Council of the European Union

Brussels, 22 January 2026
(OR. en)

5627/26

Interinstitutional File:
2026/0012 (COD)

CYBER 30
JAI 91
DATAPROTECT 23
TELECOM 30
MI 59
IND 50
CADREFIN 27
FIN 104
BUDGET 4
CODEC 93

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	21 January 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2026) 13 final
Subject:	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]

Delegations will find attached document COM(2026) 13 final.

Encl.: COM(2026) 13 final

EUROPEAN
COMMISSION

Strasbourg, 20.1.2026
COM(2026) 13 final

2026/0012 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]

{SWD(2026) 11-12} - {SEC(2026) 11}

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

This proposal is part of a package of measures that aims at aligning the Union's cybersecurity framework with the needs of stakeholders in an increasingly sophisticated cyber threat landscape and complex geopolitical reality. Essential and important entities from critical sectors are increasingly targeted by cyberattacks[1] while state threat actors leverage emerging technologies such as artificial intelligence (AI) to further scale and optimise their attacks. In this context, the resilience of critical infrastructure in the face of cyber threats is recognised as a strategic pillar for our democracies and the economic security of the Union. Both the European Preparedness Union Strategy[2] and the European Internal Security Strategy (ProtectEU)[3] have placed cybersecurity at the heart of the Union's resilience agenda. Similarly, the Communication on Strengthening EU economic security[4] identifies preventing access to sensitive information and data that could undermine the Union's economic security and preventing and mitigating disruptions to Union's critical infrastructure affecting the Union economy as priority objectives, in which effective cybersecurity measures play a crucial role. Further, the Draghi Report highlighted the need to increase security and reduce dependencies as one main area of action needed in the Union[5]. In its Communication on a Simpler and Faster Europe[6], the Commission announced its commitment to an ambitious programme to promote forward-looking, innovative policies that strengthen the Union's competitiveness and lighten the regulatory burdens on people, businesses and administrations, while maintaining the highest standard in promoting its values.

Against this background, the present proposal for a Directive amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2)] aims at addressing the problem of the complexity and diversity of the cybersecurity-related policies impacting the Union's cyber posture in particular by introducing clarifications and making compliance for regulated entities easier.

The objective of the present directive should be considered as part of the overarching goals of the Cybersecurity Act revision package involving the proposal for a Regulation by the European Parliament and the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881. The proposal for that regulation aims to tackle: (i) the misalignment between the Union's cybersecurity policy framework and stakeholders' needs in an increasingly hostile threat landscape; (ii) the stalled implementation of the European cybersecurity certification framework (ECCF); (iii) the complexity and diversity of

---

1 ENISA, ENISA Threat Landscape 2025.
2 JOIN/2025/130 final.
3 COM/2025/148 final.
4 JOIN(2025) 977 final.
5 European Commission, The future of European Competitiveness, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.
6 COM(2025) 47 final.

the cybersecurity-related policies impacting the Union's cyber posture; and (iv) increasing ICT supply chains security risks. Concerning the complexity and diversity of the cybersecurity-related policies impacting the Union's cyber posture, the Cybersecurity Act revision package proposes – as part of a reform of the European Cybersecurity Certification Framework – to promote certification as a compliance tool for businesses, and to enable the development of a scheme on the cyber posture of entities to reduce compliance costs for entities subject to the NIS 2 Directive and other relevant Union cybersecurity legislation. This approach will significantly simplify regulatory obligations for entities subject to multiple compliance requirements and ensure a more effective use of resources across national authorities.

The explanatory memorandum of the proposal for a Cybersecurity Act 2 regulation outlines the key issues underlying the proposal, as well as the specific objectives to address them. The proposal for a directive will address the specific objective 4 (SPO4) of the CSA revision impact assessment, i.e. to establish mechanisms and conditions to help facilitate compliance with cybersecurity requirements and in that way make their implementation more coherent and effective. Targeted amendments to the NIS 2 Directive aim to simplify compliance with and ensure streamlined and coherent implementation of specific aspects of the cybersecurity framework, including with regard to scope, definitions, ransomware reporting and supervision of entities providing cross-border services.

The proposal for a directive amending Directive (EU) 2022/2555 on simplification measures and alignment with the [Cybersecurity Act 2] falls within the remit of the regulatory fitness and performance programme (REFIT). Together with the revision of the Cybersecurity Act, it strongly contributes to improving clarity, removing inefficiencies and aligning procedures across legal frameworks. It contributes to the proper functioning of the internal market while ensuring the security and strategic autonomy of the Union.

- **Consistency with existing policy provisions in the policy area**

The Union has expanded its legal and policy tools with the adoption of a number of legal instruments and policy measures: (i) the NIS 2 Directive serves to strengthen cybersecurity for critical infrastructure; (ii) physical security measures are defined in its 'sister directive', the Critical Entities Resilience (CER) Directive; (iii) the Cyber Resilience Act (CRA) enhances the cybersecurity of products; (iv) the Cyber Solidarity Act (CSoA) builds EU-wide response capabilities; (v) the EU Cyber Blueprint[7] supports EU-level crisis management cooperation; (vi) the 5G Cybersecurity Toolbox (5G Toolbox) supports cybersecurity in 5G networks; (vii) the European action plan on the cybersecurity of hospitals and healthcare providers[8] helps improve their cybersecurity; and (viii) the Cybersecurity Skills Academy[9] addresses the growing challenge of the cybersecurity talent gap.

The above-mentioned cybersecurity legal framework was complemented by sector-specific legislation, i.e. the Digital Operational Resilience Act (DORA Regulation) for the financial sector, network code on sector-specific rules for cybersecurity aspects of cross-border

7 COM/2025/66 final.
8 COM(2025) 10 final.
9 COM(2023) 207 final.

electricity flows (NCCS) for the electricity sub-sector, information security rules (Part-IS[10]) for the air transport sub-sector.

This proposal for a directive, similarly to the proposal for a regulation it accompanies, is a part of a wider set of legal and policy initiatives adopted by the Union to improve the resilience of entities against security and cyber threats. It is focused on targeted amendments to the NIS 2 Directive which aim inter alia at clarifying certain aspects regarding the scope, definitions and jurisdictional rules, reduce burden in supervision of essential and important and facilitate supervision of cross-border entities by strengthening ENISA's role in operational cooperation support. Furthermore, jointly with the proposal for a regulation, this proposal creates a strong synergy stemming from the development of cyber posture certification for the NIS 2 Directive as well as potentially for facilitating compliance with other relevant Union legal acts such as the General Data Protection Regulation (GDPR), without prejudice to their specific certification requirements. These simplification measures should unlock resources to strengthen the operational cybersecurity preparedness of entities in the Union's critical sectors.

- **Consistency with other Union policies**

This proposal strengthens the security requirements for entities providing Business Wallets as set out in the proposal for a Regulation of the European Parliament and the Council on the establishment of European Business Wallets[11]. Moreover, the Commission will ensure consistency with upcoming initiatives, such as the Digital Networks Act (DNA). This proposal is aligned with the proposal for a Regulation on simplification of the digital legislation (Digital Omnibus) which contains inter alia amendments to the NIS 2 Directive, along with other Union legal acts. The Digital Omnibus proposes to facilitate compliance with cybersecurity reporting requirements, among others under the NIS 2 Directive, by reporting via a single-entry point for incident reporting, to be developed and maintained by ENISA. Furthermore, this proposal is aligned with the Proposal for a Regulation of the European Parliament and of the Council on the safety, resilience and sustainability of Space activities in the Union[12].

In addition, the proposal is in line with Future of European Competitiveness report of Mario Draghi, as highlighted above.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The legal basis for this directive is Article 114 of the Treaty on the Functioning of the European Union (TFEU), which seeks to establish and ensure the functioning of the internal market by enhancing measures for the approximation of national rules. This proposal amends Directive (EU) 2022/2555 which was adopted under Article 114 TFEU.

---

10 Commission Implementing Regulation (EU) 2023/203 and Commission Delegated Regulation (EU) 2022/1645.

11 COM/2025/838 final.

12 COM/2025/335 final.

- **Subsidiarity (for non-exclusive competence)**

The subsidiarity principle requires the assessment of the necessity and the added value of Union action. Compliance with the subsidiarity principle in this area was already recognised when adopting Directive (EU) 2022/2555 which is amended by this proposal.

This proposal facilitates compliance with Union cybersecurity legislation, reducing compliance costs and legal uncertainty for affected entities, and facilitating and improving the rate of compliance with cybersecurity requirements. It also contributes to help level the playing field on approaches to supervision and compliance checks across Member States.

- **Proportionality**

The rules proposed in this directive do not go beyond what is necessary to meet the specific objectives satisfactorily. The envisaged alignment and streamlining of scope, security measures and reporting obligations relate to Member States and businesses' requests to improve the current framework.

- **Choice of the instrument**

The proposal will amend the existing NIS 2 Directive and further streamline the obligations imposed on businesses, therefore ensure a higher level of harmonisation across the Union. The choice of legal instrument for this proposal is consistent with that of the legal text it is amending, i.e. the NIS 2 Directive. This proposal builds on the aim of the NIS 2 Directive to provide Member States with the flexibility needed to take into account national specificities.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

See the explanatory memorandum of the [proposal for the Cybersecurity Act 2].

- **Stakeholder consultations**

See the explanatory memorandum of the [proposal for the Cybersecurity Act 2].

- **Collection and use of expertise**

See the explanatory memorandum of the [proposal for the Cybersecurity Act 2].

- **Impact assessment**

See the explanatory memorandum as well as the impact assessment report accompanying the [proposal for the Cybersecurity Act 2].

- **Regulatory fitness and simplification**

See the explanatory memorandum of the [proposal for the Cybersecurity Act 2].

- **Fundamental rights**

See the explanatory memorandum of the [proposal for the Cybersecurity Act 2].

4. BUDGETARY IMPLICATIONS

Please refer to the legislative and financial statement in the [proposal for the Cybersecurity Act 2].

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

According to Article 40 of the NIS 2 Directive, the Commission will review the functioning of the Directive and report to the European Parliament and to the Council every 36 months.

- **Detailed explanation of the specific provisions of the proposal**

The proposal aims to facilitate compliance with cybersecurity obligations and unlock resources to strengthen the operational cybersecurity preparedness of entities in the Union's critical sectors.

The proposal introduces targeted amendments to the NIS 2 Directive to simplify specific aspects of the cybersecurity framework, increase legal certainty and harmonise implementation.

To make it easier for entities and suppliers to demonstrate compliance with the NIS 2 Directive, in line with the proposal for a regulation that this proposal accompanies, entities regulated by the NIS 2 Directive will be able to obtain certificates under organisational cybersecurity certification schemes developed within the ECCF.

To further facilitate compliance with cybersecurity risk-management measures for multi-country entities subject to supervision by competent authorities from several Member States, ENISA is entrusted with a new role supporting Member States in supervising those entities, facilitating mutual assistance and creating a better overview of entities in scope of the NIS 2 Directive.

Moreover, the proposal envisages that the Commission adopts guidelines on the application of supply chain security requirements that entities in scope of the NIS 2 Directive pass on to their suppliers, in order to ensure legal certainty and prevent the undue passing on of obligations on entities not in scope of the NIS 2 Directive.

Other targeted amendments to the NIS 2 Directive include:

- clarifications of the scope and definitions;
- removal of micro- and small-sized DNS service providers from the scope;
- introduction of maximum harmonisation for implementing acts under Article 21(5) (specifying cybersecurity risk-management measures) to facilitate compliance for entities and supervision for authorities;
- introduction of a new category of small mid-caps, in line with the 2025 Commission Recommendation on the definition of small mid-cap enterprises[18]; entities qualifying as small mid-caps are to be designated as important entities, reducing their compliance burden and the supervision burden on competent authorities;
- the requirement for Member States to adopt policies for the migration to post-quantum cryptography (PQC) as part of their national cybersecurity strategy; and
- introduction of a harmonised collection of data on ransomware attacks.

2026/0012 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national Parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Directive (EU) 2022/2555 of the European Parliament and of the Council[3] 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. Since the entry into force of Directive (EU) 2022/2555, progress has been made in increasing the Union's level of cyber resilience. At the same time, certain challenges have arisen during the implementation by Member States including in relation to the scope of the Directive, the implementation of the cybersecurity risk-management and incident reporting obligations and the supervision of cross-border entities. Building on the [proposal for the Cybersecurity Act 2], targeted amendments should be made to Directive (EU) 2022/2555 to address those challenges, by simplifying specific aspects in order to increase legal certainty and ensure uniform implementation of Directive (EU) 2022/2555.

(2) To reduce the burden of compliance for entities and of supervision for competent authorities, a new category of small mid-cap enterprises should be introduced in Directive (EU) 2022/2555, in line with Commission Recommendation (EU) 2025/1099[4]. Entities of a type referred to in Annex I to Directive (EU) 2022/2555,

---

1 OJ C [...], [...], p. [...]

2 OJ C [...], [...], p. [...]

3 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 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) (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

4 Commission Recommendation (EU) 2025/1099 of 21 May 2025 on the definition of small mid-cap enterprises (OJ L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).

which qualify as small mid-cap enterprises under that Recommendation, should as a main rule be designated as important entities. Further, to support the Commission 's goal of cutting administrative costs by 25 % overall and by 35 % for small and medium-sized enterprises, the general size-cap rule set out in Directive (EU) 2022/2555, whereby all entities which qualify as medium-sized enterprises under Article 2 of the Annex to Commission Recommendation 2003/361/EC[5], or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, fall within the scope of Directive (EU) 2022/2555, should be applied to Domain Name System service providers.

(3) During the implementation of Directive (EU) 2022/2555, there have been challenges in the interpretation of provisions regarding its scope. Therefore, certain scope-related provisions concerning healthcare providers, electricity producers, hydrogen undertakings and entities in the chemical sector should be clarified to ensure legal certainty and reduce compliance burden for both entities and national authorities.

(4) In order to ensure proportionality as regards electricity producers within the meaning of Article 2, point (38), of Directive (EU) 2019/944 of the European Parliament and of the Council[6], only those electricity producers with a total generation capacity of more than 1 MW should be considered to be essential or important entities under Directive (EU) 2022/2555, provided that they meet the size-cap rule. This should encompass electricity producers where a single electricity generation facility exceeds 1 MW as well as electricity producers that operate several generation facilities which together have a generation capacity of more than 1 MW. Such an approach enables a balance between the need to capture those entities where interference with their network and information system could imply a loss, non-controllability or external control of generation capacity that is on its own of relevance for the security and stability of the electricity grid, and the need not to place disproportionate administrative burden on undertakings under Directive (EU) 2022/2555.

(5) European Digital Identity Wallets as provided for in Regulation (EU) No 910/2014 of the European Parliament and of the Council[7] are an essential component of the Union's digital infrastructure, enabling secure identification and authentication and the exchange of electronic documents, including electronic attestations of attributes. Given their critical role for the public and for the provision of public and private services, any cybersecurity incident affecting those Wallets could have a broad impact. To ensure the provision of their services, the providers of European Digital Identity Wallets should be required to implement appropriate technical, operational and organisational measures to manage cybersecurity risks, prevent and respond to incidents, and cooperate with competent authorities in accordance with Directive (EU) 2022/2555. They should therefore be included among the entities covered by that Directive regardless of their size and be classified as essential entities. European

---

5 Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

6 Directive (EU) 2019/944 of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125; ELI: http://data.europa.eu/eli/dir/2019/944/oj).

7 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

Business Wallets offer similar functionalities and services tailored to the needs of economic operators and public sector bodies, building on the EU Digital Identity Framework, and are equally critical to the security and integrity of the digital economy. Consequently, providers of European Business Wallets established in accordance with [Proposal for a Regulation on the establishment of European Business Wallets][8] should be subject to the same cybersecurity requirements and obligations as providers of European Digital Identity Wallets, in order to ensure a consistent and high level of security across the entire digital identity ecosystem.

(6) Submarine data transmission infrastructure includes not only cables but also any infrastructure related to their operation. Such infrastructure includes landing stations and the terrestrial parts of the submarine cable connecting to them, such as land routes from beach manhole to landing station, data centre or point of presence. Submarine data transmission infrastructure is usually operated by entities already covered by Directive (EU) 2022/2555 including providers of public electronic communications networks and services or cloud computing service providers. However, submarine data transmission infrastructure may also be operated by other types of entities which do not currently fall within the scope of Directive (EU) 2022/2555, such as submarine data transmission infrastructure operated by providers of electronic communications networks which are not public, or by entities that lease the operation of submarine data transmission infrastructure either wholly or partially to providers of public electronic communications networks. Considering the increasing risks to submarine data transmission infrastructure and their resulting high criticality, it is necessary to ensure that all types of operators of submarine data transmission infrastructure are covered by Directive (EU) 2022/2555. Other maritime critical infrastructures, such as submarine electricity cables as well as gas, hydrogen and oil pipelines are typically already covered by Directive (EU) 2022/2555 as they are operated by transmission system operators in the sub-sectors electricity, gas, hydrogen and oil.

(7) In order to enable entities providing services across several Member States to benefit from more coherent and less burdensome supervisory approaches across the internal market, such entities should be able to demonstrate compliance with specific or all cybersecurity risk-management obligations laid down in Directive (EU) 2022/2555 by obtaining a certificate on the cyber posture under a European cybersecurity certification scheme. The development of such a scheme will benefit from the adoption of implementing acts on the technical and methodological as well as sectoral requirements concerning the cybersecurity risk-management measures under Directive (EU) 2022/2555 which are based on maximum harmonization.

(8) Given the continuously increasing reliance of our society and the economy on digital technologies, it is necessary to take mitigation measures against the quantum threat. The possibility of ‘harvest now - decrypt later attacks’, likely occurring already now, and the future risks induced by quantum attacks on forging signatures, as well as the planned deprecation of certain algorithm implementations and full disallowance of current public-key cryptographic algorithms, increase the urgency of initiating actions for the migration to post-quantum cryptography (PQC). Therefore, Member States should be required to adopt policies for the migration to PQC as part of their national cybersecurity strategy. Such policies should facilitate the acceleration of strategic planning and the creation of support measures and tools to assess the exposure of

[8] COM(2025) 838 final

cryptographic assets to the risks posed by quantum computers. Further, they should assist in creating a migration plan and in testing the roll-out of PQC in digital applications and networks, while simultaneously fostering the emergence and uptake of formally verified and evaluated European PQC solutions adhering to compliance frameworks in products and services. Those policies should align with the milestones set out in Union legal acts and Union policies as well as documents adopted by the NIS Cooperation Group, in particular the Coordinated Implementation Roadmap for the transition to PQC, adopted by the NIS Cooperation Group in June 2025, thus achieving the migration to PQC by 2030 for critical use cases and by 2035 for medium and low level use cases.

(9) Pursuant to Article 21(2), point (d), of Directive (EU) 2022/2555, essential and important entities are to ensure an appropriate level of security in their supply chain. In practice, that obligation has led many entities to request extensive information from their suppliers through heterogeneous questionnaires, formats, and processes. While such requests aim to support due diligence and risk management, they may also create a significant administrative burden for suppliers to essential and important entities, particularly when similar information must be provided repeatedly in divergent forms. To alleviate that burden and promote a consistent, proportionate and efficient approach to supply chain security assessments, the Commission should develop guidelines to recommend an appropriate level of detail, structure, and format for such information requests. Such guidelines should facilitate harmonisation, reduce unnecessary duplication, and support both entities and their suppliers in complying effectively with their obligations under Directive (EU) 2022/2555.

(10) Ransomware attacks in which malware encrypts data and systems and demands a ransom payment for release remain one of the prime threats to essential and important entities. Harmonising and improving the collection of data on ransomware attacks from affected essential and important entities would provide insights to computer security incident response teams (CSIRTs) and national authorities enabling them to ensure that future ransomware interventions are appropriate and effective, to support entities in growing their resilience and preventing future attacks, and to compile the intelligence and evidence that law enforcement agencies need to disrupt and dismantle ransomware gangs and sanction their operatives. Given the potentially sensitive nature of information to be shared regarding ransomware attacks, in particular whether an entity has paid a ransom, and if so, what amount and to whom, such information should only be submitted to CSIRTs or, where applicable, competent authorities upon their request. For the purpose of such information exchange, essential and important entities are encouraged to appoint a person that acts as a point of contact and ensures the confidentiality and trustworthiness of the information exchange. In the context of the International Counter Ransomware Initiative, the Union has endorsed a non-binding international policy statement whereby relevant institutions under the authority of the participating national governments should not pay ransomware extortion demands.

(11) Complying with the obligations to report relevant information about ransomware incidents should not result in the imposition of any additional obligations under Directive (EU) 2022/2555 to which the entity would not have been subject, had it not reported the information. To this effect, within the limits of their national legal order, Member States should address possible risks arising from increased liability linked to the reporting of relevant information about ransomware incidents.

(12) Given the cross-border dimension of many essential and important entities across the internal market and the need to ensure coherence and promote convergence and efficiency in relation to supervisory approaches, ENISA should support Member States in carrying out mutual assistance for essential and important entities which provide services in more than one Member State or which provide services in one or more Member States and have their network and information systems located in one or more other Member States. For that purpose, Member States should submit additional information to the registry of entities maintained by ENISA. Based on the information contained in the registry of essential and important entities, ENISA should conduct a comprehensive analysis on cross-border cybersecurity risks relating to essential and important entities. The analysis should be based on a methodology developed together with the Commission and the NIS Cooperation Group. That methodology could take into account the degree to which essential and important entities deploy their services on a wide cross-border basis, rely on cross-border services, are exposed to a supply chain concentration risk, can be identified as a source of supply chain concentration risk, are exposed to incidents that could have significant disruptive effects to cross-border services, or rely on network and information systems for the provision of their services that are located across different Member States and outside the Union. Based on the risk analysis report, ENISA should recommend to the relevant competent authorities to set up joint examination teams to support the supervision of entities with a higher degree of risk for the smooth functioning of the internal market in case of incidents and assist the competent authorities in the execution of joint supervisory actions upon their request.

(13) Since the objective of this Directive, namely to simplify the implementation of measures for a high common level of cybersecurity across the Union, cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve that objective.

(14) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(2) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[9] and delivered a joint opinion [date],

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Amendments to Directive (EU) 2022/2555

Directive (EU) 2022/2555 is amended as follows:

(1) Article 2 is amended as follows:

[9] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(a) in paragraph 2, point (a) is amended as follows:

(i) point (iii) is replaced by the following:

‘(iii) ‘top-level domain name registries;’;

(ii) the following points (iv) and (v) are added:

‘(iv) providers of European Digital Identity Wallets as provided in in Regulation (EU) No 910/2014;

(v) providers of European Business Wallets established in accordance with Regulation (EU) […]*.

_____

* ’Regulation (EU) […] [Proposal for a Regulation on the establishment of European Business Wallets].’;

(b) the following paragraph 3a is inserted:

‘3a. Regardless of their size, this Directive applies to entities identified as owners, managers and operators of strategic dual-use infrastructure under Regulation (EU) […]**.

_____

** ’Regulation (EU) […] [Proposal for a Regulation of the European Parliament and of the Council on establishing a framework of measures to facilitate the transport of military equipment, goods and personal across the Union.].’;

(2) Article 3 is amended as follows:

(a) paragraph 1 is amended as follows:

(i) points (a) and (b) are replaced by the following:

‘(a) entities of a type referred to in Annex I which exceed the ceilings for small mid-cap enterprises;

‘(b) qualified trust service providers, providers of European Digital Identity Wallets, providers of European Business Wallets and top-level domain name registries, regardless of their size;’;

(ii) the following point (h) is added:

‘(h) entities identified as owners, managers and operators of strategic dual-use infrastructure under Regulation (EU) […] [Proposal for a Regulation of the European Parliament and of the Council on establishing a framework of measures to facilitate the transport of military equipment, goods and personal across the Union].’;

(b) in paragraph 4, the first subparagraph is replaced by the following:

‘For the purpose of establishing the list referred to in paragraph 3, Member States shall require the entities referred to in that paragraph to submit at least the following information to the competent authorities:

(a) the name of the entity;

(b) the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable;

(c) the address of the entity or, where applicable, the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 26(3);

(d) up-to-date contact details, including email addresses, telephone numbers, the unique identifier and digital addresses of the European Business Wallet of the entity, where applicable, and its representative designated pursuant to Article 26(3), where applicable;

(e) the Member States where the entity provides services;

(f) the entity's IP ranges.';

(3) Article 5 is replaced by the following:

'*Article 5*

Minimum harmonisation

Without prejudice to Article 21(5), fifth subparagraph, this Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law.';

(4) in Article 6,

the following points (42) and (43) are added:

'(42) 'small mid-cap enterprise' means a small mid-cap enterprise as defined in the Annex to Commission Recommendation (EU) 2025/1099***;

(43) 'submarine data transmission infrastructure' means submarine cables transmitting data, the related infrastructure and other facilities or elements associated with data transmission.

*** Commission Recommendation (EU) 2025/1099 of 21 May 2025 on the definition of small mid-cap enterprises (OJ L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).';

(5) in Article 7(2), the following point (k) is added:

'(k) for the transition to post-quantum cryptography, taking into account the transition timelines and relevant requirements set out in applicable Union legal acts and policies.';

(6) in Article 15(2), the first sentence is replaced by the following:

'The CSIRTs network shall be composed of representatives of the CSIRTs designated or established pursuant to Article 10, the computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) and ENISA.';

(7) Article 21(5) is amended as follows:

(a) the second subparagraph is replaced by the following:

'The Commission may adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of

this paragraph. The Commission shall regularly assess whether implementing acts referred to in this subparagraph shall be adopted for specific sectors or types of entities to improve the functioning of the internal market. When preparing such assessments, the Commission shall focus in particular on the cross-border nature of sectors or types of entities and shall carry out an open, transparent and inclusive consultation process with relevant stakeholders and Member States.';

(b) the following fifth subparagraph is added:

'Where the Commission adopts implementing acts referred to in the first and second subparagraphs of this paragraph, Member States shall not impose any further technical, methodological or sectoral requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 on the entities in scope of those implementing acts.';

(8) in Article 23, the following paragraphs 12 and 13 are added:

'12. When adopting an implementing act pursuant to paragraph 11, first subparagraph, the Commission shall include requirements that the following information as regards ransomware attacks is submitted pursuant to paragraph 1:

(a) whether the entity detected a ransomware attack;

(b) the attack vector of the ransomware attack;

(c) whether mitigation measures have been implemented.

13. Member States shall ensure that in case of a significant incident caused by a ransomware attack, the entities concerned inform, upon request of the CSIRT or, where applicable, the competent authority via a communication channel provided by the CSIRT or, where applicable, the competent authority:

(a) if the entity has received a ransom demand and, where applicable, by whom;

(b) if a ransom was paid and if yes, what amount in what means of payment and to which recipient or receiving end, including the crypto-asset and crypto-asset service provider, where applicable.';

(9) in Article 24, the following paragraphs 4, 5 and 6 are added:

'4. In order to demonstrate compliance with Article 21, Member States may require essential and important entities to obtain a certificate on the cyber posture under a European cybersecurity certification scheme adopted pursuant to Article 75 of Regulation (EU) XXX/XXX **** [Proposal for CSA2].

5. Where the cyber posture of an essential or important entity is certified under a European cybersecurity certification scheme adopted pursuant to Article 74 of Regulation (EU) XXX/XXX**** [Proposal for CSA2] and where the certificate demonstrates compliance with the requirements laid down in an implementing act adopted pursuant to Article 21(5) of this Directive or national law transposing Article 21(1) and (2) of this Directive, competent authorities shall not subject the entity to additional measures pursuant to Article 32(2), point (b), or Article 33(2), point (b), as applicable with regard to the requirements covered by the certificate.

6. A certification pursuant to paragraph 4 shall not affect the responsibility of the essential or important entity to comply with this Directive.

**** Regulation (EU) XXX/XXX [Proposal for CSA2]';

(10) Article 26 is amended as follows:

(a) in paragraph 1, the following point (d) is added:

'(d) air carriers, which shall be considered to fall under the jurisdiction of the Member State whose competent licensing authority granted the operating licence to the entity pursuant to Regulation (EC) No 1008/2008 of the European Parliament and of the Council*****, or, where the operating licence or equivalent has not been granted in accordance with that Regulation, they shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2.

***** Regulation (EC) No 1008/2008 of the European Parliament and of the Council of 24 September 2008 on common rules for the operation of air services in the Community (Recast) (OJ L 293, 31.10.2008, p. 3, ELI: http://data.europa.eu/eli/reg/2008/1008/oj)';

(b) paragraph 3 is replaced by the following:

'3. If an essential or important entity is not established in the Union but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established. Where such an entity is an entity as referred to in paragraph 1, point (a), it shall be considered to fall under the jurisdiction of the Member State in which it provides its services. In the absence of a representative in the Union designated under this paragraph, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Directive.';

(11) Article 27 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. ENISA shall create and maintain a registry of essential and important entities as well as entities providing domain name registration services, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to information concerning DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms and air carriers stored in that registry, while ensuring that the confidentiality of information is protected where applicable.';

(b) paragraph 2 is deleted;

(c) paragraphs 3, 4 and 5 are replaced by the following:

‘3. Member States shall ensure that the essential and important entities notify the competent authority about any changes to the information they submitted under Article 3(4) without delay and in any event within two weeks of the date of the change.

4. Upon receipt of the information referred to in Article 3(4), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.

5. Where applicable, the information referred to in Article 3(4), first subparagraph, shall be submitted through the national mechanism referred to in Article 3(4), fourth subparagraph.’;

(12) the following Article 37a is inserted:

‘Article 37a

ENISA’s role in mutual assistance

1. ENISA shall assist Member States in carrying out mutual assistance within the meaning of Article 37 and help facilitate such cooperation processes for essential and important entities that provide services in more than one Member State or that provide services in one or more Member States and have their network and information systems located in one or more other Member States.

2. For the purposes set out in paragraph 1, by … [15 months after the entry into force of this Regulation], ENISA shall conduct a comprehensive analysis of cross-border cybersecurity risks relating to essential and important entities that provide services in more than one Member State or that provide services in one or more Member States and have their network and information systems located in one or more other Member States. The analysis shall evaluate the extent of possible cross-border and internal market consequences of incidents affecting such essential and important entities. For the purpose of this analysis, ENISA shall, in cooperation with the Commission and the Cooperation Group, develop a methodology. Based on the analysis, ENISA shall draw up a comprehensive cross-border cybersecurity risk assessment report, which shall be updated annually.

3. Based on the comprehensive cross-border cybersecurity risk assessment report, ENISA shall:

(a) where appropriate, recommend the relevant competent authorities to set up joint examination teams to support the supervision of specific entities;

(b) develop guidelines for joint supervisory actions;

(c) at the request of the competent authorities of the Member States concerned, establish practical arrangements for the execution of joint supervisory actions;

(d) at the request of the competent authorities of the Member States concerned and subject and proportionate to its own resources, participate in joint supervisory actions;

(e) at the request of the competent authorities of the Member States concerned, assist in the assessment of an essential or an important entity’s level of implementation of the cybersecurity risk-management measures laid down in Article 21.

4. For the purpose of paragraph 3, point (e), of this Article the competent authorities of the Member States concerned shall, where available, provide to ENISA a list of cybersecurity-risk management measures taken by the essential or important entity in accordance with Article 21, a list of supervisory or enforcement actions carried out, as well as the relevant documentation including evidence of implementation of cybersecurity policies, such as the results of security audits, that the competent authorities have undertaken pursuant to Articles 32 and 33 in respect of that entity.

5. Where a Member State receives mutual assistance as referred to in Article 37(1), first subparagraph, point (c), the single point of contact shall inform ENISA that mutual assistance took place. Where applicable, the single point of contact shall state which cross-border incident as referred to in Article 23(6) was connected to the case of mutual assistance.'

(13) Annexes I and II are amended in accordance with the Annex to this Directive.

Article 2
Transposition

1. By … [12 months after entry into force of this Directive], Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

   They shall apply those measures from … [one day after the date referred to in the first subparagraph].

2. When Member States adopt the measures referred to in paragraph 1, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

Article 3
Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 4
Addressees

This Directive is addressed to the Member States.

Done at Strasbourg,

For the European Parliament	*For the Council*
The President	*The President*
[...]	*[...]*