European Economic and Social Committee

Stage reached in procedure	Procedure completed
Committee dossier	ITRE/9/11824

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE752.795	04/09/2023	
Amendments tabled in committee		PE753.628	22/09/2023	
Committee opinion	TRAN	PE752.607	25/10/2023	
Committee opinion	AFET	PE750.145	27/10/2023	
Committee report tabled for plenary, 1st reading/single reading		A9-0426/2023	08/12/2023	Summary
Text agreed during interinstitutional negotiations		PE760.882	20/03/2024	
Text adopted by Parliament, 1st reading/single reading		T9-0355/2024	24/04/2024	Summary

Council of the EU

Document type	Reference	Date	Summary
Coreper letter confirming interinstitutional agreement	GEDA/A/(2024)001689	21/03/2024	
Draft final act	00094/2024/LEX	19/12/2024	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2023)0209	18/04/2023	Summary
Commission response to text adopted in plenary	SP(2024)394	08/08/2024	

National parliaments

Document type	Parliament /Chamber	Reference	Date	Summary
Contribution	CZ_CHAMBER	COM(2023)0209	29/06/2023	
Contribution	CZ_SENATE	COM(2023)0209	01/08/2023	
Contribution	PT_PARLIAMENT	COM(2023)0209	18/09/2023	
Contribution	FR_SENATE	COM(2023)0209	04/01/2024	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary
	Economic and Social Committee:			

EESC	opinion, report	CES2408/2023	13/07/2023	
CofA	Court of Auditors: opinion, report	52023AA0002 OJ OJ C 31.01.2025	26/09/2023	
CofR	Committee of the Regions: opinion	CDR2191/2023	29/11/2023	

Additional information		
Source	**Document**	**Date**
EP Research Service	Briefing	27/11/2023

Meetings with interest representatives published in line with the Rules of Procedure

Rapporteurs, Shadow Rapporteurs and Committee Chairs

Transparency				
Name	**Role**	**Committee**	**Date**	**Interest representatives**
GÁLVEZ Lina	Rapporteur	ITRE	18/07/2024	ISACA
GÁLVEZ Lina	Rapporteur	ITRE	28/02/2024	The Kangaroo Group
GÁLVEZ Lina	Rapporteur	ITRE	16/01/2024	Deputy Permanent Representatives of Czechia and Slovakia to the EU
GROOTHUIS Bart	Shadow rapporteur	ITRE	16/11/2023	CrowdStrike
GÁLVEZ Lina	Shadow rapporteur	ITRE	15/11/2023	CrowdStrike
ALAMETSÄ Alviina	Shadow rapporteur for opinion	TRAN	19/09/2023	Permanent Representaiton of the Netherlands to the EU
NIINISTÖ Ville	Shadow rapporteur	ITRE	19/09/2023	Security Scorecard
GROOTHUIS Bart	Shadow rapporteur	ITRE	14/09/2023	ESET, spol. s r.o.
GROOTHUIS Bart	Shadow rapporteur	ITRE	13/09/2023	VNO-NCW
GROOTHUIS Bart	Shadow rapporteur	ITRE	13/09/2023	FOX IT
NIINISTÖ Ville	Shadow rapporteur	ITRE	05/09/2023	Electronic Frontier Finland
NIINISTÖ Ville	Shadow rapporteur	ITRE	08/08/2023	Okta
GÁLVEZ Lina	Rapporteur	ITRE	18/07/2023	ENISA
GÁLVEZ Lina	Rapporteur	ITRE	18/07/2023	Romanian National Cyber Security Directorate
GÁLVEZ Lina	Rapporteur	ITRE	18/07/2023	Microsoft Corporation
GÁLVEZ Lina	Rapporteur	ITRE	18/07/2023	CyberPeace institute
GÁLVEZ Lina	Rapporteur	ITRE	12/07/2023	Centro Criptológico Nacional
GÁLVEZ Lina	Rapporteur	ITRE	11/07/2023	Embajador Representante Adjunto REPER

GÁLVEZ Lina	Rapporteur	ITRE	27/06/2023	Trellix
GROOTHUIS Bart	Shadow rapporteur	ITRE	08/06/2023	Netherlands Organisation for Applied Scientific Research TNO
GROOTHUIS Bart	Shadow rapporteur	ITRE	07/06/2023	Okta
GÁLVEZ Lina	Rapporteur	ITRE	06/06/2023	Committee of the regions rapporteur
GÁLVEZ Lina	Rapporteur	ITRE	06/06/2023	Palo Alto Networks Inc.

Final act

Corrigendum to final act 32025R0038R(01)
OJ OJ L 24.01.2025

Regulation 2025/0038
OJ OJ L 15.01.2025 Summary

Corrigendum to final act 32025R0038R(03)
OJ OJ L 06.11.2025

Measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

2023/0109(COD) - 08/12/2023 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Industry, Research and Energy adopted the report by Lina GÁLVEZ MUÑOZ (S&D, ES) on the proposal for a regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents.

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:

Coordinated governance

Members stressed that close and coordinated cooperation is needed between the public sector, the private sector, academia, civil society and the media. Moreover, the Union's response needs to be coordinated with international institutions as well as trusted and like-minded international partners. To ensure cooperation with trusted and like-minded international partners and protection against systemic rivals, entities established in third countries that are not parties to the WTO Agreement on Government Procurement (GPA) should not be allowed to participate in procurement under this Regulation.

Cybersecurity reserve

Regarding the new cybersecurity reserve, Members believe it has the potential of developing industrial capacities in the EU, including for **SMEs**, with investments in research and innovation to develop state of the art technologies, such as cloud and artificial intelligence technologies. In addition, the report proposed to maintain the participation of the industry, enhance the criteria and trust of their participation (i.e. connecting their participation to a national or local company) by clarifying the criteria and the definition of technological sovereignty and to guarantee a balance between non-EU and EU actors. In addition, Members proposed for the Cyber Emergency Mechanism a certification scheme to be used for private providers to build a longstanding and trusted partnership.

To support the establishment of the EU Cybersecurity Reserve, the Commission could consider requesting ENISA to prepare a **candidate certification scheme** for managed security services in the areas covered by the Cybersecurity Emergency Mechanism. To fulfil the additional tasks deriving from this provision, **ENISA** should receive adequate, **additional funding**.

Funding

Considering geopolitical developments and the growing cyber threat landscape and in order to ensure continuity and further development of the measures laid down in this Regulation beyond 2027, particularly the European Cyber Shield and the Cybersecurity Emergency Mechanism, it is necessary to ensure a **specific budget line** in the multiannual financial framework for the period 2028-2034. According to the report, Member States should endeavour to commit themselves to supporting all necessary measures to reduce cyber threats and incidents throughout the Union and to strengthen solidarity.

Strengthening R&I in cybersecurity

The amended text called for enhanced research and innovation (R&I) in cybersecurity to increase the resilience and the open strategic autonomy of the Union. Similarly, it is important to create synergies with R&I programmes and with existing instruments and institutions and to strengthen cooperation and coordination among the different stakeholders, including the private sector, civil society, academia, Member States, the Commission and ENISA.

Evaluation and Review

The amended text stated that by two years from the date of application of this Regulation and every two years thereafter, the Commission should carry out an evaluation concerning, *inter alia*: (i) both the positive and the negative working of the Cybersecurity Emergency Mechanism; (ii) the contribution of this Regulation to reinforce the Union's resilience and open strategic autonomy, to improve the competitiveness of the relevant industry sectors, microenterprises, SMEs including start-ups, and the development of cybersecurity skills in the Union; (iii) the use and added value of the EU Cybersecurity Reserve.

Measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

2023/0109(COD) - 18/04/2023 - Legislative proposal

PURPOSE: to lay down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents (EU Cyber solidarity act).

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: the magnitude, frequency and impact of cybersecurity incidents are increasing, including supply chain attacks aiming at cyberespionage, ransomware or disruption. They represent a major threat to the functioning of network and information systems. In view of the fast-evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage to critical infrastructures demands heightened preparedness at all levels of the Union's cybersecurity framework. That threat goes beyond Russia's military aggression on Ukraine and is likely to persist given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions.

CONTENT: with this proposal, the Commission aims to set up **Cyber Solidarity Act** which establishes EU capabilities to make Europe more resilient and reactive in front of cyber threats, while strengthening existing cooperation mechanism. It will contribute to ensuring a safe and secure digital landscape for citizens and businesses and to protecting critical entities and essential services, such as hospitals and public utilities.

This Regulation lays down measures to strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, in particular through the following actions:

European Cyber Shield

An interconnected pan-European infrastructure of Security Operations Centres (European Cyber Shield) will be established to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. It will be composed of Security Operations Centres (SOCs) across the EU, brought together in several multi-country SOC platforms, built with support from the Digital Europe Programme (DEP) to supplement national funding. The Cyber Shield will be tasked with improving the detection, analysis and response to cyber threats. These SOCs will use advanced technology such as Artificial Intelligence (AI) and data analytics to detect and share warnings on such threats with authorities across borders. They will allow for a more timely and efficient response to major threats.

Cyber Emergency Mechanism

The Cyber Emergency Mechanism will improve the Union's resilience to major cybersecurity threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant and large-scale cybersecurity incidents. It provides for actions to support preparedness, including coordinated testing of entities operating in highly critical sectors, response to and immediate recovery from significant or large-scale cybersecurity incidents or mitigate significant cyber threats and mutual assistance actions.

Also set to be created is an **EU Cybersecurity Reserve** made up of **trusted and certified private companies** ready to respond to major incidents.

European Cybersecurity Incident Review Mechanism

The proposed Regulation would also establish the Cybersecurity Incident Review Mechanism to assess and review specific cybersecurity incidents. At the request of the Commission or of national authorities (the EU-CyCLONe or the CSIRTs network), the EU Cybersecurity Agency (ENISA) will be responsible for the review of specific significant or large-scale cybersecurity incident and should deliver a report that includes lessons learned, and where appropriate, recommendations to improve Union's cyber response.

Budgetary implications

The EU Cybersecurity Shield and the Cybersecurity Emergency Mechanism of this Regulation will be supported by funding under Strategic Objective 'Cybersecurity' of Digital Europe Programme (DEP).

The total budget includes an increase of EUR 100 million that this Regulation proposes to re-allocate from other Strategic Objectives of DEP. This will bring the new total amount available for Cybersecurity actions under DEP to EUR 842.8 million. Part of the additional EUR 100 million will reinforce the budget managed by the ECCC to implement actions on SOCs and preparedness as part of their Work Programme(s). Moreover, the additional funding will serve to support the establishment of the EU Cybersecurity Reserve.

It complements the budget already foreseen for similar actions in the main DEP and Cybersecurity DEP WP from the period 2023-2027 which could bring the total to 551 million for 2023-2027, while 115 million were dedicated already in the form of pilots for 2021-2022. Including Member States contributions, the overall budget could amount up to EUR 1.109 billion.

Measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

2023/0109(COD) - 15/01/2025 - Final act

PURPOSE: to strengthen EU's solidarity and capacities to detect, prepare for and respond to cybersecurity threats and incidents.

LEGISLATIVE ACT: Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021 /694 (Cyber Solidarity Act).

CONTENT: this regulation is part of the Cybersecurity legislative package which also includes a targeted amendment to the Cybersecurity Regulation.

The regulation down measures to strengthen capacities in the Union to detect, prepare for and respond to cyber threats and incidents. It pursues the general objectives of reinforcing the competitive position of industry and services in the Union across the digital economy, including microenterprises and small and medium-sized enterprises as well as start-ups, and of contributing to the **Union's technological sovereignty** and open strategic autonomy in the area of cybersecurity, including by boosting innovation in the Digital Single Market.

The regulation establishes:

(1) Cybersecurity Alert System

A cyber security alert system is established to support the development of advanced capabilities for the Union to enhance detection, analysis and data processing capabilities in relation to cyber threats and the prevention of incidents in the Union. It is a **pan-European network of infrastructures** composed of national cyber hubs and cross-border cyber hubs adhering to it on a voluntary basis. These entities will be responsible for sharing information and detecting and responding to cyber threats. The cyber hubs will use state-of-the-art technology, such as artificial intelligence (AI) and advanced data analytics, to detect and share timely warnings on cyber threats and incidents across borders. They will strengthen the existing European framework and, in turn, authorities and relevant entities will be able to respond more efficiently and effectively to cybersecurity incidents.

(2) Cybersecurity Emergency Mechanism

This emergency mechanism is established to support the improvement of the Union's resilience to cyber threats and the preparation for and mitigation of, in a spirit of solidarity, the short-term impact of significant cybersecurity incidents, large-scale cybersecurity incidents and large-scale-equivalent cybersecurity incidents.

The cybersecurity emergency mechanism will support the following:

- **preparedness actions**, including testing entities in highly critical sectors (healthcare, transport, energy, etc.) for potential vulnerabilities, based on common risk scenarios and methodologies;

- a new **EU Cybersecurity Reserve** composed of incident response services provided by the private sector and ready to intervene, at the request of a Member State or EU institutions, bodies and agencies and associated third countries, in the event of a significant or large-scale cybersecurity incident. To benefit from support from the EU Cybersecurity Reserve, users must take all appropriate measures to mitigate the effects of the incident for which they are requesting support. Requests for support must be reviewed by the contracting authority. A response must be provided to users without delay and in any case no later than 48 hours after the submission of the request to ensure the effectiveness of the support;

- a **new EU cybersecurity reserve** consisting of incident response services from the private sector ready to intervene at the request of a member state or EU institutions, bodies, and agencies, as well as associated third countries, in case of a significant or large-scale cybersecurity incident;

- technical **mutual assistance**.

(3) A cybersecurity incident review mechanism

In order to support the objectives of promoting shared situational awareness and enabling effective response to significant cybersecurity incidents and large-scale cybersecurity incidents, the Commission or the European cyber crisis liaison organisation network (EU-CyCLONe) will be able to request ENISA, with the support of the CSIRTs network and with the approval of the Member States concerned, to review and assess cyber threats, known exploitable vulnerabilities and mitigation actions with respect to a specific significant cybersecurity incident or large-scale cybersecurity incident.

Following the completion of a review and assessment of an incident, ENISA will prepare an **incident review report**, in collaboration with the Member State concerned, relevant stakeholders, including representatives from the private sector, the Commission and other relevant Union institutions,

bodies, offices and agencies. Building on the collaboration with stakeholders, including from the private sector, the review report on specific incidents should aim to assess the causes, impact and mitigation of an incident, after it has occurred.

ENTRY INTO FORCE: 4.2.2025.

Measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents

2023/0109(COD) - 24/04/2024 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 470 votes to 23, with 90 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amends the proposal as follows:

Subject-matter and objectives

The proposed Regulation lays down measures to strengthen capacities in the Union to **detect, prepare for and respond to cybersecurity threats and incidents**, in particular through the following actions:

- the establishment of a **pan-European network of Cyber Hubs** ('European Cybersecurity Alert System') to build and enhance coordinated detection and common situational awareness capabilities;

- the establishment of a **Cybersecurity Emergency Mechanism** to support Member States and other users in preparing for, responding to, mitigating the impact of and initiating recovery from significant, large-scale and large-scale equivalent cybersecurity incidents;

- the establishment of a **European Cybersecurity Incident Review Mechanism** to review and assess significant or large-scale incidents.

This Regulation pursues the general objectives of reinforcing the competitive position of industry and service sectors in the Union across the digital economy, including microenterprises and small and medium-sized enterprises as well as start-ups, and of contributing to the Union's technological sovereignty and open strategic autonomy in the area of cybersecurity, including by boosting innovation in the Digital Single Market. It pursues those objectives by **strengthening solidarity at Union level**, reinforcing the cybersecurity ecosystem, enhancing Member States' cyber resilience and developing the skills, know-how, abilities and competencies of the workforce in relation to cybersecurity.

This Regulation is without prejudice to the Member States' essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

Establishment of the European Cybersecurity Alert System

A pan-European network of infrastructure that consists of **National Cyber Hubs and Cross-Border Cyber Hubs** joining on a voluntary basis, the European Cybersecurity Alert System should be established to support the development of advanced capabilities for the Union to enhance detection, analysis and data processing capabilities in relation to cyber threats and the prevention of incidents in the Union.

Where a Member State decides to participate in the European Cybersecurity Alert System, it should designate or, where applicable, establish a National Cyber Hub.

National Cyber Hubs may cooperate with private sector entities to exchange relevant data and information for the purpose of detecting and preventing cyber threats and incidents, including with sectoral and cross-sectoral communities of essential and important entities. Where appropriate and in accordance with national and Union law, the information requested or received by National Cyber Hubs may include telemetry, sensor and logging data.

Cross-Border Cyber Hubs

Where at least three Member States are committed to ensuring that their National Cyber Hubs work together to coordinate their cyber-detection and threat monitoring activities, those Member States may establish a Hosting Consortium.

A Cross-Border Cyber Hub should be a multi-country platform established by a written consortium agreement. It should bring together in a coordinated network structure the National Cyber Hubs of the Hosting Consortium's Member States. It should be designed to enhance the monitoring, detection and analysis of cyber threats, to prevent incidents and to support the production of cyber threat intelligence, notably through the exchange of relevant and, where appropriate, anonymised data and information, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis and prevention and protection capabilities in a trusted environment.

Emergency mechanism

A Cybersecurity Emergency Mechanism should be established to support improvement of the Union's resilience to cyber threats and prepare for and mitigate, in a spirit of solidarity, the short-term impact of significant, large-scale and large-scale-equivalent cybersecurity incidents.

The Cybersecurity Emergency Mechanism should support the following types of actions: (i) preparedness actions, namely the **coordinated preparedness testing** of entities operating in sectors of high criticality across the Union ; (ii) other preparedness actions for entities operating in sectors of high criticality and other critical sectors; (iii) actions supporting response to and initiating recovery from significant, large-scale and large-scale-

equivalent cybersecurity incidents, to be provided by trusted managed security service providers participating in the EU Cybersecurity Reserve; (iv) mutual assistance actions granted in the form of grants and under the conditions defined in the relevant work programmes referred to in the Digital Europe Programme.

Establishment of the EU Cybersecurity Reserve

An EU Cybersecurity Reserve should be established, in order to assist, upon request, in responding or providing support for responding to significant, large-scale, or large-scale-equivalent cybersecurity incidents, and initiating recovery from such incidents.

ENISA should prepare, at least every two years, a mapping of the services needed by the users. ENISA should prepare a similar mapping, after informing the Council and consulting EU-CyCLONe and the Commission. A response should be transmitted to the users without delay and in any event no later than 48 hours from the submission of the request to ensure effectiveness of the support action. The contracting authority should inform the Council and the Commission of the results of the process.

A **third country** associated with the Digital Europe Programme should apply for support from the EU Cybersecurity Pool where the agreement by which it is associated with the Digital Europe Programme provides for its participation in the Pool.

Evaluation and review

By two years from the date of application of this Regulation and at least every four years thereafter, the Commission should carry out an evaluation of the functioning of the measures laid down in this Regulation and should submit a report to the European Parliament and to the Council.