Basic information

2020/0359(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Directive	Procedure completed
A high common level of cybersecurity Repealing Directive (EU) 2016/1148 2013/0027(COD) **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 7.30.09 Public security **Legislative priorities** Joint Declaration 2021 Joint Declaration 2022	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
ITRE Industry, Research and Energy	GROOTHUIS Bart (Renew)	14/01/2021
	Shadow rapporteur MAYDELL Eva (EPP) KAILI Eva (S&D) ANDRESEN Rasmus (Greens/EFA) TOŠENOVSKÝ Evžen (ECR) MARIANI Thierry (ID) MATIAS Marisa (The Left)	

Committee for opinion	Rapporteur for opinion	Appointed
AFET Foreign Affairs	GREGOROVÁ Markéta (Greens/EFA)	22/02/2021
ECON Economic and Monetary Affairs	The committee decided not to give an opinion.	
IMCO Internal Market and Consumer Protection	LØKKEGAARD Morten (Renew)	09/02/2021

	TRAN Transport and Tourism	DALUNDE Jakop G. (Greens /EFA)	03/02/2021
	CULT Culture and Education	The committee decided not to give an opinion.	
	LIBE Civil Liberties, Justice and Home Affairs (Associated committee)	MANDL Lukas (EPP)	12/04/2021

Council of the European Union	

European Commission	**Commission DG**	**Commissioner**
	Communications Networks, Content and Technology	BRETON Thierry

European Economic and Social Committee

Key events

Date	Event	Reference	Summary
16/12/2020	Legislative proposal published	COM(2020)0823	Summary
21/01/2021	Committee referral announced in Parliament, 1st reading		
20/05/2021	Referral to associated committees announced in Parliament		
28/10/2021	Vote in committee, 1st reading		
28/10/2021	Committee decision to open interinstitutional negotiations with report adopted in committee		
04/11/2021	Committee report tabled for plenary, 1st reading	A9-0313/2021	Summary
10/11/2021	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 72)		
22/11/2021	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 72)		
13/07/2022	Approval in committee of the text agreed at 1st reading interinstitutional negotiations		
10/11/2022	Decision by Parliament, 1st reading	T9-0383/2022	Summary
10/11/2022	Results of vote in Parliament		
10/11/2022	Debate in Parliament		
28/11/2022	Act adopted by Council after Parliament's 1st reading		
14/12/2022	Final act signed		
27/12/2022	Final act published in Official Journal		

Technical information	
Procedure reference	2020/0359(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Directive
Amendments and repeals	Repealing Directive (EU) 2016/1148 2013/0027(COD)
Legal basis	Rules of Procedure EP 57_o Treaty on the Functioning of the European Union TFEU 114-p1
Other legal basis	Rules of Procedure EP 165
Mandatory consultation of other institutions	European Economic and Social Committee
Stage reached in procedure	Procedure completed
Committee dossier	ITRE/9/04961

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE692.602	03/05/2021	
Amendments tabled in committee		PE693.680	03/06/2021	
Amendments tabled in committee		PE693.723	03/06/2021	
Committee opinion	TRAN	PE689.861	14/07/2021	
Committee opinion	IMCO	PE691.156	14/07/2021	
Committee opinion	AFET	PE691.371	15/07/2021	
Committee opinion	LIBE	PE693.822	15/10/2021	
Committee report tabled for plenary, 1st reading/single reading		A9-0313/2021	04/11/2021	Summary
Text adopted by Parliament, 1st reading/single reading		T9-0383/2022	10/11/2022	Summary

Council of the EU

Document type	Reference	Date	Summary
Draft final act	00032/2022/LEX	14/12/2022	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2020)0823	16/12/2020	Summary
Document attached to the procedure	SEC(2020)0430	16/12/2020	
Document attached to the procedure	SWD(2020)0344	16/12/2020	

Document attached to the procedure	SWD(2020)0345	16/12/2020	
Commission response to text adopted in plenary	SP(2022)688	17/01/2023	

National parliaments

Document type	Parliament /Chamber	Reference	Date	Summary
Contribution	CZ_CHAMBER	COM(2020)0823	25/02/2021	
Contribution	ES_PARLIAMENT	COM(2020)0823	18/03/2021	
Contribution	PT_PARLIAMENT	COM(2020)0823	18/03/2021	
Contribution	ES_PARLIAMENT	SWD(2020)0344	22/03/2021	
Contribution	ES_PARLIAMENT	SWD(2020)0345	22/03/2021	
Contribution	CZ_SENATE	COM(2020)0823	24/03/2021	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary
EDPS	Document attached to the procedure	N9-0025/2021 OJ C 183 11.05.2021, p. 0003	11/03/2021	
EESC	Economic and Social Committee: opinion, report	CES5749/2020	27/04/2021	
ECB	European Central Bank: opinion, guideline, report	CON/2022/0014 OJ C 233 16.06.2022, p. 0022	11/04/2022	

Additional information

Source	Document	Date
European Parliament	Briefing	19/02/2021
European Commission	EUR-Lex	

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
GROOTHUIS Bart	Rapporteur	ITRE	21/06/2022	Considerati Brussels B.V.
GROOTHUIS Bart	Rapporteur	ITRE	20/06/2022	ICANN
GROOTHUIS Bart	Rapporteur	ITRE	10/06/2022	ICANN

GROOTHUIS Bart	Rapporteur	ITRE	24/03/2022	ICANN
GROOTHUIS Bart	Rapporteur	ITRE	23/03/2022	Broadcom
GROOTHUIS Bart	Rapporteur	ITRE	17/03/2022	BUSINESSEUROPE
GROOTHUIS Bart	Rapporteur	ITRE	09/03/2022	Palo Alto Networks Inc.
GROOTHUIS Bart	Rapporteur	ITRE	03/03/2022	Hanbury Strategy and Communications Limited
GROOTHUIS Bart	Rapporteur	ITRE	03/03/2022	DIGITALEUROPE
GROOTHUIS Bart	Rapporteur	ITRE	10/02/2022	Provincie Flevoland

Other Members

Transparency

Name	Date	Interest representatives
PETERSEN Morten	11/11/2021	Euritas

Final act

Corrigendum to final act 32022L2555R(04)
OJ L 000 22.12.2023, p. 0000

Directive 2022/2555
OJ L 333 27.12.2022, p. 0080 Summary

A high common level of cybersecurity

2020/0359(COD) - 27/12/2022 - Final act

PURPOSE: to strengthen cybersecurity and resilience across the EU.

LEGISLATIVE ACT: Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

CONTENT: the Directive establishes measures that aim to achieve a **common high level of cybersecurity** across the Union with a view to further improving the resilience and incident response capabilities of both the public and private sectors and the EU as a whole. The new Directive, called 'NIS 2', will replace the current Network and Information Security Directive (NIS Directive).

Objective

The revised Directive aims to **harmonise cybersecurity requirements** and implementation of cybersecurity measures in different Member States. To achieve this, it sets out minimum rules for a regulatory framework and lays down mechanisms for effective cooperation among relevant authorities in each Member State.

The NIS2 Directive will form the basis for **cybersecurity risk management** measures and **reporting obligations** in all key sectors covered by the Directive, namely energy, transport, banking, financial market infrastructure, health, drinking water, digital infrastructure, public administrations and the space sector, as well as in important sectors such as postal services, waste management, chemicals, food, medical device manufacturing, electronics, machinery, vehicle engines and digital suppliers.

Scope

The new NIS2 Directive introduces a **size-cap rule** as a general rule for identification of regulated entities. This means that all medium and large entities operating in the sectors covered by the Directive or providing services within its scope will fall within its scope.

The Directive will apply to public administration entities at central and regional level. In addition, Member States may decide to apply it also to such entities at local level and to educational institutions, in particular where they carry out critical research activities.

The Directive will not apply to public administration entities carrying out activities in the fields of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences. Parliaments and central banks are also excluded from the scope.

The Directive lays down minimum rules for a regulatory framework and does not prevent Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity.

While the revised directive maintains this general rule, its text includes additional provisions to ensure **proportionality**, a higher level of risk management and clear-cut criticality criteria for allowing national authorities to determine further entities covered.

Coordinated cyber security frameworks

The Directive sets out obligations for Member States to adopt **national cybersecurity strategies**, designate or establish competent authorities, cyber crisis management authorities, single cyber security contact points and computer security incident response centres (CSIRTs).

Cooperation at EU level

The Directive sets out mechanisms for effective cooperation between the competent authorities of each Member State. It establishes a **Cooperation Group** to support and facilitate strategic cooperation and information exchange between Member States and to build confidence. A **network of national CSIRTs** is established to contribute to confidence building and to promote swift and effective operational cooperation between Member States.

The Directive also formally establishes the European cyber crisis liaison organisation network (EU-CyCLONe), which will support the coordinated management of large-scale cyber security incidents.

Voluntary peer learning mechanism

A voluntary peer learning mechanism will enhance mutual trust and learning from good practices and experiences in the Union, thereby contributing to a common high level of cyber security.

The Cooperation Group will establish, by 17 January 2025, with the assistance of the Commission and ENISA and, where appropriate, the CSIRT network, the methodology and organisational aspects of peer reviews with a view to learning from shared experiences, building mutual trust, achieving a common high level of cybersecurity, as well as strengthening Member States' cybersecurity capacities and policies necessary for the implementation of the Directive.

Simplification of reporting obligations

The Directive streamlines the reporting obligations to avoid over-reporting and creating an excessive burden for the entities concerned.

In order to simplify the reporting of information required under the Directive and to reduce the administrative burden on entities, Member States will provide technical means, such as a single entry point, automated systems, online forms, user-friendly interfaces, templates and dedicated platforms for the use of entities, irrespective of whether they fall within the scope of the Directive, for the submission of the relevant information to be reported.

Lastly, the Directive provides for **remedies and penalties** to ensure compliance with the legislation.

ENTRY INTO FORCE: 16.1.2023

TRANSPOSITION: no later than 17.10.2024. The provisions will apply from 18.10.2024.

A high common level of cybersecurity

2020/0359(COD) - 16/12/2020 - Legislative proposal

PURPOSE: to introduce new measures for a common level of cybersecurity across the EU.

PROPOSED ACT: Directive 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: Directive (EU) 2016/1148 of the European Parliament and the Council aimed at building cybersecurity capabilities across the EU, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the EU's economy and society to function effectively.

However, since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union’s level of cybersecurity resilience.

CONTENT: this proposal builds on and repeals Directive (EU) 2016/1148 on security of network and information systems (NIS Directive), which is the first piece of EU-wide legislation on cybersecurity and provides legal measures to boost the overall level of cybersecurity in the EU. The proposal modernises the existing legal framework taking account of the increased digitisation of the internal market in recent years and an evolving cybersecurity threat landscape.

Specific provisions

Scope

The proposal should apply to certain public or private essential entities operating in the sectors listed in Annex I (energy; transport; banking; financial market infrastructures; health, drinking water; waste water; digital infrastructure; public administration and space) and certain important entities operating in the sectors listed in Annex II (postal and courier services; waste management; manufacture, production and distribution of chemicals; food production, processing and distribution; manufacturing and digital providers).

Micro and small entities are excluded from the scope of the Directive, except for providers of electronic communications networks or of publicly available electronic communications services, trust service providers, Top-level domain name (TLD) name registries and public administration, and certain other entities, such as the sole provider of a service in a Member State.

National cybersecurity frameworks

The proposal stipulates that Member States are required to adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of cybersecurity. The proposed directive also establishes a framework for Coordinated Vulnerability Disclosure and requires Member States to designate computer security incident response teams to act as trusted intermediaries and facilitate the interaction between the reporting entities and the manufacturers or providers of ICT products and ICT services.

Member States are required to put in place National Cybersecurity Crisis Management Frameworks, by designating national competent authorities responsible for the management of large-scale cybersecurity incidents and crises.

Cybersecurity risk management and reporting obligations

The proposal requires Member States to provide that management bodies of all entities under the scope to approve the cybersecurity risk management measures taken by the respective entities and to follow specific cybersecurity-related training. Member States are required to ensure that entities under the scope take appropriate and proportionate technical and organisational measures to manage the cybersecurity risks posed to the security of network and information systems.

TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data. Furthermore, such entities are required to provide efficient access to domain registration data for legitimate access seekers.

Jurisdiction and registration

As a rule, essential and important entities are deemed to be under the jurisdiction of the Member State where they provide their services. However, certain types of entities (DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery network providers, as well as certain digital providers) are deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.

Information sharing

Member States should provide rules enabling entities to engage in cybersecurity-related information sharing within the framework of specific cybersecurity information-sharing arrangements.

Supervision and enforcement

Competent authorities are required to supervise the entities under the scope of the proposed directive, and in particular to ensure their compliance with the security and incident notification requirements. The proposal also requires Members States to impose administrative fines to essential and important entities and defines certain maximum fines.

A high common level of cybersecurity

2020/0359(COD) - 04/11/2021 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Industry, Research and Energy adopted the report by Bart GROOTHUIS (Renew Europe, NL) on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

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 and scope

This Directive should apply to public and private entities of a type referred to as **essential entities** in Annex I and as **important entities** in Annex II who provide their services or carry out their activities within the Union. It should not apply to entities that qualify as micro and small enterprises. No later than 6 months after the transposition deadline, Member States should draw up a list of essential and important entities. This list should be updated regularly and at least every two years.

Essential and significant entities should **submit at least the following information to the competent authorities**: (i) name of the entity, (ii) address and updated contact details, including e-mail addresses, (iii) IP ranges, (iv) telephone numbers and (v) the relevant sector(s) and sub-sector(s) listed in Annexes I and II. Entities should inform the competent authorities of any changes to this information.

To this end, the European Union Agency for Cyber Security (ENISA), in cooperation with the Cooperation Group, should issue guidelines and templates on notification obligations as soon as possible. Processing of personal data under the Directive would be carried out in accordance with the General Data Protection Regulation (GDPR).

National cyber security strategy

The strategy should also include a framework for the allocation of roles and responsibilities of public bodies and entities and other relevant actors, a single point of contact on cyber security for SMEs, and an assessment of the general level of cyber security awareness among citizens.

Member States should also adopt:

- a cybersecurity policy for each sector covered by the Directive;

- requirements for encryption and the use of open source cyber security products;

- a policy related to maintaining the overall availability and **integrity of the public core of the open Internet**, including the cybersecurity of undersea communications cables;

- a policy to promote the development and integration of emerging technologies, such as artificial intelligence, into cybersecurity enhancing tools and applications;

- a policy to promote **cyber hygiene**, increasing general awareness of cyber security threats and best practices among citizens;

- a policy to promote active **cyber defence**;

- a policy to help authorities develop competences and understanding of the security aspects needed to design, build and manage connected places;

- a policy specifically addressing the **ransomware** threat and disrupting the ransomware business model;

- a policy, including relevant procedures and **governance frameworks**, to support and promote the development of public-private partnerships in cyber security.

ENISA should provide guidance to Member States to align national cyber security strategies with the requirements and obligations set out in the Directive.

Coordinated vulnerability disclosure and European vulnerability database

ENISA should develop and maintain a European vulnerability database leveraging the global Common Vulnerabilities and Exposures (CVE) registry. To this end, ENISA should adopt the necessary technical and organisational measures to ensure the security and integrity of the database.

Computer Security Incident Response Teams (CSIRTs)

Member States should ensure the possibility of effective, efficient and secure information exchange on all classification levels between their own CSIRTs and CSIRTs from third countries on the same classification level. CSIRTs should develop at least the following technical capabilities

- the ability to conduct real-time or near-real-time monitoring of networks and information systems, and anomaly detection;

- the ability to support intrusion prevention and detection;

- the ability to collect and conduct complex forensic data analysis, and to reverse engineer cyber threats;

- the ability to filter malign traffic;

- the ability to enforce strong authentication and access privileges and controls; and

- the ability to analyse cyber threats.

CSIRTs should be responsible for monitoring cyber threats, vulnerabilities and incidents at national level and **acquiring real-time threat intelligence**, responding to incidents and assisting entities involved, as well as contributing to the deployment of secure information sharing tools.

ENISA should publish, in cooperation with the Commission, a biennial report on the state of cyber security in the EU and submit it to the European Parliament.

Reporting obligations

Member States should establish a **single point of contact** for all notifications required under the Directive and other relevant EU legislation.

Essential and important entities should notify CSIRTs about significant incidents that have an impact on the availability of their service within 24 hours of becoming aware of the incident. They should notify CIRTs about significant incidents that breach the confidentiality and integrity of their services **within 72 hours** of becoming aware of the incident.

Fines

To ensure effective enforcement of the obligations laid down in this Directive, each competent authority should have the power to impose or request the imposition of administrative fines if the infringement was intentional, negligent or the entity concerned had received notice of the entity's non-compliance.

A high common level of cybersecurity

2020/0359(COD) - 10/11/2022 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 577 votes to 6 with 31 abstentions a legislative resolution on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

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

Strengthening EU-wide cybersecurity and resilience

This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market and to further improve the resilience and incident response capacities of both the public and private sector and the EU as a whole.

To that end, this Directive lays down:

- obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);

- cybersecurity risk management measures and reporting obligations for entities in 'critical' sectors such as energy, transport, banking, financial market infrastructure, health, drinking water, digital infrastructure, public administrations and the space sector, as well as in 'important' sectors such as postal services, waste management, chemicals, food, medical device manufacturing, electronics, machinery, vehicle engines and digital suppliers;

- **rules and obligations** on cybersecurity information sharing;

- **supervisory and enforcement obligations** on Member States.

The Directive lays down **minimum rules** for a regulatory framework and does not prevent Member States from adopting or maintaining provisions ensuring a higher level of cyber security.

Scope of application

All **medium and large entities** operating in the sectors covered by the Directive or providing services falling within its scope will fall within its scope.

As **public administrations** are often the target of cyber-attacks, the Directive will apply to public administration entities at central and regional level. In addition, Member States may decide to apply it also to such entities at local level as well as to educational institutions, in particular where they carry out critical research activities.

The Directive will not apply to public administration entities carrying out activities in the field of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences. Parliaments and central banks are also excluded from the scope.

The Directive includes additional provisions to ensure **proportionality**, a higher level of risk management and clear criteria on the **criticality of entities** to determine which ones are covered.

Cooperation at EU level

The Directive sets out mechanisms for effective cooperation between the competent authorities of each Member State. It establishes a **Cooperation Group** to support and facilitate strategic cooperation and information exchange between Member States and to build confidence. **A network of national CSIRTs** is established to contribute to confidence building and to promote swift and effective operational cooperation between Member States.

The Directive also formally establishes the European cyber crisis liaison organisation network (**EU-CyCLONe**), which will support the coordinated management of large-scale cyber security incidents.

Voluntary peer learning mechanism

Peer reviews should be introduced to help learn from shared experiences, **build mutual trust** and achieve a common high level of cyber security. The Cooperation Group should establish, no later than 2 years after the date of entry into force of the Directive, with the assistance of the Commission and ENISA and, where appropriate, the CSIRT network, the methodology and organisational aspects of peer reviews. Participation in peer reviews should be voluntary.

Simplification of reporting obligations

The Directive streamlines the reporting obligations to avoid over-reporting and creating an excessive burden for the entities concerned.

In order to simplify the reporting of information required under the Directive and to reduce the administrative burden on entities, Member States should provide technical means, such as a single entry point, automated systems, online forms, user-friendly interfaces, templates and dedicated platforms for the use of entities, irrespective of whether they fall within the scope of the Directive, for the submission of the relevant information to be reported.

Lastly, the Directive provides for **remedies and penalties** to ensure compliance with the legislation.