►B 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)

(Text with EEA relevance)

(OJ L 333, 27.12.2022, p. 80)

Corrected by:

►C1 Corrigendum, OJ L 90206, 22.12.2023, p. 1 (2022/2555)

▼B

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)

(Text with EEA relevance)

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. 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.

2. To that end, this Directive lays down:

(a) 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);

(b) cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557;

(c) rules and obligations on cybersecurity information sharing;

(d) supervisory and enforcement obligations on Member States.

Article 2

Scope

1. This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union.

▼B

Article 3(4) of the Annex to that Recommendation shall not apply for the purposes of this Directive.

2. Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where:

(a) services are provided by:

(i) providers of public electronic communications networks or of publicly available electronic communications services;

(ii) trust service providers;

(iii) top-level domain name registries and domain name system service providers;

(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;

(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;

(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;

(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;

(f) the entity is a public administration entity:

(i) of central government as defined by a Member State in accordance with national law; or

(ii) at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.

3. Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557.

▼B

4. Regardless of their size, this Directive applies to entities providing domain name registration services.

5. Member States may provide for this Directive to apply to:

(a) public administration entities at local level;

(b) education institutions, in particular where they carry out critical research activities.

6. This Directive is without prejudice to the Member States' responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.

7. This Directive does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.

8. Member States may exempt specific entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 7 of this Article, from the obligations laid down in Article 21 or 23 with regard to those activities or services. In such cases, the supervisory and enforcement measures referred to in Chapter VII shall not apply in relation to those specific activities or services. Where the entities carry out activities or provide services exclusively of the type referred to in this paragraph, Member States may decide also to exempt those entities from the obligations laid down in Articles 3 and 27.

9. Paragraphs 7 and 8 shall not apply where an entity acts as a trust service provider.

10. This Directive does not apply to entities which Member States have exempted from the scope of Regulation (EU) 2022/2554 in accordance with Article 2(4) of that Regulation.

11. The obligations laid down in this Directive shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.

12. This Directive applies without prejudice to Regulation (EU) 2016/679, Directive 2002/58/EC, Directives 2011/93/EU ([1]) and 2013/40/EU ([2]) of the European Parliament and of the Council and Directive (EU) 2022/2557.

([1]) Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

([2]) Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

▼B

13. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities in accordance with this Directive only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of entities concerned.

14. Entities, the competent authorities, the single points of contact and the CSIRTs shall process personal data to the extent necessary for the purposes of this Directive and in accordance with Regulation (EU) 2016/679, in particular such processing shall rely on Article 6 thereof.

The processing of personal data pursuant to this Directive by providers of public electronic communications networks or providers of publicly available electronic communications services shall be carried out in accordance with Union data protection law and Union privacy law, in particular Directive 2002/58/EC.

Article 3

Essential and important entities

1. For the purposes of this Directive, the following entities shall be considered to be essential entities:

(a) entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC;

(b) qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size;

(c) providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC;

(d) public administration entities referred to in Article 2(2), point (f)(i);

(e) any other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities pursuant to Article 2(2), points (b) to (e);

(f) entities identified as critical entities under Directive (EU) 2022/2557, referred to in Article 2(3) of this Directive;

(g) if the Member State so provides, entities which that Member State identified before 16 January 2023 as operators of essential services in accordance with Directive (EU) 2016/1148 or national law.

▼B

2. For the purposes of this Directive, entities of a type referred to in Annex I or II which do not qualify as essential entities pursuant to paragraph 1 of this Article shall be considered to be important entities. This includes entities identified by Member States as important entities pursuant to Article 2(2), points (b) to (e).

3. By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services. Member States shall review and, where appropriate, update that list on a regular basis and at least every two years thereafter.

4. 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 address and up-to-date contact details, including email addresses, IP ranges and telephone numbers;

(c) where applicable, the relevant sector and subsector referred to in Annex I or II; and

(d) where applicable, a list of the Member States where they provide services falling within the scope of this Directive.

The entities referred to in paragraph 3 shall notify any changes to the details submitted pursuant to the first subparagraph of this paragraph without delay, and, in any event, within two weeks of the date of the change.

The Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA), shall without undue delay provide guidelines and templates regarding the obligations laid down in this paragraph.

Member States may establish national mechanisms for entities to register themselves.

5. By 17 April 2025 and every two years thereafter, the competent authorities shall notify:

(a) the Commission and the Cooperation Group of the number of essential and important entities listed pursuant to paragraph 3 for each sector and subsector referred to in Annex I or II; and

(b) the Commission of relevant information about the number of essential and important entities identified pursuant to Article 2(2), points (b) to (e), the sector and subsector referred to in Annex I or II to which they belong, the type of service that they provide, and the provision, from among those laid down in Article 2(2), points (b) to (e), pursuant to which they were identified.

▼B

6. Until 17 April 2025 and upon request of the Commission, Member States may notify the Commission of the names of the essential and important entities referred to in paragraph 5, point (b).

Article 4

Sector-specific Union legal acts

1. Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities. Where sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive shall continue to apply to the entities not covered by those sector-specific Union legal acts.

2. The requirements referred to in paragraph 1 of this Article shall be considered to be equivalent in effect to the obligations laid down in this Directive where:

(a) cybersecurity risk-management measures are at least equivalent in effect to those laid down in Article 21(1) and (2); or

(b) the sector-specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the CSIRTs, the competent authorities or the single points of contact under this Directive and where requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 23(1) to (6) of this Directive.

3. The Commission shall, by 17 July 2023, provide guidelines clarifying the application of paragraphs 1 and 2. The Commission shall review those guidelines on a regular basis. When preparing those guidelines, the Commission shall take into account any observations of the Cooperation Group and ENISA.

Article 5

Minimum harmonisation

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.

Article 6

Definitions

For the purposes of this Directive, the following definitions apply:

▼B

(1) ‘network and information system’ means:

(a) an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972;

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

(2) ‘security of network and information systems’ means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems;

(3) ‘cybersecurity’ means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;

(4) ‘national cybersecurity strategy ’ means a coherent framework of a Member State providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them in that Member State;

(5) ‘near miss’ means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise;

(6) ‘incident’ means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;

(7) ‘large-scale cybersecurity incident’ means an incident which causes a level of disruption that exceeds a Member State’s capacity to respond to it or which has a significant impact on at least two Member States;

(8) ‘incident handling’ means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident;

▼B

(9) ‘risk’ means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

(10) ‘cyber threat’ means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(11) ‘significant cyber threat’ means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity’s services by causing considerable material or non-material damage;

(12) ‘ICT product’ means an ICT product as defined in Article 2, point (12), of Regulation (EU) 2019/881;

(13) ‘ICT service’ means an ICT service as defined in Article 2, point (13), of Regulation (EU) 2019/881;

(14) ‘ICT process’ means an ICT process as defined in Article 2, point (14), of Regulation (EU) 2019/881;

(15) ‘vulnerability’ means a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat;

(16) ‘standard’ means a standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council ([3]);

(17) ‘technical specification’ means a technical specification as defined in Article 2, point (4), of Regulation (EU) No 1025/2012;

(18) ‘internet exchange point’ means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;

(19) ‘domain name system’ or ‘DNS’ means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources;

([3]) Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

▼B

(20) ‘DNS service provider’ means an entity that provides:

(a) publicly available recursive domain name resolution services for internet end-users; or

(b) authoritative domain name resolution services for third-party use, with the exception of root name servers;

(21) ‘top-level domain name registry’ or ‘TLD name registry’ means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use;

(22) ‘entity providing domain name registration services’ means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller;

(23) ‘digital service’ means a service as defined in Article 1(1), point (b), of Directive (EU) 2015/1535 of the European Parliament and of the Council ([4]);

(24) ‘trust service’ means a trust service as defined in Article 3, point (16), of Regulation (EU) No 910/2014;

(25) ‘trust service provider’ means a trust service provider as defined in Article 3, point (19), of Regulation (EU) No 910/2014;

(26) ‘qualified trust service’ means a qualified trust service as defined in Article 3, point (17), of Regulation (EU) No 910/2014;

(27) ‘qualified trust service provider’ means a qualified trust service provider as defined in Article 3, point (20), of Regulation (EU) No 910/2014;

(28) ‘online marketplace’ means an online marketplace as defined in Article 2, point (n), of Directive 2005/29/EC of the European Parliament and of the Council ([5]);

(29) ‘online search engine’ means an online search engine as defined in Article 2, point (5), of Regulation (EU) 2019/1150 of the European Parliament and of the Council ([6]);

([4]) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

([5]) Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’) (OJ L 149, 11.6.2005, p. 22).

([6]) Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57).

▼B

(30) ‘cloud computing service’ means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;

(31) ‘data centre service’ means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;

(32) ‘content delivery network’ means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;

(33) ‘social networking services platform’ means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations;

(34) ‘representative’ means a natural or legal person established in the Union explicitly designated to act on behalf of a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, or a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the Union, which may be addressed by a competent authority or a CSIRT in the place of the entity itself with regard to the obligations of that entity under this Directive;

(35) ‘public administration entity’ means an entity recognised as such in a Member State in accordance with national law, not including the judiciary, parliaments or central banks, which complies with the following criteria:

(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

(b) it has legal personality or is entitled by law to act on behalf of another entity with legal personality;

(c) it is financed, for the most part, by the State, regional authorities or by other bodies governed by public law, is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities or by other bodies governed by public law;

(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital;

▼B

(36) ‘public electronic communications network’ means a public electronic communications network as defined in Article 2, point (8), of Directive (EU) 2018/1972;

(37) ‘electronic communications service’ means an electronic communications service as defined in Article 2, point (4), of Directive (EU) 2018/1972;

(38) ‘entity’ means a natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;

(39) ‘managed service provider’ means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers’ premises or remotely;

(40) ‘managed security service provider’ means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management;

(41) ‘research organisation’ means an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions.

CHAPTER II

COORDINATED CYBERSECURITY FRAMEWORKS

Article 7

National cybersecurity strategy

1. Each Member State shall adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include:

(a) objectives and priorities of the Member State’s cybersecurity strategy covering in particular the sectors referred to in Annexes I and II;

(b) a governance framework to achieve the objectives and priorities referred to in point (a) of this paragraph, including the policies referred to in paragraph 2;

(c) a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single points of contact, and the CSIRTs under this Directive, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts;

▼B

(d) a mechanism to identify relevant assets and an assessment of the risks in that Member State;

(e) an identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors;

(f) a list of the various authorities and stakeholders involved in the implementation of the national cybersecurity strategy;

(g) a policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2557 for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate;

(h) a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens.

2. As part of the national cybersecurity strategy, Member States shall in particular adopt policies:

(a) addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services;

(b) on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products;

(c) managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Article 12(1);

(d) related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables;

(e) promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures;

(f) promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities;

(g) supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure;

▼B

(h) including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law;

(i) strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs;

(j) promoting active cyber protection.

3. Member States shall notify their national cybersecurity strategies to the Commission within three months of their adoption. Member States may exclude information which relates to their national security from such notifications.

4. Member States shall assess their national cybersecurity strategies on a regular basis and at least every five years on the basis of key performance indicators and, where necessary, update them. ENISA shall assist Member States, upon their request, in the development or the update of a national cybersecurity strategy and of key performance indicators for the assessment of that strategy, in order to align it with the requirements and obligations laid down in this Directive.

Article 8

Competent authorities and single points of contact

1. Each Member State shall designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VII (competent authorities).

2. The competent authorities referred to in paragraph 1 shall monitor the implementation of this Directive at national level.

3. Each Member State shall designate or establish a single point of contact. Where a Member State designates or establishes only one competent authority pursuant to paragraph 1, that competent authority shall also be the single point of contact for that Member State.

4. Each single point of contact shall exercise a liaison function to ensure cross-border cooperation of its Member State's authorities with the relevant authorities of other Member States, and, where appropriate, with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities within its Member State.

5. Member States shall ensure that their competent authorities and single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive.

6. Each Member State shall notify the Commission without undue delay of the identity of the competent authority referred to in paragraph 1 and of the single point of contact referred to in paragraph 3, of the tasks of those authorities, and of any subsequent changes thereto. Each Member State shall make public the identity of its competent authority. The Commission shall make a list of the single points of contact publicly available.

▼B

Article 9

National cyber crisis management frameworks

1. Each Member State shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities). Member States shall ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general national crisis management.

2. Where a Member State designates or establishes more than one cyber crisis management authority pursuant to paragraph 1, it shall clearly indicate which of those authorities is to serve as the coordinator for the management of large-scale cybersecurity incidents and crises.

3. Each Member State shall identify capabilities, assets and procedures that can be deployed in the case of a crisis for the purposes of this Directive.

4. Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular:

(a) the objectives of national preparedness measures and activities;

(b) the tasks and responsibilities of the cyber crisis management authorities;

(c) the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels;

(d) national preparedness measures, including exercises and training activities;

(e) the relevant public and private stakeholders and infrastructure involved;

(f) national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.

5. Within three months of the designation or establishment of the cyber crisis management authority referred to in paragraph 1, each Member State shall notify the Commission of the identity of its authority and of any subsequent changes thereto. Member States shall submit to the Commission and to the European cyber crisis liaison organisation network (EU-CyCLONe) relevant information relating to the requirements of paragraph 4 about their national large-scale cybersecurity incident and crisis response plans within three months of the adoption of those plans. Member States may exclude information where and to the extent that such exclusion is necessary for their national security.

▼B

Article 10

Computer security incident response teams (CSIRTs)

1. Each Member State shall designate or establish one or more CSIRTs. The CSIRTs may be designated or established within a competent authority. The CSIRTs shall comply with the requirements set out in Article 11(1), shall cover at least the sectors, subsectors and types of entity referred to in Annexes I and II, and shall be responsible for incident handling in accordance with a well-defined process.

2. Member States shall ensure that each CSIRT has adequate resources to carry out effectively its tasks as set out in Article 11(3).

3. Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders. To that end, Member States shall ensure that each CSIRT contributes to the deployment of secure information-sharing tools.

4. The CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 29 with sectoral or cross-sectoral communities of essential and important entities.

5. The CSIRTs shall participate in peer reviews organised in accordance with Article 19.

6. Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network.

7. The CSIRTs may establish cooperation relationships with third countries' national computer security incident response teams. As part of such cooperation relationships, Member States shall facilitate effective, efficient and secure information exchange with those third countries' national computer security incident response teams, using relevant information-sharing protocols, including the traffic light protocol. The CSIRTs may exchange relevant information with third countries' national computer security incident response teams, including personal data in accordance with Union data protection law.

8. The CSIRTs may cooperate with third countries' national computer security incident response teams or equivalent third-country bodies, in particular for the purpose of providing them with cybersecurity assistance.

9. Each Member State shall notify the Commission without undue delay of the identity of the CSIRT referred to in paragraph 1 of this Article and the CSIRT designated as coordinator pursuant to Article 12(1), of their respective tasks in relation to essential and important entities, and of any subsequent changes thereto.

10. Member States may request the assistance of ENISA in developing their CSIRTs.

▼B

Article 11

Requirements, technical capabilities and tasks of CSIRTs

1. The CSIRTs shall comply with the following requirements:

(a) the CSIRTs shall ensure a high level of availability of their communication channels by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times; they shall clearly specify the communication channels and make them known to constituency and cooperative partners;

(b) the CSIRTs' premises and the supporting information systems shall be located at secure sites;

(c) the CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular to facilitate effective and efficient handovers;

(d) the CSIRTs shall ensure the confidentiality and trustworthiness of their operations;

(e) the CSIRTs shall be adequately staffed to ensure availability of their services at all times and they shall ensure that their staff is trained appropriately;

(f) the CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of their services.

The CSIRTs may participate in international cooperation networks.

2. Member States shall ensure that their CSIRTs jointly have the technical capabilities necessary to carry out the tasks referred to in paragraph 3. Member States shall ensure that sufficient resources are allocated to their CSIRTs to ensure adequate staffing levels for the purpose of enabling the CSIRTs to develop their technical capabilities.

3. The CSIRTs shall have the following tasks:

(a) monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;

(b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;

(c) responding to incidents and providing assistance to the essential and important entities concerned, where applicable;

▼B

(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;

(e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;

(f) participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;

(g) where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1);

(h) contributing to the deployment of secure information-sharing tools pursuant to Article 10(3).

The CSIRTs may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential and important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned. Such scanning shall not have any negative impact on the functioning of the entities' services.

When carrying out the tasks referred to in the first subparagraph, the CSIRTs may prioritise particular tasks on the basis of a risk-based approach.

4. The CSIRTs shall establish cooperation relationships with relevant stakeholders in the private sector, with a view to achieving the objectives of this Directive.

5. In order to facilitate cooperation referred to in paragraph 4, the CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to:

(a) incident-handling procedures;

(b) crisis management; and

(c) coordinated vulnerability disclosure under Article 12(1).

Article 12

Coordinated vulnerability disclosure and a European vulnerability database

1. Each Member State shall designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure. The CSIRT designated as coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party. The tasks of the CSIRT designated as coordinator shall include:

▼B

(a) identifying and contacting the entities concerned;

(b) assisting the natural or legal persons reporting a vulnerability; and

(c) negotiating disclosure timelines and managing vulnerabilities that affect multiple entities.

Member States shall ensure that natural or legal persons are able to report, anonymously where they so request, a vulnerability to the CSIRT designated as coordinator. The CSIRT designated as coordinator shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT designated as coordinator of each Member State concerned shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.

2. ENISA shall develop and maintain, after consulting the Cooperation Group, a European vulnerability database. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the European vulnerability database, with a view in particular to enabling entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services. All stakeholders shall be provided access to the information about the vulnerabilities contained in the European vulnerability database. That database shall include:

(a) information describing the vulnerability;

(b) the affected ICT products or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited;

(c) the availability of related patches and, in the absence of available patches, guidance provided by the competent authorities or the CSIRTs addressed to users of vulnerable ICT products and ICT services as to how the risks resulting from disclosed vulnerabilities can be mitigated.

Article 13

Cooperation at national level

1. Where they are separate, the competent authorities, the single point of contact and the CSIRTs of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.

▼B

2. Member States shall ensure that their CSIRTs or, where applicable, their competent authorities, receive notifications of significant incidents pursuant to Article 23, and incidents, cyber threats and near misses pursuant to Article 30.

3. Member States shall ensure that their CSIRTs or, where applicable, their competent authorities inform their single points of contact of notifications of incidents, cyber threats and near misses submitted pursuant to this Directive.

4. In order to ensure that the tasks and obligations of the competent authorities, the single points of contact and the CSIRTs are carried out effectively, Member States shall, to the extent possible, ensure appropriate cooperation between those bodies and law enforcement authorities, data protection authorities, the national authorities under Regulations (EC) No 300/2008 and (EU) 2018/1139, the supervisory bodies under Regulation (EU) No 910/2014, the competent authorities under Regulation (EU) 2022/2554, the national regulatory authorities under Directive (EU) 2018/1972, the competent authorities under Directive (EU) 2022/2557, as well as the competent authorities under other sector-specific Union legal acts, within that Member State.

5. Member States shall ensure that their competent authorities under this Directive and their competent authorities under Directive (EU) 2022/2557 cooperate and exchange information on a regular basis with regard to the identification of critical entities, on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents affecting entities identified as critical entities under Directive (EU) 2022/2557, and the measures taken in response to such risks, threats and incidents. Member States shall also ensure that their competent authorities under this Directive and their competent authorities under Regulation (EU) No 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2018/1972 exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats.

6. Member States shall simplify the reporting through technical means for notifications referred to in Articles 23 and 30.

CHAPTER III

COOPERATION AT UNION AND INTERNATIONAL LEVEL

Article 14

Cooperation Group

1. In order to support and facilitate strategic cooperation and the exchange of information among Member States, as well as to strengthen trust and confidence, a Cooperation Group is established.

2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 7.

▼B

3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) and the competent authorities under Regulation (EU) 2022/2554 may participate in the activities of the Cooperation Group in accordance with Article 47(1) of that Regulation.

Where appropriate, the Cooperation Group may invite the European Parliament and representatives of relevant stakeholders to participate in its work.

The Commission shall provide the secretariat.

4. The Cooperation Group shall have the following tasks:

(a) to provide guidance to the competent authorities in relation to the transposition and implementation of this Directive;

(b) to provide guidance to the competent authorities in relation to the development and implementation of policies on coordinated vulnerability disclosure, as referred to in Article 7(2), point (c);

(c) to exchange best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, training, exercises and skills, capacity building, standards and technical specifications as well as the identification of essential and important entities pursuant to Article 2(2), points (b) to (e);

(d) to exchange advice and cooperate with the Commission on emerging cybersecurity policy initiatives and the overall consistency of sector-specific cybersecurity requirements;

(e) to exchange advice and cooperate with the Commission on draft delegated or implementing acts adopted pursuant to this Directive;

(f) to exchange best practices and information with relevant Union institutions, bodies, offices and agencies;

(g) to exchange views on the implementation of sector-specific Union legal acts that contain provisions on cybersecurity;

(h) where relevant, to discuss reports on the peer review referred to in Article 19(9) and draw up conclusions and recommendations;

(i) to carry out coordinated security risk assessments of critical supply chains in accordance with Article 22(1);

▼B

(j) to discuss cases of mutual assistance, including experiences and results from cross-border joint supervisory actions as referred to in Article 37;

(k) upon the request of one or more Member States concerned, to discuss specific requests for mutual assistance as referred to in Article 37;

(l) to provide strategic guidance to the CSIRTs network and EU-CyCLONe on specific emerging issues;

(m) to exchange views on the policy on follow-up actions following large-scale cybersecurity incidents and crises on the basis of lessons learned of the CSIRTs network and EU-CyCLONe;

(n) to contribute to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the competent authorities or the CSIRTs;

(o) to organise regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Cooperation Group and gather input on emerging policy challenges;

(p) to discuss the work undertaken in relation to cybersecurity exercises, including the work done by ENISA;

(q) to establish the methodology and organisational aspects of the peer reviews referred to in Article 19(1), as well as to lay down the self-assessment methodology for Member States in accordance with Article 19(5), with the assistance of the Commission and ENISA, and, in cooperation with the Commission and ENISA, to develop codes of conduct underpinning the working methods of designated cybersecurity experts in accordance with Article 19(6);

(r) to prepare reports for the purpose of the review referred to in Article 40 on the experience gained at a strategic level and from peer reviews;

(s) to discuss and carry out on a regular basis an assessment of the state of play of cyber threats or incidents, such as ransomware.

The Cooperation Group shall submit the reports referred to in the first subparagraph, point (r), to the Commission, to the European Parliament and to the Council.

5. Member States shall ensure effective, efficient and secure cooperation of their representatives in the Cooperation Group.

6. The Cooperation Group may request from the CSIRTs network a technical report on selected topics.

7. By 1 February 2024 and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks.

▼B

8. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first subparagraph of this paragraph in accordance with paragraph (4), point (e).

9. The Cooperation Group shall meet on a regular basis and in any event at least once a year with the Critical Entities Resilience Group established under Directive (EU) 2022/2557 to promote and facilitate strategic cooperation and the exchange of information.

Article 15

CSIRTs network

1. In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of national CSIRTs is established.

2. The CSIRTs network shall be composed of representatives of the CSIRTs designated or established pursuant to Article 10 and the computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU). The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively provide assistance for the cooperation among the CSIRTs.

3. The CSIRTs network shall have the following tasks:

(a) to exchange information about the CSIRTs' capabilities;

(b) to facilitate the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs;

(c) to exchange relevant information about incidents, near misses, cyber threats, risks and vulnerabilities;

(d) to exchange information with regard to cybersecurity publications and recommendations;

(e) to ensure interoperability with regard to information-sharing specifications and protocols;

(f) at the request of a member of the CSIRTs network potentially affected by an incident, to exchange and discuss information in relation to that incident and associated cyber threats, risks and vulnerabilities;

(g) at the request of a member of the CSIRTs network, to discuss and, where possible, implement a coordinated response to an incident that has been identified within the jurisdiction of that Member State;

▼B

(h) to provide Member States with assistance in addressing cross-border incidents pursuant to this Directive;

(i) to cooperate, exchange best practices and provide assistance to the CSIRTs designated as coordinators pursuant to Article 12(1) with regard to the management of the coordinated disclosure of vulnerabilities which could have a significant impact on entities in more than one Member State;

(j) to discuss and identify further forms of operational cooperation, including in relation to:

(i) categories of cyber threats and incidents;

(ii) early warnings;

(iii) mutual assistance;

(iv) principles and arrangements for coordination in response to cross-border risks and incidents;

(v) contribution to the national large-scale cybersecurity incident and crisis response plan referred to in Article 9(4) at the request of a Member State;

(k) to inform the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (j), and, where necessary, request guidance in that regard;

(l) to take stock of cybersecurity exercises, including those organised by ENISA;

(m) at the request of an individual CSIRT, to discuss the capabilities and preparedness of that CSIRT;

(n) to cooperate and exchange information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and cyber threats across the Union;

(o) where relevant, to discuss the peer-review reports referred to in Article 19(9);

(p) to provide guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.

4. By 17 January 2025, and every two years thereafter, the CSIRTs network shall, for the purpose of the review referred to in Article 40, assess the progress made with regard to the operational cooperation and adopt a report. The report shall, in particular, draw up conclusions and recommendations on the basis of the outcome of the peer reviews referred to in Article 19, which are carried out in relation to the national CSIRTs. That report shall be submitted to the Cooperation Group.

5. The CSIRTs network shall adopt its rules of procedure.

6. The CSIRTs network and EU-CyCLONe shall agree on procedural arrangements and cooperate on the basis thereof.

▼B

Article 16

European cyber crisis liaison organisation network (EU-CyCLONe)

1. EU-CyCLONe is established to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies.

2. EU-CyCLONe shall be composed of the representatives of Member States' cyber crisis management authorities as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on services and activities falling within the scope of this Directive, the Commission. In other cases, the Commission shall participate in the activities of EU-CyCLONe as an observer.

ENISA shall provide the secretariat of EU-CyCLONe and support the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information.

Where appropriate, EU-CyCLONe may invite representatives of relevant stakeholders to participate in its work as observers.

3. EU-CyCLONe shall have the following tasks:

(a) to increase the level of preparedness of the management of large-scale cybersecurity incidents and crises;

(b) to develop a shared situational awareness for large-scale cybersecurity incidents and crises;

(c) to assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures;

(d) to coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises;

(e) to discuss, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans referred to in Article 9(4).

4. EU-CyCLONe shall adopt its rules of procedure.

5. EU-CyCLONe shall report on a regular basis to the Cooperation Group on the management of large-scale cybersecurity incidents and crises, as well as trends, focusing in particular on their impact on essential and important entities.

▼B

6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements provided for in Article 15(6).

7. By 17 July 2024 and every 18 months thereafter, EU-CyCLONe shall submit to the European Parliament and to the Council a report assessing its work.

Article 17

International cooperation

The Union may, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in particular activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements shall comply with Union data protection law.

Article 18

Report on the state of cybersecurity in the Union

1. ENISA shall adopt, in cooperation with the Commission and the Cooperation Group, a biennial report on the state of cybersecurity in the Union and shall submit and present that report to the European Parliament. The report shall, inter alia, be made available in machine-readable data and include the following:

(a) a Union-level cybersecurity risk assessment, taking account of the cyber threat landscape;

(b) an assessment of the development of cybersecurity capabilities in the public and private sectors across the Union;

(c) an assessment of the general level of cybersecurity awareness and cyber hygiene among citizens and entities, including small and medium-sized enterprises;

(d) an aggregated assessment of the outcome of the peer reviews referred to in Article 19;

(e) an aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union, including those at sector level, as well as of the extent to which the Member States' national cybersecurity strategies are aligned.

2. The report shall include particular policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union, and a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.

3. ENISA, in cooperation with the Commission, the Cooperation Group and the CSIRTs network, shall develop the methodology, including the relevant variables, such as quantitative and qualitative indicators, of the aggregated assessment referred to in paragraph 1, point (e).

▼B

Article 19

Peer reviews

1. ►C1 The Cooperation Group shall, by 17 January 2025, establish, with the assistance ◄ of the Commission and ENISA, and, where relevant, the CSIRTs network, the methodology and organisational aspects of peer reviews with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing Member States' cybersecurity capabilities and policies necessary to implement this Directive. Participation in peer reviews is voluntary. The peer reviews shall be carried out by cybersecurity experts. The cybersecurity experts shall be designated by at least two Member States, different from the Member State being reviewed.

The peer reviews shall cover at least one of the following:

(a) the level of implementation of the cybersecurity risk-management measures and reporting obligations laid down in Articles 21 and 23;

(b) the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the competent authorities;

(c) the operational capabilities of the CSIRTs;

(d) the level of implementation of mutual assistance referred to in Article 37;

(e) the level of implementation of the cybersecurity information-sharing arrangements referred to in Article 29;

(f) specific issues of cross-border or cross-sector nature.

2. The methodology referred to in paragraph 1 shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States designate cybersecurity experts eligible to carry out the peer reviews. The Commission and ENISA shall participate as observers in the peer reviews.

3. Member States may identify specific issues as referred to in paragraph 1, point (f), for the purposes of a peer review.

4. Before commencing a peer review as referred to in paragraph 1, Member States shall notify the participating Member States of its scope, including the specific issues identified pursuant to paragraph 3.

5. Prior to the commencement of the peer review, Member States may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated cybersecurity experts. The Cooperation Group shall, with the assistance of the Commission and ENISA, lay down the methodology for the Member States' self-assessment.

▼B

6. Peer reviews shall entail physical or virtual on-site visits and off-site exchanges of information. In line with the principle of good cooperation, the Member State subject to the peer review shall provide the designated cybersecurity experts with the information necessary for the assessment, without prejudice to Union or national law concerning the protection of confidential or classified information and to the safeguarding of essential State functions, such as national security. The Cooperation Group, in cooperation with the Commission and ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated cybersecurity experts. Any information obtained through the peer review shall be used solely for that purpose. The cybersecurity experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that peer review to any third parties.

7. Once subject to a peer review, the same aspects reviewed in a Member State shall not be subject to a further peer review in that Member State for two years following the conclusion of the peer review, unless otherwise requested by the Member State or agreed upon after a proposal of the Cooperation Group.

8. Member States shall ensure that any risk of conflict of interest concerning the designated cybersecurity experts is revealed to the other Member States, the Cooperation Group, the Commission and ENISA, before the commencement of the peer review. The Member State subject to the peer review may object to the designation of particular cybersecurity experts on duly substantiated grounds communicated to the designating Member State.

9. Cybersecurity experts participating in peer reviews shall draft reports on the findings and conclusions of the peer reviews. Member States subject to a peer review may provide comments on the draft reports concerning them and such comments shall be attached to the reports. The reports shall include recommendations to enable improvement on the aspects covered by the peer review. The reports shall be submitted to the Cooperation Group and the CSIRTs network where relevant. A Member State subject to the peer review may decide to make its report, or a redacted version of it, publicly available.

CHAPTER IV

CYBERSECURITY RISK-MANAGEMENT MEASURES AND REPORTING OBLIGATIONS

Article 20

Governance

1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.

▼B

2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

▼B

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

4. Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.

5. By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures referred to in paragraph 2 with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

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.

When preparing the implementing acts referred to in the first and second subparagraphs of this paragraph, the Commission shall, to the extent possible, follow European and international standards, as well as relevant technical specifications. The Commission shall exchange advice and cooperate with the Cooperation Group and ENISA on the draft implementing acts in accordance with Article 14(4), point (e).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

Article 22

Union level coordinated security risk assessments of critical supply chains

1. The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors.

▼B

2. The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated security risk assessment referred to in paragraph 1.

Article 23

Reporting obligations

1. Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability.

Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt.

In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.

2. Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.

3. An incident shall be considered to be significant if:

(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;

(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:

(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

▼B

(b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

(c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;

(d) a final report not later than one month after the submission of the incident notification under point (b), including the following:

(i) a detailed description of the incident, including its severity and impact;

(ii) the type of threat or root cause that is likely to have triggered the incident;

(iii) applied and ongoing mitigation measures;

(iv) where applicable, the cross-border impact of the incident;

(e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident.

5. The CSIRT or the competent authority shall provide, without undue delay and where possible within 24 hours of receiving the early warning referred to in paragraph 4, point (a), a response to the notifying entity, including initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures. Where the CSIRT is not the initial recipient of the notification referred to in paragraph 1, the guidance shall be provided by the competent authority in cooperation with the CSIRT. The CSIRT shall provide additional technical support if the entity concerned so requests. Where the significant incident is suspected to be of criminal nature, the CSIRT or the competent authority shall also provide guidance on reporting the significant incident to law enforcement authorities.

6. Where appropriate, and in particular where the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and ENISA of the significant incident. Such information shall include the type of information received in accordance with paragraph 4. In so doing, the CSIRT, the competent authority or the single point of contact shall, in accordance with Union or national law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

▼B

7. Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, a Member State's CSIRT or, where applicable, its competent authority, and, where appropriate, the CSIRTs or the competent authorities of other Member States concerned, may, after consulting the entity concerned, inform the public about the significant incident or require the entity to do so.

8. At the request of the CSIRT or the competent authority, the single point of contact shall forward notifications received pursuant to paragraph 1 to the single points of contact of other affected Member States.

9. The single point of contact shall submit to ENISA every three months a summary report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30. In order to contribute to the provision of comparable information, ENISA may adopt technical guidance on the parameters of the information to be included in the summary report. ENISA shall inform the Cooperation Group and the CSIRTs network about its findings on notifications received every six months.

10. The CSIRTs or, where applicable, the competent authorities shall provide to the competent authorities under Directive (EU) 2022/2557 information about significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30 by entities identified as critical entities under Directive (EU) 2022/2557.

11. The Commission may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraph 1 of this Article and to Article 30 and of a communication submitted pursuant to paragraph 2 of this Article.

By 17 October 2024, the Commission shall, with regard to DNS service providers, TLD name registries, 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, adopt implementing acts further specifying the cases in which an incident shall be considered to be significant as referred to in paragraph 3. The Commission may adopt such implementing acts with regard to other essential and important entities.

The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first and second subparagraphs of this paragraph in accordance with Article 14(4), point (e).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

▼B

Article 24

Use of European cybersecurity certification schemes

1. In order to demonstrate compliance with particular requirements of Article 21, Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. Furthermore, Member States shall encourage essential and important entities to use qualified trust services.

2. The Commission is empowered to adopt delegated acts, in accordance with Article 38, to supplement this Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881. Those delegated acts shall be adopted where insufficient levels of cybersecurity have been identified and shall include an implementation period.

Before adopting such delegated acts, the Commission shall carry out an impact assessment and shall carry out consultations in accordance with Article 56 of Regulation (EU) 2019/881.

3. Where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 of this Article is available, the Commission may, after consulting the Cooperation Group and the European Cybersecurity Certification Group, request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881.

Article 25

Standardisation

1. In order to promote the convergent implementation of Article 21(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems.

2. ENISA, in cooperation with Member States, and, where appropriate, after consulting relevant stakeholders, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered.

CHAPTER V

JURISDICTION AND REGISTRATION

Article 26

Jurisdiction and territoriality

1. Entities falling within the scope of this Directive shall be considered to fall under the jurisdiction of the Member State in which they are established, except in the case of:

▼B

(a) providers of public electronic communications networks or providers of publicly available electronic communications services, which shall be considered to fall under the jurisdiction of the Member State in which they provide their services;

(b) 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 or of social networking services platforms, which 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;

(c) public administration entities, which shall be considered to fall under the jurisdiction of the Member State which established them.

2. For the purposes of this Directive, an entity as referred to in paragraph 1, point (b), shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union.

3. If an entity as referred to in paragraph 1, point (b), 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. 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.

4. The designation of a representative by an entity as referred to in paragraph 1, point (b), shall be without prejudice to legal actions, which could be initiated against the entity itself.

5. Member States that have received a request for mutual assistance in relation to an entity as referred to in paragraph 1, point (b), may, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has a network and information system on their territory.

Article 27

Registry of entities

1. ENISA shall create and maintain a registry of 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

▼B

services platforms, 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 that registry, while ensuring that the confidentiality of information is protected where applicable.

2. Member States shall require entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025:

(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'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 and telephone numbers of the entity and, where applicable, its representative designated pursuant to Article 26(3);

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

(f) the entity's IP ranges.

3. Member States shall ensure that the entities referred to in paragraph 1 notify the competent authority about any changes to the information they submitted under paragraph 2 without delay and in any event within three months of the date of the change.

4. Upon receipt of the information referred to in paragraphs 2 and 3, except for that referred to in paragraph 2, point (f), 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 paragraphs 2 and 3 of this Article shall be submitted through the national mechanism referred to in Article 3(4), fourth subparagraph.

Article 28

Database of domain name registration data

1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall require TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data.

2. For the purposes of paragraph 1, Member States shall require the database of domain name registration data to contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. Such information shall include:

▼B

(a) the domain name;

(b) the date of registration;

(c) the registrant's name, contact email address and telephone number;

(d) the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.

3. Member States shall require the TLD name registries and the entities providing domain name registration services to have policies and procedures, including verification procedures, in place to ensure that the databases referred to in paragraph 1 include accurate and complete information. Member States shall require such policies and procedures to be made publicly available.

4. Member States shall require the TLD name registries and the entities providing domain name registration services to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.

5. Member States shall require the TLD name registries and the entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with Union data protection law. Member States shall require the TLD name registries and the entities providing domain name registration services to reply without undue delay and in any event within 72 hours of receipt of any requests for access. Member States shall require policies and procedures with regard to the disclosure of such data to be made publicly available.

6. Compliance with the obligations laid down in paragraphs 1 to 5 shall not result in a duplication of collecting domain name registration data. To that end, Member States shall require TLD name registries and entities providing domain name registration services to cooperate with each other.

CHAPTER VI

INFORMATION SHARING

Article 29

Cybersecurity information-sharing arrangements

1. Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing:

▼B

(a) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.

2. Member States shall ensure that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers. Such exchange shall be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared.

3. Member States shall facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 of this Article. Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements. In laying down the details of the involvement of public authorities in such arrangements, Member States may impose conditions on the information made available by the competent authorities or the CSIRTs. Member States shall offer assistance for the application of such arrangements in accordance with their policies referred to in Article 7(2), point (h).

4. Member States shall ensure that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.

5. ENISA shall provide assistance for the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance.

Article 30

Voluntary notification of relevant information

1. Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis, by:

(a) essential and important entities with regard to incidents, cyber threats and near misses;

▼B

(b) entities other than those referred to in point (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses.

2. Member States shall process the notifications referred to in paragraph 1 of this Article in accordance with the procedure laid down in Article 23. Member States may prioritise the processing of mandatory notifications over voluntary notifications.

Where necessary, the CSIRTs and, where applicable, the competent authorities shall provide the single points of contact with the information about notifications received pursuant to this Article, while ensuring the confidentiality and appropriate protection of the information provided by the notifying entity. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.

CHAPTER VII

SUPERVISION AND ENFORCEMENT

Article 31

General aspects concerning supervision and enforcement

1. Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive.

2. Member States may allow their competent authorities to prioritise supervisory tasks. Such prioritisation shall be based on a risk-based approach. To that end, when exercising their supervisory tasks provided for in Articles 32 and 33, the competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.

3. The competent authorities shall work in close cooperation with supervisory authorities under Regulation (EU) 2016/679 when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks of the supervisory authorities under that Regulation.

4. Without prejudice to national legislative and institutional frameworks, Member States shall ensure that, in the supervision of compliance of public administration entities with this Directive and the imposition of enforcement measures with regard to infringements of this Directive, the competent authorities have appropriate powers to carry out such tasks with operational independence vis-à-vis the public administration entities supervised. Member States may decide on the imposition of appropriate, proportionate and effective supervisory and enforcement measures in relation to those entities in accordance with the national legislative and institutional frameworks.

▼B

Article 32

Supervisory and enforcement measures in relation to essential entities

1. Member States shall ensure that the supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to:

(a) on-site inspections and off-site supervision, including random checks conducted by trained professionals;

(b) regular and targeted security audits carried out by an independent body or a competent authority;

(c) ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity;

(d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;

(e) requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;

(f) requests to access data, documents and information necessary to carry out their supervisory tasks;

(g) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.

The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.

3. When exercising their powers under paragraph 2, point (e), (f) or (g), the competent authorities shall state the purpose of the request and specify the information requested.

4. Member States shall ensure that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the power at least to:

▼B

(a) issue warnings about infringements of this Directive by the entities concerned;

(b) adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive;

(c) order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;

(d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;

(e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;

(f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g) designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23;

(h) order the entities concerned to make public aspects of infringements of this Directive in a specified manner;

(i) impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph.

5. Where enforcement measures adopted pursuant to paragraph 4, points (a) to (d) and (f), are ineffective, Member States shall ensure that their competent authorities have the power to establish a deadline by which the essential entity is requested to take the necessary action to remedy the deficiencies or to comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that their competent authorities have the power to:

(a) suspend temporarily, or request a certification or authorisation body, or a court or tribunal, in accordance with national law, to suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity;

(b) request that the relevant bodies, courts or tribunals, in accordance with national law, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions in that entity.

▼B

Temporary suspensions or prohibitions imposed pursuant to this paragraph shall be applied only until the entity concerned takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such enforcement measures were applied. The imposition of such temporary suspensions or prohibitions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

The enforcement measures provided for in this paragraph shall not be applicable to public administration entities that are subject to this Directive.

6. Member States shall ensure that any natural person responsible for or acting as a legal representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the power to ensure its compliance with this Directive. Member States shall ensure that it is possible to hold such natural persons liable for breach of their duties to ensure compliance with this Directive.

As regards public administration entities, this paragraph shall be without prejudice to national law as regards the liability of public servants and elected or appointed officials.

7. When taking any of the enforcement measures referred to in paragraph 4 or 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:

(a) the seriousness of the infringement and the importance of the provisions breached, the following, inter alia, constituting serious infringement in any event:

  (i) repeated violations;

  (ii) a failure to notify or remedy significant incidents;

  (iii) a failure to remedy deficiencies following binding instructions from competent authorities;

  (iv) the obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement;

  (v) providing false or grossly inaccurate information in relation to cybersecurity risk-management measures or reporting obligations laid down in Articles 21 and 23;

(b) the duration of the infringement;

(c) any relevant previous infringements by the entity concerned;

(d) any material or non-material damage caused, including any financial or economic loss, effects on other services and the number of users affected;

▼B

(e) any intent or negligence on the part of the perpetrator of the infringement;

(f) any measures taken by the entity to prevent or mitigate the material or non-material damage;

(g) any adherence to approved codes of conduct or approved certification mechanisms;

(h) the level of cooperation of the natural or legal persons held responsible with the competent authorities.

8. The competent authorities shall set out a detailed reasoning for their enforcement measures. Before adopting such measures, the competent authorities shall notify the entities concerned of their preliminary findings. They shall also allow a reasonable time for those entities to submit observations, except in duly substantiated cases where immediate action to prevent or respond to incidents would otherwise be impeded.

9. Member States shall ensure that their competent authorities under this Directive inform the relevant competent authorities within the same Member State under Directive (EU) 2022/2557 when exercising their supervisory and enforcement powers aiming to ensure compliance of an entity identified as a critical entity under Directive (EU) 2022/2557 with this Directive. Where appropriate, the competent authorities under Directive (EU) 2022/2557 may request the competent authorities under this Directive to exercise their supervisory and enforcement powers in relation to an entity that is identified as a critical entity under Directive (EU) 2022/2557.

10. Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.

Article 33

Supervisory and enforcement measures in relation to important entities

1. When provided with evidence, indication or information that an important entity allegedly does not comply with this Directive, in particular Articles 21 and 23 thereof, Member States shall ensure that the competent authorities take action, where necessary, through *ex post* supervisory measures. Member States shall ensure that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to:

▼B

(a) on-site inspections and off-site *ex post* supervision conducted by trained professionals;

(b) targeted security audits carried out by an independent body or a competent authority;

(c) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned;

(d) requests for information necessary to assess, *ex post*, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27;

(e) requests to access data, documents and information necessary to carry out their supervisory tasks;

(f) requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.

The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.

3. When exercising their powers under paragraph 2, point (d), (e) or (f), the competent authorities shall state the purpose of the request and specify the information requested.

4. Member States shall ensure that the competent authorities, when exercising their enforcement powers in relation to important entities, have the power at least to:

(a) issue warnings about infringements of this Directive by the entities concerned;

(b) adopt binding instructions or an order requiring the entities concerned to remedy the deficiencies identified or the infringement of this Directive;

(c) order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct;

(d) order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period;

▼B

(e) order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat;

(f) order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;

(g) order the entities concerned to make public aspects of infringements of this Directive in a specified manner;

(h) impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (g) of this paragraph.

5. Article 32(6), (7) and (8) shall apply *mutatis mutandis* to the supervisory and enforcement measures provided for in this Article for important entities.

6. Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an important entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.

Article 34

General conditions for imposing administrative fines on essential and important entities

1. Member States shall ensure that the administrative fines imposed on essential and important entities pursuant to this Article in respect of infringements of this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.

2. Administrative fines shall be imposed in addition to any of the measures referred to in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g).

3. When deciding whether to impose an administrative fine and deciding on its amount in each individual case, due regard shall be given, as a minimum, to the elements provided for in Article 32(7).

4. Member States shall ensure that where they infringe Article 21 or 23, essential entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.

▼B

5. Member States shall ensure that where they infringe Article 21 or 23, important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.

6. Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement of this Directive in accordance with a prior decision of the competent authority.

7. Without prejudice to the powers of the competent authorities pursuant to Articles 32 and 33, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities.

8. Where the legal system of a Member State does not provide for administrative fines, that Member State shall ensure that this Article is applied in such a manner that the fine is initiated by the competent authority and imposed by competent national courts or tribunals, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by the competent authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. The Member State shall notify to the Commission the provisions of the laws which it adopts pursuant to this paragraph by 17 October 2024 and, without delay, any subsequent amendment law or amendment affecting them.

Article 35

Infringements entailing a personal data breach

1. Where the competent authorities become aware in the course of supervision or enforcement that the infringement by an essential or important entity of the obligations laid down in Articles 21 and 23 of this Directive can entail a personal data breach, as defined in Article 4, point (12), of Regulation (EU) 2016/679 which is to be notified pursuant to Article 33 of that Regulation, they shall, without undue delay, inform the supervisory authorities as referred to in Article 55 or 56 of that Regulation.

2. Where the supervisory authorities as referred to in Article 55 or 56 of Regulation (EU) 2016/679 impose an administrative fine pursuant to Article 58(2), point (i), of that Regulation, the competent authorities shall not impose an administrative fine pursuant to Article 34 of this Directive for an infringement referred to in paragraph 1 of this Article arising from the same conduct as that which was the subject of the administrative fine under Article 58(2), point (i), of Regulation (EU) 2016/679. The competent authorities may, however, impose the enforcement measures provided for in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g), of this Directive.

3. Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority shall inform the supervisory authority established in its own Member State of the potential data breach referred to in paragraph 1.

▼B

Article 36

Penalties

Member States shall lay down rules on penalties applicable to infringements of national measures adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 17 January 2025, notify the Commission of those rules and of those measures and shall notify it, without delay of any subsequent amendment affecting them.

Article 37

Mutual assistance

1. Where an entity provides services in more than one Member State, or provides services in one or more Member States and its network and information systems are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with and assist each other as necessary. That cooperation shall entail, at least, that:

(a) the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken;

(b) a competent authority may request another competent authority to take supervisory or enforcement measures;

(c) a competent authority shall, upon receipt of a substantiated request from another competent authority, provide the other competent authority with mutual assistance proportionate to its own resources so that the supervisory or enforcement measures can be implemented in an effective, efficient and consistent manner.

The mutual assistance referred to in the first subparagraph, point (c), may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed shall not refuse that request unless it is established that it does not have the competence to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks of the competent authority, or the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the essential interests of the Member State's national security, public security or defence. Before refusing such a request, the competent authority shall consult the other competent authorities concerned as well as, upon the request of one of the Member States concerned, the Commission and ENISA.

▼B

2. Where appropriate and with common agreement, the competent authorities of various Member States may carry out joint supervisory actions.

CHAPTER VIII

DELEGATED AND IMPLEMENTING ACTS

Article 38

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 24(2) shall be conferred on the Commission for a period of five years from 16 January 2023.

3. The delegation of power referred to in Article 24(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 24(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 39

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

▼B

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.

CHAPTER IX

FINAL PROVISIONS

Article 40

Review

By 17 October 2027 and every 36 months thereafter, the Commission shall review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of the size of the entities concerned, and the sectors, subsectors and types of entity referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. To that end and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The report shall be accompanied, where necessary, by a legislative proposal.

Article 41

Transposition

1. By 17 October 2024, 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 18 October 2024.

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 42

Amendment of Regulation (EU) No 910/2014

In Regulation (EU) No 910/2014, Article 19 is deleted with effect from 18 October 2024.

Article 43

Amendment of Directive (EU) 2018/1972

In Directive (EU) 2018/1972, Articles 40 and 41 are deleted with effect from 18 October 2024.

▼B

Article 44

Repeal

Directive (EU) 2016/1148 is repealed with effect from 18 October 2024.

References to the repealed Directive shall be construed as references to this Directive and shall be read in accordance with the correlation table set out in Annex III.

Article 45

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 46

Addressees

This Directive is addressed to the Member States.

▼B

ANNEX I

SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings as defined in Article 2, point (57), of Directive (EU) 2019/944 of the European Parliament and of the Council ([1]), which carry out the function of 'supply' as defined in Article 2, point (12), of that Directive
		— Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944
		— Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/944
		— Producers as defined in Article 2, point (38), of Directive (EU) 2019/944
		— Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council ([2]) — Market participants as defined in Article 2, point (25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2, points (18), (20) and (59), of Directive (EU) 2019/944 — Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider
	(b) District heating and cooling	— Operators of district heating or district cooling as defined in Article 2, point (19), of Directive (EU) 2018/2001 of the European Parliament and of the Council ([3])
	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		— Central stockholding entities as defined in Article 2, point (f), of Council Directive 2009/119/EC ([4])
	(d) Gas	— Supply undertakings as defined in Article 2, point (8), of Directive 2009/73/EC of the European Parliament and of the Council ([5])
		— Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC
		— Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC
		— Storage system operators as defined in Article 2, point (10), of Directive 2009/73/EC

▼B

Sector	Subsector	Type of entity
		— LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC
		— Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities
	(e) Hydrogen	— Operators of hydrogen production, storage and transmission
2. Transport	(a) Air	— Air carriers as defined in Article 3, point (4), of Regulation (EC) No 300/2008 used for commercial purposes
		— Airport managing bodies as defined in Article 2, point (2), of Directive 2009/12/EC of the European Parliament and of the Council ([6]), airports as defined in Article 2, point (1), of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council ([7]), and entities operating ancillary installations contained within airports
		— Traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of Regulation (EC) No 549/2004 of the European Parliament and of the Council ([8])
	(b) Rail	— Infrastructure managers as defined in Article 3, point (2), of Directive 2012/34/EU of the European Parliament and of the Council ([9])
		— Railway undertakings as defined in Article 3, point (1), of Directive 2012/34/EU, including operators of service facilities as defined in Article 3, point (12), of that Directive
	(c) Water	— Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council ([10]), not including the individual vessels operated by those companies

▼B

Sector	Subsector	Type of entity
		— Managing bodies of ports as defined in Article 3, point (1), of Directive 2005/65/EC of the European Parliament and of the Council ([11]), including their port facilities as defined in Article 2, point (11), of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		— Operators of vessel traffic services (VTS) as defined in Article 3, point (o), of Directive 2002/59/EC of the European Parliament and of the Council ([12])
	(d) Road	— Road authorities as defined in Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962 ([13]) responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity
		— Operators of Intelligent Transport Systems as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council ([14])
3. Banking		Credit institutions as defined in Article 4, point (1), of Regulation (EU) No 575/2013 of the European Parliament and of the Council ([15])
4. Financial market infrastructures		— Operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU of the European Parliament and of the Council ([16])
		— Central counterparties (CCPs) as defined in Article 2, point (1), of Regulation (EU) No 648/2012 of the European Parliament and of the Council ([17])
5. Health		— Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council ([18])
		— EU reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council ([19])
		— Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council ([20]) — Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 — Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list) within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council ([21])

▼B

Sector	Subsector	Type of entity
6. Drinking water		Suppliers and distributors of water intended for human consumption as defined in Article 2, point (1)(a), of Directive (EU) 2020/2184 of the European Parliament and of the Council ([22]), excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods
7. Waste water		Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2, points (1), (2) and (3), of Council Directive 91/271/EEC ([23]), excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity
8. Digital infrastructure		— Internet Exchange Point providers
		— DNS service providers, excluding operators of root name servers
		— TLD name registries
		— Cloud computing service providers
		— Data centre service providers
		— Content delivery network providers
		— Trust service providers
		— Providers of public electronic communications networks
		— Providers of publicly available electronic communications services
9. ICT service management (business-to-business)		— Managed service providers — Managed security service providers
10. Public administration		— Public administration entities of central governments as defined by a Member State in accordance with national law
		— Public administration entities at regional level as defined by a Member State in accordance with national law

▼B

Sector	Subsector	Type of entity
11. Space		Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

(1) Directive (EU) 2019/944 of the European Parliament and of the Council 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).
(2) Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).
(3) Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).
(4) Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p. 9).
(5) Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).
(6) Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).
(7) Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).
(8) Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p. 1).
(9) Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p. 32).
(10) Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).
(11) Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).
(12) Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).
(13) Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21).
(14) Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).
(15) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).
(16) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).
(17) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).
(18) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).
(19) Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26).
(20) Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 67).
(21) Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1).
(22) Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (OJ L 435, 23.12.2020, p. 1).
(23) Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p. 40).

▼B

ANNEX II

OTHER CRITICAL SECTORS

Sector	Subsector	Type of entity
1. Postal and courier services		Postal service providers as defined in Article 2, point (1a), of Directive 97/67/EC, including providers of courier services
2. Waste management		Undertakings carrying out waste management as defined in Article 3, point (9), of Directive 2008/98/EC of the European Parliament and of the Council ([1]), excluding undertakings for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, as referred to in Article 3, points (9) and (14), of Regulation (EC) No 1907/2006 of the European Parliament and of the Council ([2]) and undertakings carrying out the production of articles, as defined in Article 3, point (3), of that Regulation, from substances or mixtures
4. Production, processing and distribution of food		Food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council ([3]) which are engaged in wholesale distribution and industrial production and processing
5. Manufacturing	(a) Manufacture of medical devices and *in vitro* diagnostic medical devices	Entities manufacturing medical devices as defined in Article 2, point (1), of Regulation (EU) 2017/745 of the European Parliament and of the Council ([4]), and entities manufacturing *in vitro* diagnostic medical devices as defined in Article 2, point (2), of Regulation (EU) 2017/746 of the European Parliament and of the Council ([5]) with the exception of entities manufacturing medical devices referred to in Annex I, point 5, fifth indent, of this Directive
	(b) Manufacture of computer, electronic and optical products	Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2

02022L2555 — EN — 27.12.2022 — 000.004 — 56

▼B

Sector	Subsector	Type of entity
	(d) Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
	(e) Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2
	(f) Manufacture of other transport equipment	Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2
6. Digital providers		— Providers of online marketplaces
		— Providers of online search engines
		— Providers of social networking services platforms
7. Research		Research organisations

([1]) Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3).
([2]) Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1).
([3]) Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p. 1).
([4]) Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).
([5]) Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

▼B

ANNEX III

CORRELATION TABLE

Directive (EU) 2016/1148	This Directive
Article 1(1)	Article 1(1)
Article 1(2)	Article 1(2)
Article 1(3)	-
Article 1(4)	Article 2(12)
Article 1(5)	Article 2(13)
Article 1(6)	Article 2(6) and (11)
Article 1(7)	Article 4
Article 2	Article 2(14)
Article 3	Article 5
Article 4	Article 6
Article 5	–
Article 6	–
Article 7(1)	Article 7(1) and (2)
Article 7(2)	Article 7(4)
Article 7(3)	Article 7(3)
Article 8(1) to (5)	Article 8(1) to (5)
Article 8(6)	Article 13(4)
Article 8(7)	Article 8(6)
Article 9(1), (2) and (3)	Article 10(1), (2) and (3)
Article 9(4)	Article 10(9)
Article 9(5)	Article 10(10)
Article 10(1), (2) and (3), first subparagraph	Article 13(1), (2) and (3)
Article 10(3), second subparagraph	Article 23(9)
Article 11(1)	Article 14(1) and (2)
Article 11(2)	Article 14(3)
Article 11(3)	Article 14(4), first subparagraph, points (a) to (q) and (s), and paragraph (7)

▼B

Directive (EU) 2016/1148	This Directive
Article 11(4)	Article 14(4), first subparagraph, point (r), and second subparagraph
Article 11(5)	Article 14(8)
Article 12(1) to (5)	Article 15(1) to (5)
Article 13	Article 17
Article 14(1) and (2)	Article 21(1) to (4)
Article 14(3)	Article 23(1)
Article 14(4)	Article 23(3)
Article 14(5)	Article 23(5), (6) and (8)
Article 14(6)	Article 23(7)
Article 14(7)	Article 23(11)
Article 15(1)	Article 31(1)
Article 15(2), first subparagraph, point (a)	Article 32(2), point (e)
Article 15(2), first subparagraph, point (b)	Article 32(2), point (g)
Article 15(2), second subparagraph	Article 32(3)
Article 15(3)	Article 32(4), point (b)
Article 15(4)	Article 31(3)
Article 16(1) and (2)	Article 21(1) to (4)
Article 16(3)	Article 23(1)
Article 16(4)	Article 23(3)
Article 16(5)	–
Article 16(6)	Article 23(6)
Article 16(7)	Article 23(7)
Article 16(8) and (9)	Article 21(5) and Article 23(11)
Article 16(10)	–
Article 16(11)	Article 2(1), (2) and (3)
Article 17(1)	Article 33(1)
Article 17(2), point (a)	Article 32(2), point (e)
Article 17(2), point (b)	Article 32(4), point (b)

▼B

Directive (EU) 2016/1148	This Directive
Article 17(3)	Article 37(1), points (a) and (b)
Article 18(1)	Article 26(1), point (b), and paragraph (2)
Article 18(2)	Article 26(3)
Article 18(3)	Article 26(4)
Article 19	Article 25
Article 20	Article 30
Article 21	Article 36
Article 22	Article 39
Article 23	Article 40
Article 24	–
Article 25	Article 41
Article 26	Article 45
Article 27	Article 46
Annex I, point (1)	Article 11(1)
Annex I, points (2)(a)(i) to (iv)	Article 11(2), points (a) to (d)
Annex I, point (2)(a)(v)	Article 11(2), point (f)
Annex I, point (2)(b)	Article 11(4)
Annex I, points (2)(c)(i) and (ii)	Article 11(5), point (a)
Annex II	Annex I
Annex III, points (1) and (2)	Annex II, point (6)
Annex III, point (3)	Annex I, point (8)