Brussels, 26 November 2021 (OR. en) 14337/21, "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148." Unofficial clean version of provisions, 30 Mar 2022.

CHAPTER I
General provisions

Article 1
Subject matter

1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union so as to improve the functioning of the internal market.
2. To that end, this Directive:
   (a) lays down obligations on Member States to adopt national cybersecurity strategies, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs);
   (b) lays down cybersecurity risk management and reporting obligations for entities of a type referred to in Annexes I and II;
   (c) lays down rules and obligations on cybersecurity information sharing.

Article 2
Scope

1. This Directive applies to public and private entities of the types listed in Annexes I and II which meet or exceed the ceilings for medium-sized enterprises within the meaning of Commission Recommendation 2003/361/EC[27]. Article 3(4) and Article 6(2) second and third subparagraphs of the Annex to that Recommendation shall not apply for the purposes of this Directive.
2. Regardless of the size of the entities referred to in paragraph 1, this Directive also applies where:
   (a) the services are provided by one of the following entities:
      (i) providers of public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I;
      (ii) qualified trust service providers referred to in point XX of Annex I;
      (iii) non-qualified trust service providers referred to in point XX of Annex I;
      (iv) top–level domain name registries referred to in point 8 of Annex I;
   (b)
   (c) 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;
   (d) a potential disruption of the service provided by the entity could have significant impact on public safety, public security or public health;
   (e) a potential disruption of the service provided by the entity could induce significant systemic risks, in particular for the sectors where such disruption could have a cross-border impact;
   (f)
   (g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council[28] [Resilience of Critical Entities Directive], **[**or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive**]**.

2a. Regardless of their size, this Directive also applies to public administration entities of central governments recognised as such in a Member State in accordance with national law and referred to in point 9 of Annex I. Member States may establish that this Directive also applies to public administration entities at regional and local levels.

3.
This Directive is without prejudice to the Member States' responsibilities to safeguard national security

or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.

3a. (1) This Directive does not apply to:

(a) entities that fall outside the scope of Union law and in any event all entities that mainly carry out activities in the areas of defence, national security, public security or law enforcement regardless of which entity is carrying out those activities and whether it is a public entity or a private entity, without prejudice to point (2);

(b) entities that carry out activities in the areas of the judiciary, parliaments or central banks.

(2) Where public administration entities carry out activities in these areas only as part of their overall activities, they shall be excluded in their entirety from the scope of this Directive.

3aa. This Directive does not apply to:

(i) activities of entities which fall outside the scope of Union law and in any event all activities concerning national security or defence, regardless of which entity is carrying out those activities and whether it is a public entity or a private entity;

(ii) activities of entities in the judiciary, the parliaments, central banks and in the area of public security, including public administration entities carrying out law enforcement activities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

3aaa. The obligations laid down in this Directive do not entail the supply of information the disclosure of which is contrary to the Member States' essential interests of national security, public security or defence.

3aaaa. This Directive is without prejudice to Union law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC.

3b. This Directive does not apply to entities which are exempted from the Regulation (EU) XXXX/XXXX of the European Parliament and of the Council [the DORA Regulation] in accordance with Art 2 para 4 of the DORA Regulation.

4. This Directive applies without prejudice to Directives 2011/93/EU[30] and 2013/40/EU[31] of the European Parliament and of the Council.

5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities according to 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 essential or important entities.

Article 2bis

Essential and important entities

1. Of the entities to which this Directive applies, the following shall be considered essential:

(i) entities of a type provided for in points 1 to 8a and 10 of Annex I to this Directive which exceed the ceilings for medium-sized enterprises as defined in Commission Recommendation 2003/361/EC;

(ii) medium-sized entities referred to in Article 2(2), points (a) (i);

(iii) entities referred to in Article 2(2), points (a) (ii) and (iv) of this Directive, irrespective of the size;

(iv) entities referred to in Article 2(2) point (g) and Article 2(2a) of this Directive, irrespective of the size;

(v) if established by the Member States, entities which the Member States identified before the entry into force of this Directive as operators of essential services in accordance with Directive (EU) 2016/1148 or national law;

(vi) entities which exceed the ceilings for medium-sized enterprises as defined in Commission Recommendation 2003/361/EC of the type provided for in Annex II that Member States determine that are essential on the basis of criteria referred to in Article 2(2), points (c) to (e);

(vii) medium-sized entities within the meaning of Commission Recommendation 2003/361/EC that Member States determine that are essential on the basis of criteria referred to in Article 2(2), points (c) to (e);

(viii) micro or small-sized entities within the meaning of Commission Recommendation 2003/361/EC provided for in paragraph (2), point (a) (i) or identified pursuant to paragraph (2), points (c) to (e) of this Article that Member States determine that are essential on the basis of national risk assessments.

2. The entities to which this Directive applies, the following shall be considered important entities:

(i) entities of a type provided for in Annex I to this Directive which qualify as medium-sized enterprises within the meaning of Commission Recommendation 2003/361/EC and entities of the type provided for in Annex II which meet or exceed the ceilings for medium-sized enterprises within the meaning of Commission Recommendation 2003/361/EC[32];

(ii) entities referred to in Article 2(2) point (iii) of this Directive, irrespective of the size;

(iii) small and micro entities referred to in Article 2(2) (a) (i);

(iv) small and micro entities that Member States determine that are important entities on the basis of Article 2(2)(c) to (e).

Article 2a

Notification Mechanisms

1. Member States may establish national mechanism for self-notification that require all entities under the scope of this Directive to submit at least their name, address, contact details, the sector in which they operate or type of service that they provide and, where applicable, the list of Member States where they provide services subject to this Directive, to the competent authorities under this Directive or bodies designated for this purpose by the Member States.
2. Member States shall submit to the Commission in relation to the entities that they identified pursuant to Article 2(2) points (b) to (e), at least relevant information on the number of identified entities, the sector they belong to or type of service they provide as per the Annexes, and the specific provision(s) of Article 2(2) based on which they were identified by [12 months after the transposition deadline of this Directive]. Member States shall review this information, on a regular basis, and at least every two years thereafter and, where appropriate, update it.

Article 2b

Sector-specific Union acts

1. Where sector–specific Union legal acts require essential or important entities to adopt cybersecurity risk management measures or to notify significant incidents or cyber threats, 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 VI, shall not apply to such entities. If 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 provisions.

2. The requirements referred in paragraph 1 of this Article shall be considered equivalent in effect to the obligations laid down in this Directive if the respective sector specific Union act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the competent authorities under this Directive or the designated CSIRTs and if:

(a) cybersecurity risk management measures, are at least equivalent in effect to those laid down in Article 18 (1) and (2) of this Directive; or

(b) requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 20 (1) to (6).

3. The Commission shall periodically review the application of the equivalent effect requirements provided for in paragraphs 1 and 2 of this Article in relation to sector- specific provisions of Union legal acts. The Commission shall consult the Cooperation Group and ENISA when preparing those periodical reviews.

Article 3

Minimum harmonisation

Without prejudice to their other obligations under Union law, Member States may, adopt or maintain provisions ensuring a higher level of cybersecurity in the areas covered by this Directive.

Article 4

Definitions

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

(1) 'network and information system' means:

(a) an electronic communications network within the meaning of Article 2(1) of Directive (EU) 2018/1972;

(b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data;

(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 compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or of the services offered by, or accessible via, those network, and information systems;

(2a) 'electronic communications services' means electronics communications services within the meaning of Article 2(4) of Directive (EU) 2018/1972;

(3) 'cybersecurity' means cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council[33];

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

(5) 'incident' means any 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;

(5a) 'large-scale cybersecurity incident' means an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it.

(6) 'incident handling' means all actions and procedures aiming at detection, analysis and containment of and a response to an incident;

(6a) 'risk' means the potential for loss or disruption caused by an incident and shall be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of said incident.

(7) 'cyber threat' means cyber threat within the meaning Article 2(8) of Regulation (EU) 2019/881;

(7a) 'significant cyber threat' means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to severely impact the network and information systems of an entity or its users by causing considerable material or non- material losses;

(8) 'vulnerability' means a weakness, susceptibility or flaw of an ICT asset or a system that can be exploited by a cyber threat;

(8a) 'near misses' means an event that could potentially have caused harm to the network and information systems of an entity or its users, but was successfully prevented from fully transpiring;

(9) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of i) a DNS service provider, a top-level domain (TLD) name registry, a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point ~~1~~**6** of the Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive;

(10) 'standard' means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[34];

(11) 'technical specification' means a technical specification within the meaning of Article 2(4) of Regulation (EU) No 1025/2012;

(12) 'internet exchange point (IXP)' 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; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

(13) 'domain name system (DNS)' means a hierarchical distributed naming system which allows end-users to reach services and resources on the internet;

(14) 'DNS service provider' means an entity that provides recursive or authoritative domain name resolution services for third-party usage, with the exception of the root name servers;

(15) 'top–level domain 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, while excluding the situations where top-level domain names are used by a registry only for own use;

(15a) 'entities providing domain name registration services for the TLD' means TLD name registries, registrars for the TLDs and agents of registrars such as resellers and providers of proxy services;

(16) 'digital service' means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council[35];

(16a) 'trust services' means trust services within the meaning of Article 3(16) of Regulation (EU) No 910/2014;

(16b) 'qualified trust service provider' means a qualified trust service provider within the meaning of Article 3(20) of Regulation (EU) No 910/2014;

(17) 'online marketplace' means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council[36];

(18) 'online search engine' means a digital service within the meaning of Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council[37];

(19) '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 when those are distributed over several locations;

(20) 'data centre service' means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control; (OJ L 186, 11.7.2019, p. 57).

(21) '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;

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

(23) 'public administration entity' means, an entity recognised as such in a Member State in accordance with national law, that 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 it 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 authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it 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.

(24) 'entity' means any 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;

(25) 'essential entity' means any entity of a type provided for in the Annex I and designated as 'essential' in accordance with Article 2bis(1);

(26) 'important entity' means any entity of the type provided for in Annexes I and II and designated 'important' in accordance with Article 2bis(2).

(26a) 'ICT product' means an ICT product within the meaning of Article 2(12) of Regulation (EU) 2019/881;

(26aa) 'ICT service' means an ICT service within the meaning of Article 2(13) of Regulation (EU) 2019/881;

(26ab) 'ICT process' means an ICT process within the meaning of Article 2(14) of Regulation (EU) 2019/881.

(26ac) 'Managed service provider' means any entity that delivers services, such as network, application, infrastructure and security, via ongoing and regular management, support and active administration on customers' premises, in their MSP's data centre (hosting), or in a third-party data centre.

(26ad) 'Managed security service provider' means any entity which provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services.

It also includes the use of high-availability security operation centres (either from their own facilities or from other data centre providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture.

CHAPTER II

Coordinated cybersecurity regulatory frameworks

Article 5

National cybersecurity strategy

1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following:

(a) objectives and priorities of the Member States' strategy on cybersecurity;

(b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 and the roles and responsibilities of the various authorities and actors involved in the implementation of the strategy;

(c) guidance to identify relevant assets and assess cybersecurity risks in that Member State;

(d) an identification of the measures ensuring preparedness, response and recovery to incidents, including cooperation between the public and private sectors;

(e)

(f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[38] [Resilience of Critical Entities Directive] for the purposes of information sharing on cybersecurity risks, cyber threats and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate;

(fa) policy framework for coordination and cooperation between competent authorities under this Directive and competent authorities designated under sector-specific legislation.

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

following policies:

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

(b) a policy regarding the inclusion and specification of cybersecurity-related requirements for ICT products and services in public procurement, including cybersecurity certification;

(c) a policy on management of vulnerabilities, encompassing the promotion and facilitation of voluntary coordinated vulnerability disclosure within the meaning of Article 6(1);

(d) a policy related to sustaining the general availability, integrity and confidentiality of the public core of the open internet;

(e) a policy on promoting and developing cybersecurity education and training, skills, awareness raising and research and development initiatives;

(f) a policy on supporting academic and research institutions to develop cybersecurity tools and secure network infrastructure;

(g) a policy, relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between companies in compliance with Union law;

(h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cyber~~security~~ threats.

3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. In doing so, Member States may exclude elements of the strategy which relate to national security.

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, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon their request, in the development of a national strategy and of key performance indicators for the assessment of the strategy.

Article 6

Coordinated vulnerability disclosure and a European vulnerability registry

1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of coordinated vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity, the potential vulnerability owner and the manufacturer or provider of ICT products or ICT services. Any natural or legal person may report, possibly anonymously, a vulnerability referred to in Article 4(8) to the designated CSIRT. The designated CSIRT shall ensure a diligent follow-up of the report and the confidentiality of the identity of the person who reports the vulnerability. Where the reported vulnerability could potentially have significant impact on entities in more than one Member State, the designated CSIRT of each Member State concerned shall, where appropriate, cooperate with other designated CSIRTs within the CSIRTs network.

2. ENISA shall develop and maintain a European vulnerability registry, in consultation with the Cooperation Group. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register, on a voluntary basis, publicly known vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties. The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance issued by national competent authorities or CSIRTs addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated. ENISA shall ensure that the European vulnerability registry uses secure and resilient communication and information infrastructure.

Article 7

National cybersecurity crisis management frameworks

1. Each Member State shall designate one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises. Member States shall ensure that competent authorities have adequate resources to perform, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general crisis management.
2. Each Member State shall identify capabilities, assets and procedures that can be deployed in case of a crisis for the purposes of this Directive.
3. Each Member State shall adopt a national cybersecurity incident and crisis response plan where objectives and modalities in the management of large-scale cybersecurity incidents and crises are set out. The plan shall lay down, in particular, the following:
   (a) objectives of national preparedness measures and activities;
   (b) tasks and responsibilities of the national competent authorities;
   (c) cybersecurity crisis management procedures, including their integration into the general national crisis management framework and information exchange channels;
   (d) preparedness measures, including regular exercises and training activities;
   (e) relevant public and private parties 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.
4. Member States shall inform the Commission about the designation of their competent authorities referred to in paragraph 1 and submit relevant information relating to the requirements of paragraph 3 of this Article about their national cybersecurity incident and crisis response plans within three months from that designation and the adoption of those plans. Member States may exclude specific information where and to the extent that it is ~~strictly~~ necessary for their national security, public security or defence.

Article 8

National competent authorities and single points of contact

1. Each Member State shall designate one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VI of this Directive. Member States may designate to that effect an existing authority or existing authorities.
2. The competent authorities referred to paragraph 1 shall monitor the application of this Directive at national level.
3. Each Member State shall designate one national single point of contact on cybersecurity ('single point of contact'). Where a Member State designates only one competent authority, 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 in other Member States, as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.
5. Member States shall ensure that the competent authorities referred to in paragraph 1 and the 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. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group referred to in Article 12.
6. Each Member State shall notify to the Commission, without undue delay, the designation of the competent authority referred to in paragraph 1 and single point of contact referred to in paragraph 3, their tasks, and any subsequent change thereto. Each Member State shall make public their designation. The Commission shall publish the list of the designated single points of contacts.

Article 9

Computer security incident response teams (CSIRTs)

1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in Article 10(1), covering at least the sectors, subsectors or entities referred to in Annexes I and II, and be responsible for incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority referred to in Article 8.

2. Member States shall ensure that each CSIRT has adequate resources to carry out effectively their tasks as set out in Article 10(2). When carrying out these tasks, CSIRTs may prioritise the provision of particular services to entities based on a risk-based approach.

3. Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure to exchange information with essential and important entities and other relevant interested parties. To this end, Member States shall ensure that the CSIRTs contribute to the deployment of secure information sharing tools.

4. CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 26 with trusted sectorial or cross-sectorial communities of essential and important entities.

5. CSIRTs shall participate in peer learnings organised in accordance with Article 16.

6. Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 13.

7. Member States shall communicate to the Commission without undue delay the CSIRTs designated in accordance with paragraph 1, the CSIRT coordinator designated in accordance with Article 6(1) and their respective tasks provided in relation to the entities referred to in Annexes I and II.

8. Member States may request the assistance of ENISA in developing national CSIRTs.

Article 10

Requirements and tasks of CSIRTs

1. CSIRTs shall comply with the following requirements:
   (a) CSIRTs shall ensure a high level of availability of their communications ~~services~~ channels by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. CSIRTs shall clearly specify the communication channels and make them known to constituency and cooperative partners;
   (b) CSIRTs' premises and the supporting information systems shall be located in secure sites;
   (c) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular, to facilitate effective and efficient handovers;
   (d) CSIRTs shall be adequately staffed to ensure availability at all times;
   (e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services;
   (f) CSIRTs shall have the possibility to participate in international cooperation networks.
2. CSIRTs shall have the following tasks:
   (a) monitoring cyber threats, vulnerabilities and incidents at national level;
   (b) providing early warning, alerts, announcements and dissemination of information to essential and important entities as well as to competent authorities and other relevant interested parties on cyber threats, vulnerabilities and incidents;
   (c) responding to incidents;
   (d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;
   (e) providing, a proactive scanning of the network and information systems to detect vulnerabilities with potential significant impact provided that, where there is no consent of that entity, the network and information systems are not intruded or their functioning negatively impacted;
   (f) participating in the CSIRTs network and providing mutual assistance according to their capacities and competencies to other members of the network upon their request.

(fa) where applicable, acting as a coordinator for the purpose of the coordinated vulnerability disclosure process pursuant to Article 6 (1) that shall include in particular facilitating the interaction between the reporting entities, the potential vulnerability owner and the manufacturer or provider of ICT products or ICT services in cases where this is necessary, identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure time lines and managing vulnerabilities that affect multiple organisations (multi-party coordinated vulnerability disclosure).

3. CSIRTs shall establish cooperation relationships with relevant actors in the private sector, with a view to better achieving the objectives of the Directive.

3a. CSIRTs may establish cooperation relationships with national CSIRTs of third countries. As part of this cooperation, they may exchange relevant, information, including personal data in accordance with Union law on data protection.

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

(a) incident handling procedures;

(b) cybersecurity crisis management;

(c) coordinated vulnerability disclosure.

Article 11

Cooperation at national level

1. Where they are separate, the competent authorities referred to in Article 8, the single point of contact and the CSIRT(s) of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.

2. Member States shall ensure that either their competent authorities or their CSIRTs receive notifications on incidents, and significant cyber threats and near misses submitted pursuant to this Directive. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities, pursuant to
Article 20.

3. Each Member State shall ensure that its competent authorities or CSIRTs inform its single point of contact of notifications on incidents, significant cyber threats and near misses submitted pursuant to this Directive.

4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities, CSIRTs, single points of contact as well as law enforcement authorities, data protection authorities, and the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]], the competent authorities under Commission Implementing Regulation 2019/1583, the national regulatory authorities designated in accordance with Directive (EU) 2018/1972, the national authorities designated pursuant to Article 17 of Regulation (EU) No 910/2014, the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council [the DORA Regulation], as well as competent authorities designated by other sector-specific Union legal acts, within that Member State.

5. Member States shall ensure that their competent authorities under this Directive and the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] regularly exchange on the identification of critical entities, cybersecurity risks, cyber threats and incidents as well as on non-cyber risks, threats and incidents affecting essential entities identified as critical, [or as entities equivalent to critical entities,] pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken in response to those risks and incidents. Member States shall also ensure that competent authorities under this Directive and the competent authorities designated under Regulation XXXX/XXXX [DORA Regulation], Directive 2018/1972 and Regulation (EU) 910/2014 regularly exchange relevant information.

With regard to trust service providers and in particular, in cases where that supervisory role under this Directive is assigned to a different body than the supervisory bodies designated pursuant to Regulation

(EU) 910/2014, the national competent authorities under this Directive shall cooperate closely, in a timely manner, by exchanging the relevant information in order to ensure effective supervision and compliance of trust service providers with the requirements set out in this Directive and Regulation [XXXX/XXXX] and, where applicable, the national competent authority under this Directive shall, without undue delay, inform the eIDAS supervisory body about any notified significant cyber threat or incident with impact on trust services.

5a. For the purpose~~s~~ of simplifying the reporting of incidents, Member States may establish a single-entry point for all notifications required under this Directive, as well as under Regulation (EU) 2016/679 and Directive 2002/58/EC, where appropriate. Member States may use the single entry point for notifications required under other sector-specific Union legal acts. This single-entry point shall not affect the application of the provisions of Regulation (EU) 2016/679 and Directive 2002/58/EC, in particular those relating to independent supervisory authorities.

CHAPTER III
EU Cooperation

Article 12
Cooperation Group

1. In order to support and to 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 6.
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 designated under Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group in accordance with Article 42(1) of Regulation (EU) XXXX/XXXX [the DORA Regulation].

   Where appropriate, the Cooperation Group may invite 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) providing guidance to competent authorities in relation to the transposition and implementation of this Directive;
   (aa) providing guidance in relation to the development and implementation of policies on coordinated vulnerability disclosure as referred to in Article 5(2) (c) and Article 6(1);
   (b) exchanging 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, trainings, exercises and skills, building capacity as well as standards and technical specifications;
   (c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives;
   (d) exchanging advice and cooperating with the Commission on draft Commission implementing acts adopted pursuant to this Directive;
   (e) exchanging best practices and information with relevant Union institutions, bodies, offices and agencies;
   (ea) exchanging views on the implementation of sectorial legislation with cybersecurity aspects;
   (f) discussing reports on the peer ~~review~~ learnings referred to in Article 16(7);
   (g) discussing experiences ~~results~~ from joint-supervisory activities in cross-border cases as referred to in Article 34;
   (h) providing strategic guidance to the CSIRTs network and EU–CyCLONe on specific emerging issues;

(ha) exchanging views on policy follow-up of large-scale cybersecurity incidents on the basis of lessons learned of the CSIRTs network and EU–CyCLONe;

(i) contributing to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the Member States' competent authorities or CSIRTs;

(j) organising regular joint meetings with relevant private interested parties from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges;

(k) discussing the work undertaken in relation to cybersecurity exercises, including the work done by ENISA**;**

(ka) establish the peer-learning mechanism in accordance with Article 16 of this Directive.

5. The Cooperation Group may request from the CSIRT**s** network a technical report on selected topics.

6. By … 24 months after the date of entry into force of this Directive 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. The timeframe of the first programme adopted under this Directive shall be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148.

7. 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 37(2).

8. The Cooperation Group shall meet regularly and at least once a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to promote strategic cooperation and facilitate exchange of information.

Article 13

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 the national CSIRTs is established.

2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs designated in accordance with Article 9 and CERT–EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support cooperation among the CSIRTs.

3. The CSIRTs network shall have the following tasks:

(a) exchanging information on CSIRTs' capabilities;

(b) exchanging relevant information on incidents, near misses, cyber threats, risks and vulnerabilities;

(ba) exchanging information in regard to cybersecurity publications and recommendations;

(bb) sharing of technical solutions facilitating the technical handling of incidents;

(bc) exchanging best practices, tools and processes in regards to the tasks of the CSIRTs;

(c) at the request of a member of the CSIRTs network potentially affected by an incident, exchanging and discussing information in relation to that incident and associated cyber threats, risks and vulnerabilities

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

(e) providing Member States with support in addressing cross–border incidents pursuant to this Directive;

(f) cooperating, exchanging best practices and providing assistance to designated CSIRTs referred to in Article 6 with regard to the management of coordinated disclosure of vulnerabilities affecting multiple manufacturers or providers of ICT products, ICT services and ICT processes established in different Member States;

(g) discussing and identifying 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 modalities for coordination in response to cross–border risks and incidents;

(v) contribution to the national cybersecurity incident and crisis response plan referred to in Article 7 (3) at the request of a Member State;

(h) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (g), and, where necessary, requesting guidance in that regard;

(i) taking stock from cybersecurity exercises, including from those organised by ENISA;

(j) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT;

(k) cooperating and exchanging information, with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and threats across the Union;

(l) discussing the peer-~~review~~ learning reports referred to in Article 16(7);

(m) issuing 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. For the purpose of the review referred to in Article 35 and by □24 months after the date of entry into force of this Directive□, and every two years thereafter, the CSIRTs network shall assess the progress made with the operational cooperation and produce a report. The report shall, in particular, draw conclusions on the outcomes of the peer-learning referred to in Article 16 carried out in relation to national CSIRTs, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group.

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

6. The CSIRT network shall cooperate with the EU-CyCLONe on the basis of agreed procedural arrangements.

Article 14

The European cyber crises liaison organisation network (EU - CyCLONe)

1. In order to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of information among Member States and Union institutions, bodies and agencies, the European Cyber Crises Liaison Organisation Network (EU - CyCLONe) is hereby established.

2. EU-CyCLONe shall be composed of the representatives of Member States' cyber crisis management authorities designated in accordance with Article 7. The Commission shall participate in the activities of the network as an observer. ENISA shall provide the secretariat of the network 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.

3. EU-CyCLONe shall have the following tasks:

   (a) increasing the level of preparedness of the management of large scale cybersecurity incidents and crises;

   (b) developing a shared situational awareness for large scale cybersecurirty incidents and crisis;

   (ba) assessing the consequences and impact of relevant large scale cybersecurity incidents and proposing possible mitigation measures;

   (c) coordinating the management of large scale cybersecurity incidents and crisis and supporting decision-making at political level in relation to such incidents and crisis;

   (d) at a request of a Member State, discussing its national cybersecurity incident and

crisis response plans referred to in Article 7(3);

4. EU-CyCLONe shall adopt its rules of procedure.
5. EU-CyCLONe shall regularly report to the Cooperation Group on the management of large scale cybersecurity incidents and crisis management, focusing in particular on their impact on essential and important entities.
6. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements.
7. EU-CyCLONe shall submit to the European Parliament and the Council a report assessing its work by [24 months after the date of entering into force of this Directive].

Article 14a
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 some activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe, in accordance with Union law on data protection.

Article 15

Report on the state of cybersecurity in the Union

1. ENISA shall issue, in cooperation with the Commission and the Cooperation Group, a biennial report on the state of cybersecurity in the Union. In particular, the report shall include the following:
   (aa) a Union-level cybersecurity risk assessment, taking account of the threat landscape;
   (a) an assessment of the development of cybersecurity capabilities in the public and private sectors across the Union;
   (b)
   (c) an aggregated assessment based on cybersecurity quantitative and qualitative indicators, providing for an overview of the maturity level of cybersecurity capabilities, including sector-specific capabilities.
2. The report shall include particular policy recommendations for increasing the level of cybersecurity across the Union and a summary of the findings for the particular period from the Agency's EU Cybersecurity Technical Situation Reports issued by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.

Article 16

Peer-learnings

1. With a view to strengthening mutual trust, achieving a high common level of cybersecurity, as well as strengthening the Member States' cybersecurity capabilities and policies necessary for effectively implementing this Directive, the Cooperation Group shall establish, with the support of the Commission and after consulting ENISA, and, where relevant, the CSIRTs network, and at the latest by 24 months following the entry into force of this Directive, the methodology for an objective, non-discriminatory and fair peer learning system concerning the Member States' implementation of this Directive. Participation in the peer-learning is voluntary. The system shall consist of assessment rounds conducted by cybersecurity experts drawn from Member States and shall cover one or several of the following aspects:
   (i) the implementation of the cybersecurity risk management requirements and reporting obligations referred to in Articles 18 and 20;
   (ii) the capabilities, including the available resources, and the exercise of the tasks of the national competent authorities referred to in Article 8 and CSIRTs referred to in Article 9;
   (iii) the implementation of mutual assistance referred to in Article 34;
   (iv) the implementation of the information-sharing framework, referred to in Article 26.
2. The criteria based on which Member States are to designate experts eligible to participate in the peer-learning rounds shall be objective, non-discriminatory, fair and transparent and be included in the

methodology referred to in paragraph 1. ENISA and the Commission may designate experts to participate as observers in the peer-learning rounds.

3.

3a. Prior to the commencement of the peer-learning rounds, Member States may carry out a self-assessment of the aspects covered by that particular peer learning round and provide that self-assessment to the designated experts referred to in paragraph 2.

4. Peer-learnings may entail physical or virtual on-site visits and off-site exchanges. In view of the principle of good cooperation, the Member States taking part in the peer-learning shall provide the designated experts with the information necessary for the assessment, without prejudice to national or Union laws concerning protection of confidential or classified information or to safeguarding essential State functions, such as national security. Any information obtained through the peer-learning process shall be used solely for that purpose. The experts participating in the peer-learning shall not disclose any sensitive or confidential information obtained in that context to any third parties. The Member State participating in the peer-learning may object to the designation of particular experts on duly justified grounds communicated to the Cooperation Group.

5. Once subject to a peer-learning round, the same aspects shall not be subject to further peer-learning rounds for the participating Member States during the four years following the conclusion of that peer-learning round, unless the Member State concerned requests it or agrees upon proposal by the Cooperation Group.

6.

7. Experts participating in peer-leaning rounds shall draft reports on the findings and conclusions of the assessments. Member States shall be allowed to provide comments on their respective draft reports, which shall be attached to the report. The final reports shall be submitted to the Cooperation Group. Member States may decide to make their respective reports publicly available.

CHAPTER IV

Cybersecurity risk management and reporting obligations

SECTION I

Cybersecurity risk management and reporting

Article 17

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 18, oversee its implementation and can be held accountable for the non-compliance by the entities with the obligations under this Article.

   The application of this paragraph shall be without prejudice to the Member State's national laws as regards the liability rules in public institutions, as well as the liability of public servants and elected and appointed officials.

2. Member States shall ensure that the members of the management body are required to follow trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.

Article 18

Cybersecurity risk management measures

1a. This Directive applies an "all-hazard" approach that includes the protection of network and information systems and their physical environment from any event that could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of services offered by, or accessible via, network and information systems.

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network, and

information systems which those entities use in the provision of their services. Having regard to the state of the art and the cost of implementation, those measures shall ensure a level of security of network and information systems appropriate to the risk presented. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, its size, the likelihood of occurrence of incidents and their severity. Having regard of the level and type of the risk posed to society in the event of incidents affecting essential or important entities, cybersecurity risk management measures imposed on important entities may be less stringent than those imposed on essential entities.

2. The measures referred to in paragraph 1 shall include at least the following:
   (a) risk analysis and information system security policies;
   (b) incident handling (prevention, detection, ~~and~~ response and recovery from ~~to~~ incidents);
   (c) business continuity and crisis management;
   (d) supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers such as providers of data storage and processing services or managed security services;
   (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) policy on the use of ~~c~~ryptography and encryption;
   (ga) human resources security, access control policies and asset management.
3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities are required to 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, where considering appropriate measures referred to in point (d) of paragraph 2, entities are required to take into account the results of the coordinated risk assessments carried out in accordance with Article 19 (1).
4. Member States shall ensure that where an entity finds that respectively its services or tasks are not in compliance with the requirements laid down in paragraph 2, it shall, without undue delay, take all necessary corrective measures to bring the service concerned into compliance.
5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications, as well as sectoral specificities, as necessary, of the elements referred to in paragraph 2 of this Article. The Commission shall adopt by [18 months after the entry into force of this Directive] implementing acts in order to lay down the technical and the methodological specifications for entities referred to in Article 24(1) and trust service providers referred to in point 8 of Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2). When preparing such implementing acts, the Commission shall, to the greatest extent possible, follow international and European standards, as well as relevant technical specifications and exchange advice with the Cooperation Group and ENISA on the draft implementing act in accordance with Article 12(4)(d).
6.

Article 19

EU coordinated 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, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.
2. The Commission, after consulting with the Cooperation Group and ENISA, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.

Article 20

Reporting obligations

1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of these incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident. The act of the notification in itself shall not make the notifying entity subject to increased liability.
2. Where applicable, the essential and important entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The act of the notification in itself shall not make the notifying entity subject to increased liability.
3. An incident shall be considered significant if:
   (a) the incident has caused or has the potential to cause severe ~~substantial~~ operational disruption of the service or financial losses for the entity concerned;
   (b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.
4. Member States shall ensure that, for the purpose of the notification under paragraph 1, the entities concerned shall submit to the competent authorities or the CSIRT:
   (a) without undue delay and in any event within 24 hours after having become aware of the incident, an initial notification as an early warning, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;
   (b) upon the request of a competent authority or a CSIRT, an intermediate report on relevant status updates;
   (c) a final report not later than one month after the submission of the ~~report~~ initial notification under point (a), including at least the following:
      (i) a detailed description of the incident, its severity and impact;
      (ii) the type of threat or root cause that likely triggered the incident;
      (iii) applied and ongoing mitigation measures.

   Member States shall provide that in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines laid down in points (a) and (c). In particular, a deviation from the deadline referred to in point (c) can be justified in cases where the incident is still ongoing.
5. The competent national authorities or the CSIRT shall provide, without undue delay after receiving the initial notification referred to in point (a) of paragraph 4, a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures. Where the CSIRT did not receive the notification referred to in paragraph 1, the guidance shall be provided by the competent authority in collaboration with the CSIRT. The CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities.
6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority, the CSIRT or the Single Point of Contact shall inform the other affected Member States and ENISA of the incident. Such information shall include at least the elements provided for in paragraph (4) of this Article. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.
7. Where public awareness is necessary to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the competent authority or the

CSIRT, and where appropriate the authorities or the CSIRTs of other Member States concerned may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.

8. At the request of the competent authority or the CSIRT, 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 six months a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraph 1 and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report. ENISA shall inform every six months the Cooperation Group and the CSIRTs network about its findings on the notifications received.

10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with paragraphs 1 and 2 by essential entities identified as critical entities, [or as entities equivalent to critical entities,] pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].

11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraphs 1 and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

Article 21

Use of European cybersecurity certification schemes

1. In order to demonstrate compliance with certain requirements of Article 18 Member States may require entities to use particular ICT products, services and processes certified under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The ICT products, services and processes subject to certification may be developed by an essential or important entity or procured from third parties.

2. The Commission may adopt implementing acts specifying which categories of essential or important entities shall be required to use certain certified ICT products, services and processes or obtain a certificate under which European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2). When preparing such implementing acts, the Commission shall, in accordance with Article 56 of Regulation (EU) 2019/881:

   (i) take into account the impact of the measures on the manufacturers or providers of such ICT products, services or processes and on the users in terms of the cost of those measures and the societal or economic benefits stemming from the anticipated enhanced level of security for the targeted ICT products, services or processes as well as their alternative availability on the market;

   (ii) carry out an open, transparent and inclusive consultation process with all relevant stakeholders and Member States;

   (iii) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measures on the manufacturers, or providers of ICT products, services or processes, or users thereof, particularly SMEs;

   (iv) take into account the existence and implementation of relevant Member State laws.

3. The Commission may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme pursuant to Article 48(2) of Regulation (EU) 2019/881 in cases where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 of this Article is available.

Article 22

Standardisation

1. In order to promote the convergent implementation of Article 18(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 or internationally accepted standards and specifications relevant to the security of network and information systems.
2. ENISA, in collaboration with Member States, 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 Member States' national standards, which would allow for those areas to be covered.

Article 23

Databases of domain names and registration data

1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD name registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate, and complete domain name registration data in a dedicated database facility with due diligence in accordance with Union data protection law as regards data which are personal data.
2. Member States shall ensure that the databases of domain name registration data referred to in paragraph 1 contain relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs, including at least the following data:
   - **a)** domain name
   - **b)** date of registration
   - **c)** registrant data, including:
     - **(i)** for individuals - name, surname and e-mail address;
     - **(ii)** for legal persons - name and e-mail address.
3. Member States shall ensure that the TLD name registries and the entities providing domain name registration services for the TLD have policies and procedures in place to ensure that the databases include accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.
4. Member States shall ensure that the TLD name registries and the entities providing domain name registration services for the TLD publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.
5. Member States shall ensure that the TLD name registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that the TLD name registries and the entities providing domain name registration services for the TLD reply without undue delay and in any case within 72 hours to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

Section II

Jurisdiction and Registration

Article 24

Jurisdiction and territoriality

1a. Entities under this Directive shall be deemed to be under the jurisdiction of the Member State where they provide their services. Entities referred to in points 1 to 7 and 10 of Annex I, trust service providers and Internet Exchange Point providers referred to in point 8 of Annex I, and points 1 to 5 of Annex II shall be deemed under the jurisdiction of the Member State on the territory of which they are established.

1. DNS service providers, TLD name registries, and entities providing domain name registration services for the TLD, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, and managed security service providers referred to in point 8 and point 8a of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.
2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are predominantly taken. If the place where such decisions are predominantly taken cannot be determined or such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State where the entities have the establishment with the highest number of employees in the Union. Where the services are provided by a group of undertakings, the main establishment shall be deemed to be the main establishment of the group of undertakings.
3. If an entity referred to in paragraph 1 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 entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. In the absence of a designated representative within the Union under this Article, any Member State in which the entity provides services may take legal actions against the entity for non-compliance with the obligations under this Directive.
4. The designation of a representative by an entity referred to in paragraph 1 shall be without prejudice to legal actions, which could be initiated against the entity itself.

4a. Member States that have received a request for mutual assistance in relation to the entities referred to in paragraph 1, may, within the limits of the request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has the network and information system on their territory.

Article 25

Registry for certain digital infrastructure entities and digital providers

1. Member States shall ensure that the entities referred to in Article 24(1) having their main establishment on their territory, or, if not established in the Union, having their designated representative in the Union established on their territory are required to submit the following information to the competent authorities by [12 months after entering into force of the Directive at the latest]:
   (a) the name of the entity;
   (aa) the type of entity as per Annexes I and II to this Directive;
   (b) the address of its main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 24(3);
   (c) up-to-date contact details, including email addresses and telephone numbers of the entities and of their representatives;
   (d) Member States where the entity provides the service.

   Where applicable, this information shall be submitted through the national mechanisms of self-notification referred to in Article 2a.
2. Member States shall ensure that the entities referred to in paragraph 1 also notify any changes to the details they submitted under paragraph 1 without delay, and in any event, within three months from the date on which the change took effect.
3. The Member States' single points of contact shall forward the information referred to in paragraphs 1 and 2 to ENISA.

3a. Based on the information received according to paragraph 3 of this Article, ENISA shall create and maintain a registry for the entities referred to in paragraph 1. Upon request of Member States, ENISA shall enable access of relevant competent authorities to the registry, while ensuring the necessary guarantees to protect confidentiality of information where applicable.

4.

CHAPTER V
Information sharing

Article 26
Cybersecurity information-sharing arrangements

1. Member States shall ensure that essential and important entities may exchange on a voluntary basis relevant cybersecurity information among themselves including information relating to cyber threats, near misses, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools, where such information sharing:
   (a) aims at preventing, detecting, responding to or mitigating incidents;
   (b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection techniques, mitigation strategies, or response and recovery stages.
2. Member States shall ensure that the exchange of information takes place within communities of essential and important entities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared.
3. Member States may set out rules specifying the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. Such rules may also lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their policies referred to in Article 5(2) (g).
4. Essential and important entities shall notify the competent authorities of their participation in the 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 support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by providing best practices and guidance.

Article 27
Voluntary notification of relevant information

1. Without prejudice to Article 20, Member States shall ensure that essential and important entities may notify, on a voluntary basis, to the competent authorities or the CSIRTs any relevant incidents, cyber threats or near misses.
2. Member States shall ensure that, without prejudice to Article 3, entities falling outside the scope of this Directive may submit notifications, on a voluntary basis, of significant incidents, cyber threats or near misses. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Without prejudice to the investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.
3. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on the Member State concerned.

CHAPTER VI
Supervision and enforcement

Article 28
General aspects concerning supervision and enforcement

1. Member States shall ensure that competent authorities effectively monitor and take the measures

necessary to ensure compliance with this Directive, in particular the obligations laid down in Articles 18, 20 and 23. Member States may allow competent authorities to prioritise supervision, which shall be based on a risk-based approach.

2. Competent authorities shall work in close cooperation with data protection authorities, competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], supervisory bodies designated pursuant to Regulation (EU) 910/2014 and other competent authorities designated under sector-specific Union legal acts when addressing cybersecurity incidents.

3. 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 enforcement of potential sanctions for non-compliance, the competent authorities have the appropriate powers to conduct such tasks with operational independence vis-à-vis the entities supervised. Member States may decide on the imposition of appropriate, proportionate and effective measures of supervision and enforcement in relation to these entities in accordance with the national frameworks and legal order.

Article 29

Supervision and enforcement for essential entities

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

2. Member States shall ensure that competent authorities, where exercising their supervisory tasks in relation to essential entities, follow a risk-based approach and have the power to subject those entities at least to:

   (a) on-site inspections and off-site supervision, including random checks;

   (b) regular security audits;

   (c) targeted security audits based on risk assessments or risk-related available information;

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

   (e) requests of information necessary to assess the cybersecurity measures adopted by the entity, including documented cybersecurity policies;

   (f) requests to access data, documents or any information necessary for the performance of 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.

2a. Where exercising their supervisory tasks provided for in paragraph 2 of this Article, competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.

3. Where exercising their powers under points (e) to (g) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.

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

   (a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;

   (b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringements of the obligations laid down in this Directive;

   (c) order those entities to cease conduct that is non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;

   (d) order those entities to bring their risk management measures and/or reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;

   (e) order those entities to inform the natural or legal person(s) to whom they provide services or

activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;

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

(g)

(h) order those entities to make public aspects of non-compliance with the obligations laid down in this Directive in a specified manner, when such public disclosure does not lead to a harmful exposure of the respective entity;

(i)

(j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (i) of this paragraph, depending on the circumstances of each individual case.

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

(a) suspend or request a certification or authorisation body or courts according to national laws to suspend a certification or authorisation concerning part or all the services or activities provided by an essential entity;

(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.

These sanctions shall be applied only until the entity takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied.

The sanctions provided in this paragraph are not applicable to public administration entities subject to this Directive.

6. Member States shall ensure that any natural person responsible for or acting as a 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 powers to ensure its compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive. As regards public administration entities, this provision shall be without prejudice to the Member States' laws as regards the liability of public servants and elected and appointed officials.

7. Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 4 and 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. Among the infringements that should be considered as serious: repeated violations, failure to notify or remedy incidents with a significant disruptive effect, failure to remedy deficiencies following binding instructions from competent authorities obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement, providing false or grossly inaccurate information in relation to risk management requirements or reporting obligations set out in Articles 18 and 20.

(b) the duration of the infringement, including the element of repeated infringements;

(c) the actual damage caused or losses incurred or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this aspect, account shall be taken, amongst others of actual or potential financial or economic losses, effects on other services, number of users affected or potentially affected;

(d) the intentional or negligent character of the infringement;

(e) measures taken by the entity to prevent or mitigate the damage and/or losses;

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

(g) the level of cooperation of the natural or legal person(s) held responsible with the competent authorities.

8. The competent authorities shall set out a detailed reasoning for their enforcement decisions. Before taking such decisions, the competent authorities shall notify the entities concerned of their preliminary findings and allow a reasonable time for those entities to submit observations, unless in case of imminent danger.

9. Member States shall ensure that their competent authorities under this Directive inform the relevant competent authorities within that same Member State designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity identified as critical, [or as an entity equivalent to a critical entity], under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] with the obligations pursuant to this Directive. Where appropriate, competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], may request competent authorities under this Directive ~~may~~ to exercise their supervisory and enforcement powers in relation to an essential entity under the scope of this Directive that is also identified as critical [or equivalent] under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].

10. Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum pursuant to Article 29 (1) of Regulation (EU) XXXX/XXXX [DORA] when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity designated as critical ICT third-party service provider pursuant to Article 28 of Regulation (EU) XXXX/XXXX [DORA] with the obligations pursuant to this Directive.

10a. Member States shall ensure that their competent authorities under this Directive inform the relevant competent authorities designated pursuant to Regulation (EU) 910/2014 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an entity designated as trust service providers pursuant to Regulation (EU) 910/2014, with the obligations pursuant to this Directive.

Article 30

Supervision and enforcement for important entities

1. When provided with evidence or indication or information that an important entity is allegedly not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall ensure that the competent authorities take action, where necessary, through *ex post* supervisory measures.

2. Member States shall ensure that the competent authorities, where exercising their supervisory tasks in relation to important entities, follow a risk-based approach and have the power to subject those entities at least to:

(a) on-site inspections and off-site ex post supervision;

(b) targeted security audits based on risk assessments or risk-related available information;

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

(d) requests for any information necessary to assess ex-post the cybersecurity measures;

(e) requests to access data, documents and/or information necessary for the performance of the supervisory tasks;

(ea) 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.

2a. Where exercising their supervisory tasks provided for in paragraph 2 of this Article, competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.

3. Where exercising their powers pursuant to points (d) to (ea) of paragraph 2, the competent authorities shall state the purpose of the request and specify the information requested.

4. Member States shall ensure that the competent authorities, where exercising their enforcement powers

in relation to important entities, have the power at least to:

(a) issue warnings on the entities' non-compliance with the obligations laid down in this Directive;

(b) issue binding instructions or an order requiring those entities to remedy the deficiencies identified or the infringement of the obligations laid down in this Directive;

(c) order those entities to cease conduct that is in non-compliant with the obligations laid down in this Directive and desist from repeating that conduct;

(d) order those entities to bring their risk management measures or the reporting obligations in compliance with the obligations laid down in Articles 18 and 20 in a specified manner and within a specified period;

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

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

(g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner, when such public disclosure does not lead to a harmful exposure of the respective entity;

(h)

(i) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to, or instead of, the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.

5. Article 29 (6) to (8) shall also apply to the supervisory and enforcement measures provided for in this Article for important entities

Article 31

General conditions for imposing administrative fines on essential and important entities

1. Member States shall ensure that the imposition of administrative fines on essential and important entities pursuant to this Article in respect of infringements of the obligations laid down in this Directive are, in each individual case, effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a) to (h) of Article 30(4).

3. Where 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 29(7).

4. Member States shall ensure that infringements by the essential entities of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 4 000 000 EUR or, in the case of a legal person, 2% of the total worldwide annual turnover of the undertaking to which the essential entity belongs in the preceding financial year, whichever is higher.

4a. Member States shall ensure that infringements by the important entities of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least

2 000 000 EUR or, in the case of a legal person, 1% of the total worldwide annual turnover of the undertaking to which the important entity belongs in the preceding financial year, whichever is higher.

5. 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 in accordance with a prior decision of the competent authority.

6. Without prejudice to the powers of competent authorities pursuant to Articles 29 and 30, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities referred to in Article 4(23) subject to the obligations provided for by this

Directive.

6a. Where the legal system of the Member State does not provide for administrative fines, Member States shall ensure that this Article may be applied in such a manner that the fine is initiated by the competent authority and imposed by competent national courts, 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. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by […] and, without delay, any subsequent amendment law or amendment affecting them.

Article 32

Infringements entailing a personal data breach

1. Where, in the course of supervision or enforcement, the competent authorities have become aware that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 of this Directive may entails a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall, without undue delay, inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation.
2. Where the supervisory authorities competent in accordance with Articles 55 and 56 of Regulation (EU) 2016/679 decide to exercise their powers pursuant to Article 58(2)(i) of that Regulation and impose an administrative fine, the competent authorities referred to in Article 8 of this Directive shall not impose an administrative fine for an infringement by the same deed of Article 31 of this Directive. The competent authorities may, however, apply the enforcement actions or exercise the sanctioning powers provided for in points (a) to (i) of Article 29 (4), Article 29 (5), and points (a) to (h) of Article 30 (4) 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 may inform the supervisory authority established in the same Member State.

Article 33

Penalties

1. Member States shall lay down rules on penalties applicable to the infringements of national provisions 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.
2. Member States shall, by [two] years following the entry into force of this Directive, notify the Commission of those rules and of those measures and shall notify it, without undue delay of any subsequent amendment affecting them.

Article 34

Mutual assistance

1. Where an essential or important entity is providing services in more than one Member State, or is providing services in one or more Member States, but 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 the supervisory or enforcement measures;
   (c) a competent authority shall, upon receipt of a justified request from another competent authority, provide the other competent authority with assistance proportionate to the resources at its own disposal so that the supervision or enforcement actions can be implemented in an effective, efficient and consistent manner. Such mutual assistance 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 may not refuse that request unless, after an exchange with the other authorities concerned, it is established that ~~either~~ the authority is not competent to provide the requested assistance or does not have the necessary resources or the requested assistance is not proportionate to the supervisory tasks of the competent authority carried out or the request concerns information or entails activities which are in conflict with that Member State's national security or public security or defence.

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

CHAPTER VII

Transitional and final provisions

Article 35

Review

The Commission shall periodically 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 sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. For the purpose of the review, the Commission shall take into account the reports of the CSIRTs network on the experience gained at an operational level. The first report shall be submitted by… 54 months after the date of entry into force of this Directive.

~~Article 36~~

~~Exercise of the delegation~~

[Deleted in its entirety]

Article 37

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.
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.

Article 38

Transposition

1. By … 24 months after the date of entry into force of this Directive, Member States shall adopt and publish the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from … [one day after the date referred to in the first subparagraph].
2. When Member States adopt those measures, 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 39

Amendment of Regulation (EU) No 910/2014

In Regulation (EU) No 910/2014, Article 19 is deleted with effect from… [date of the transposition deadline of this Directive].

Article 40

Amendment of Directive (EU) 2018/1972

In Directive (EU) 2018/1972, Articles 40 and 41 are deleted with effect from… [date of the transposition deadline of this Directive].

Article 41

Repeal

Directive (EU) 2016/1148 is repealed with effect from.. [date of transposition deadline of the Directive]. References to Directive (EU) 2016/1148 shall be construed as references to this Directive and read in accordance with the correlation table set out in Annex III.

Article 42

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 43

Addressees

This Directive is addressed to the Member States. Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

---

27 Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

28 [insert the full title and OJ publication reference when known]

29 [deleted]

30 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).

31 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).

32 Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition off micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

33 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)(OJ L 151, 7.6.2019, p.15).

34 Regulation (EU) No 1025/2012 of the European Parliament and of the Council 25 October 2012 on European standardization, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/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).

35 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).

36 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).

37 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

38 [insert the full title and OJ publication reference when known]