








# Procedure file

Basic information	
COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	Awaiting Council's 1st reading position
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 <a href="#">Industry, Research and Energy</a>		02/05/2023
		 <a href="#">GÁLVEZ MUÑOZ Lina</a>	
		Shadow rapporteur	
		 <a href="#">NIEBLER Angelika</a>	
		 <a href="#">GROOTHUIS Bart</a>	
		 <a href="#">NIINISTÖ Ville</a>	
		 <a href="#">TOŠENOVSKÝ Evžen</a>	
	Committee for opinion	Rapporteur for opinion	Appointed
	AFET <a href="#">Foreign Affairs</a>		16/06/2023
		 <a href="#">TUDORACHE Dragoș</a>	
	BUDG <a href="#">Budgets</a>	The committee decided not to give an opinion.	
	CONT <a href="#">Budgetary Control</a>	The committee decided not to give an opinion.	
	IMCO <a href="#">Internal Market and Consumer Protection</a>	The committee decided not to give an opinion.	
	TRAN <a href="#">Transport and Tourism</a>		07/07/2023
		 <a href="#">FALCĂ Gheorghe</a>	
	LIBE <a href="#">Civil Liberties, Justice and Home Affairs</a>	The committee decided not to give an opinion.	

### Key events

18/04/2023	Legislative proposal published	<a href="#">COM(2023)0209</a>	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	<a href="#">A9-0426/2023</a>	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	<a href="#">PE760.882</a> GEDA/A/(2024)001689	
24/04/2024	Decision by Parliament, 1st reading	<a href="#">T9-0355/2024</a>	

### 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 173-p3; Treaty on the Functioning of the EU TFEU 322-p1
Mandatory consultation of other institutions	<a href="#">European Economic and Social Committee</a>
Stage reached in procedure	Awaiting Council's 1st reading position
Committee dossier	ITRE/9/11824

### Documentation gateway

Legislative proposal		<a href="#">COM(2023)0209</a>	18/04/2023	EC	Summary
Economic and Social Committee: opinion, report		<a href="#">CES2408/2023</a>	13/07/2023	ESC	
Committee draft report		<a href="#">PE752.795</a>	04/09/2023	EP	
Amendments tabled in committee		<a href="#">PE753.628</a>	22/09/2023	EP	
Committee opinion	TRAN	<a href="#">PE752.607</a>	25/10/2023	EP	

Committee opinion	<b>AFET</b>	<a href="#">PE750.145</a>	27/10/2023	EP	
Committee of the Regions: opinion		<a href="#">CDR2191/2023</a>	29/11/2023	CofR	
Committee report tabled for plenary, 1st reading/single reading		<a href="#">A9-0426/2023</a>	08/12/2023	EP	Summary
Text agreed during interinstitutional negotiations		<a href="#">PE760.882</a>	20/03/2024	EP	
Coreper letter confirming interinstitutional agreement		GEDA/A/(2024)001689	21/03/2024	CSL	
Text adopted by Parliament, 1st reading/single reading		<a href="#">T9-0355/2024</a>	24/04/2024	EP	

#### Additional information

Research document	<a href="#">Briefing</a>	27/11/2023
-------------------	--------------------------	------------

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

**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 Unions cybersecurity framework. That threat goes beyond Russias 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 Unions 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 Unions 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 SOC's 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

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 Unions 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.

Transparency				
GÁLVEZ MUÑOZ Lina	Rapporteur	ITRE	28/02/2024	The Kangaroo Group
GÁLVEZ MUÑOZ 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 MUÑOZ 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	FOX IT
GROOTHUIS Bart	Shadow rapporteur	ITRE	13/09/2023	VNO-NCW
NIINISTÖ Ville	Shadow rapporteur	ITRE	05/09/2023	Electronic Frontier Finland