Council of the European Union

Brussels, 12 October 2021
(OR. en)

12019/1/21
REV 1

LIMITE

CYBER 241
JAI 1005
DATAPROTECT 220
TELECOM 345
MI 687
CSC 320
CSCI 121
CODEC 1231

Interinstitutional File:
2020/0359(COD)

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	9583/2/21, 11724/21
No. Cion doc.:	14150/20
Subject:	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 - Presidency compromise proposal

Delegations will find in Annex the revised Presidency compromise proposal on the text of the NIS 2 Directive based on the written comments received from Member States. This proposal will be presented at the HWPCI meeting on 13 September 2021 (physical) and later discussed at the HWPCI meetings on 15 and 18 October 2021 (VTC). Delegations are invited to send their contributions by **Friday, 15 October 2021 COB.**

Most recent changes compared to the Commission proposal are indicated in **bold and underline** or ~~strikethrough.~~ All other changes are marked in **bold** or ~~strikethrough~~.

ANNEX

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

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

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

Acting in accordance with the ordinary legislative procedure,

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

Whereas:

(1) Directive (EU) 2016/1148 of the European Parliament and the Council[3] aimed at building cybersecurity capabilities across the Union, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the Union's economy and society to function effectively.

(2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national cybersecurity strategies, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group[4] and a network of national Computer Security Incident Response Teams ('CSIRTs network')[5]. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges.

---

[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1, 19.7.2016 p. 1).

[4] Article 11 of Directive (EU) 2016/1148.

[5] Article 12 of Directive (EU) 2016/1148.

(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence and cause major damage to the Union economy and society. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market.

(4) The legal basis of Directive (EU) 1148/2016 was Article 114 of the Treaty on the Functioning of the European Union (TFEU), the objective of which is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. The cybersecurity requirements imposed on entities providing services or economically relevant activities vary considerably among Member States in terms of type of requirement, their level of detail and the method of supervision. Those disparities entail additional costs and create difficulties for undertakings that offer goods or services cross-border. Requirements imposed by one Member State that are different from, or even in conflict with, those imposed by another Member State, may substantially affect those cross-border activities. Furthermore, the possibility of suboptimal design or implementation of cybersecurity ~~standards~~**measures** in one Member State is likely to have repercussions on the level of cybersecurity of other Member States, notably given the intense cross-border exchanges. The review of Directive (EU) 2016/1148 has shown a wide divergence in its implementation by Member States, including in relation to its scope, the delimitation of which was very largely left to the discretion of the Member States. Directive (EU) 2016/1148 also provided the Member States with very wide discretion as regards implementing the security and incident reporting obligations set out therein. Those obligations were therefore implemented in significantly different ways at national level. Similar divergence in the implementation occurred in relation to that Directive's provisions on supervision and enforcement.

(5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different ~~standards~~**measures**. This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.

(6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[6], are of relevance.

(6a) Union law on the protection of personal data and privacy applies to any processing of personal data under this Directive. In particular, this Directive is without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council and therefore should in particular not affect ~~notably~~ the tasks and powers of the independent supervisory authorities competent to monitor compliance with the respective Union data protection law.

(7) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy in light of the considerations set out in recitals (4) to (6). The sectors covered by Directive (EU) 2016/1148 should therefore be extended to provide a comprehensive coverage of the sectors and services of vital importance for key societal and economic activities within the internal market. The rules should not be different according to whether the entities are operators of essential services or digital service providers. That differentiation has proven obsolete, since it does not reflect the actual importance of the sectors or services for the societal and economic activities in the internal market.

---

6 The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).

(8) In accordance with Directive (EU) 2016/1148, Member States were responsible for determining which entities meet the criteria to qualify as operators of essential services ('identification process'). In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty for the risk management requirements and reporting obligations for all relevant entities, a uniform criterion should be established that determines the entities falling within the scope of application of this Directive. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[7], that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. ~~Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion.~~ **In order to ensure a clear overview of the entities falling within the scope of this Directive, Member States ~~should~~ can establish national ~~registration~~ mechanisms for self-notification ~~which can may require~~ requiring entities that meet this size-related criterion and to which this Directive applies to ~~register~~ notify with the competent ~~relevant~~ authorities under this Directive or bodies designated for that ~~is~~ purpose by the Member States. The mechanisms of self-notification ~~Those registries~~ should also include public administration entities to which this Directive applies. Self-notification should not be required where appropriate registers exist at national level, allowing for the identification of entities falling within the scope of this Directive.**

(9) **M**~~However, m~~**icro or** small ~~or micro~~ entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services, should also be covered by this Directive. Member States should be responsible for ~~establishing a list of such entities, and~~ submit**ting** ~~it~~ to the Commission **at least relevant information ~~relating to the list, including~~ on the number of identified entities, their type, ~~their size~~ and~~,~~ the specific criteria based on which they were identified. Member States can also ~~and, where~~ decide, where in accordance with national security rules, to submit to the Commission the names of ~~the entities~~ these entities.**

[7] 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).

(9a) Public administration entities that carry out activities in the areas of public security, law enforcement, as well as the judiciary and parliaments should be excluded from the scope of this Directive. For the purpose of this Directive, entities with regulatory competence encompassing enforcement and prosecution powers should not be considered as carrying out activities in the area of law enforcement. Therefore, they should not be excluded on these grounds from the scope of this Directive.

(9aa) Member States can establish that entities identified as operators of essential services in accordance with Directive (EU) 2016/1148 are considered essential entities.

(10) The Commission, in cooperation with the Cooperation Group, may issue guidelines on the implementation of the criteria applicable to micro and small enterprises.

(11) ~~Depending on the sector in which they operate or the type of service they provide, the entities falling within the scope of this Directive should be classified into two categories: essential and important. That categorisation should take into account the level of criticality of the sector or of the type of service, as well as the level of dependency of other sectors or types of services.~~ Both essential and important entities should be subject to the same risk management requirements and reporting obligations. The supervisory and penalty regimes between these two categories of entities should be differentiated to ensure a fair balance between **risk-based** requirements and obligations on one hand, and the administrative burden stemming from the supervision of compliance on the other hand.

(12) **This Directive sets out the baseline for cybersecurity risk management measures and reporting obligations across all sectors that fall within its scope. In order to avoid unnecessary fragmentation of cybersecurity provisions of Union legal acts, when additional sector-specific provisions pertaining to** cybersecurity risk management measures **and reporting obligations appear to be necessary to ensure a high level of cybersecurity, the Commission should assess whether such provisions could be stipulated in an implementing act under the empowerment provided for in this Directive. Should such acts not be suitable for that purpose,** sector-specific legislation **could** contribute to ensuring **a** high levels of cybersecurity, while taking full account of the specificities and complexities of ~~those~~ **the** sectors **concerned**. **At the same time, such sector-specific provisions of Union legal acts should duly take into account the need for a comprehensive and harmonised cybersecurity framework.** ~~This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications.~~ This ~~Directive~~ is without prejudice to the existing implementing powers that have been conferred ~~to~~ **on** the Commission in a number of sectors, including transport and energy.

(12a) Where a sector–specific Union legal act **contains provisions** requir**ing** essential or important entities to **adopt measures of at least equivalent effect to the obligations laid down in this Directive related to** cybersecurity risk management ~~measures~~ **and obligations** to notify **significant** incidents or significant cyber threats ~~of at least an equivalent effect to the obligations laid down in this Directive~~, those sector-specific provisions**, including on supervision and enforcement,** should apply. **When determining the equivalent effect of obligations set out in the sector-specific provisions of a Union legal act, the following aspects should be considered: (i) the cybersecurity risk management measures should consist of appropriate and proportionate ~~governance requirements and~~ technical and organisational measures to manage the risks posed to the security of network and information systems which the relevant entities use in the provision of their services, and should include as a minimum all the elements laid down in this Directive; (ii) the obligation to notify significant incidents and cyber threats should be at least equivalent to the obligations set out in this Directive as regards the content, format and timelines of the notifications; (iii) the reporting modalities by entities and the relevant ~~o~~ authorities of sector-specific Union legal acts should ~~(~~be at least equivalent ~~with~~ to ~~/reflect at the a minimum)~~ the requirements set out in this Directive as regards their content, format and timelines and should take into account the role of the CSIRTs; (iv) the cross-border cooperation requirements for the relevant authorities should be at least equivalent to those set out in this Directive. If the sector-specific provisions of a Union legal act do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive should continue to apply to the entities not covered by those sector-specific provisions.**

(12aa) The Commission **should periodically review the application of the equivalent effect requirement in relation to sector-specific provisions of Union legal acts and** ~~may~~ **can** issue guidelines **or recommendations** ~~**on necessary actions or measures to be taken by the competent authorities designated under sector-specific Union legal acts in order to address potential gaps in relation to this Directive**~~ **in this regard.** ~~in relation to the implementation of the lex specialis.~~ **The Commission is to consult the Cooperation Group when preparing the periodical review and developing those potential guidelines**, **recommendations** ~~**and**~~ **or measures**.

(12aa) Future sector-specific Union legal acts should take due account of the definitions outlined in Article 4 of this Directive.

(12ab) Where sector-specific provisions of Union legal acts require essential or important entities to adopt measures of at least equivalent effect to the reporting obligations laid down in this Directive, overlapping reporting obligations should be avoided, and coherence and effectiveness of handling of notifications of cyber threats or incidents should be ensured. For that purpose, those sector-specific provisions can allow Member States to establish a common, automatic and direct reporting mechanism for notifying significant incidents and cyber threats to both the authorities whose tasks are set out in the respective sector-specific provisions and the competent authorities, including the single point of contact and CSIRTs as appropriate, responsible for the cybersecurity tasks provided for in this Directive, or for a mechanism that ensures systematic and immediate sharing of information and cooperation among the relevant authorities and CSIRTs concerning the handling of such notifications. For the purposes of simplifying reporting and of implementing the common, automatic and direct reporting mechanism, Member States can utilise the single-entry point they establish according to Article 11(5a) of this Directive. To ensure harmonisation, reporting obligations of sector-specific Union legal acts should be aligned with those specified under this Directive.

(13) Regulation XXXX/XXXX of the European Parliament and of the Council should be considered to be a sector-specific Union legal act in relation to this Directive with regard to the financial sector entities. The provisions of Regulation XXXX/XXXX relating to information and communications technology (ICT) risk management measures, management of ICT-related incidents and notably incident reporting, as well as on digital operational resilience testing, information sharing arrangements and ICT third party risk should apply instead of those set ~~up~~ **out in** this Directive. Member States should therefore not apply the provisions of this Directive on cybersecurity risk management, ~~information sharing~~ and reporting obligations, and supervision and enforcement to ~~any~~ financial entities covered by Regulation XXXX/XXXX. At the same time, it is important to maintain a strong relationship and the exchange of information with the financial sector under this Directive. To that end, Regulation XXXX/XXXX allows ~~all financial supervisors,~~ the European Supervisory Authorities (ESAs) for the financial sector and the national competent authorities under Regulation XXXX/XXXX~~,~~ to participate in **the** ~~strategic policy discussions and technical~~ **work of** ~~workings~~ of the Cooperation Group, and to exchange information and cooperate with the single points of contact designated under this Directive**,** ~~and~~ **as well as** with the national CSIRTs. The competent authorities under Regulation XXXX/XXXX should transmit details of major ICT-related incidents **and significant cyber threats** also to the single points of contact **or the national CSIRTs** designated under this Directive. **This ~~can be achieved, for example,~~is achievable by automatic and direct forwarding of incident notifications or a common reporting platform.** Moreover, Member States should continue to include the financial sector in their cybersecurity strategies and national CSIRTs ~~may~~ **can** cover the financial sector in their activities.

(13a) In order to avoid gaps between and duplications of cybersecurity obligations imposed on entities in the aviation sector referred to in point 2 (a) of the Annex, national authorities designated under Regulations 300/2008, 2018/1139 ~~and this Directive~~ and competent authorities under this Directive should cooperate in relation to the implementation of cybersecurity risk management measures and the supervision of those measures at national level. The compliance of an entity with the cybersecurity risk management measures under this Directive can be considered by the national authorities designated under Regulations 300/2008 and 2018/1139 compliant with the requirements laid down in Regulations 300/2008 and 2018/1139, and Commission Implementing Regulations ~~2019/1583~~ and Delegated Acts based on Regulations 300/2008 and 2018/1139.

(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered **as** essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent authority under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on incidents, and cyber threats, and the exercise of supervisory tasks. **Competent a**~~A~~uthorities under both Directives should cooperate and exchange information, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents **as well as on non-cyber risks, threats and incidents** affecting critical entities or **entities equivalent to critical entities,** ~~as well as on~~ **including** the cybersecurity **and physical** measures taken by critical entities **and the results of supervisory activities carried out with regard to such entities. Furthermore, in order to streamline supervisory activities between the competent authorities designated under both directives and in order to minimise the administrative burden for the entities concerned, competent authorities should endeavour to** ~~**align**~~ **harmonise incident notification templates and supervisory processes.** ~~Upon request of 9583/2/21~~ **Where appropriate,** competent authorities under Directive (EU) XXX/XXX~~,~~ **can request** competent authorities under this Directive ~~should be allowed~~ to exercise their supervisory and enforcement powers ~~on~~ **in relation to** an essential entity identified as critical. ~~Both **Competent authorities under both Directives** should cooperate and exchange information for th**at** purpose.~~

(14a) Entities belonging to the digital infrastructure sector are in essence based on network and information systems and therefore the obligations imposed on those entities by this Directive should address in a comprehensive manner the physical security of such systems as part of their cybersecurity risk management and reporting obligations. Since those matters are covered by this Directive, the obligations laid down in Chapters III to VI of Directive (EU) XXX/XXX [CER] do not apply to such entities.

(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to ~~all~~ providers of DNS services along the DNS **provisioning and** resolution chain, **the entities providing domain name registration services, the** ~~including~~ operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers.

(16) Cloud computing services should cover services that allow on-demand and broad remote access to a scalable and elastic pool of shareable and distributed computing resources. Those computing resources include resources such as networks, servers or other infrastructure, operating systems, software, storage, applications and services. **The service models of cloud computing include Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), ~~and~~ Software-as-a-Service (SaaS) and Network as a Service (NaaS).** The deployment models of cloud computing should include private, community, public and hybrid cloud. The aforementioned service and deployment models have the same meaning as the terms of service and deployment models defined under ISO/IEC 17788:2014 standard. The capability of the cloud computing user to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the cloud computing service provider could be described as on-demand administration. The term 'broad remote access' is used to describe that the cloud capabilities are provided over the network and accessed through mechanisms promoting use of heterogeneous thin or thick client platforms (including mobile phones, tablets, laptops, workstations).

The term ‘scalable’ refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term ‘elastic pool’ is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term ‘shareable’ is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment. The term ‘distributed’ is used to describe those computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing.

(17) Given the emergence of innovative technologies and new business models, new cloud computing deployment and service models are expected to appear on the market in response to evolving customer needs. In that context, cloud computing services may be delivered in a highly distributed form, even closer to where data are being generated or collected, thus moving from the traditional model to a highly distributed one (‘edge computing’).

(18) Services offered by data centre service providers may not always be provided in a form of cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to the security of network and information systems, this Directive should cover also providers of such data centre services that are not cloud computing services. For the purpose of this Directive, the term ‘data centre service’ should cover provision of 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. The term ‘data centre service’ does not apply to in-house, corporate data centres owned and operated for own purposes of the concerned entity.

(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council[8], as well as express and courier delivery service providers, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain and in particular clearance, sorting or distribution, including pick-up services. Transport services that are not undertaken in conjunction with one of those steps should fall outside of the scope of postal services.

(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.

(21) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, Member States should be able to designate more than one national competent authority responsible for fulfilling the tasks linked to the security of the network and information systems of essential and important entities under this Directive. Member States should be able to assign this role to an existing authority.

---

[8] Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service (OJ L 15, 21.1.1998, p. 14).

(22) In order to facilitate cross-border cooperation and communication among authorities and to enable this Directive to be implemented effectively, it is necessary for each Member State to designate a national single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at Union level.

(23) **Without prejudice to the exchange of information in the CSIRTs network and CyCLONe, c**~~C~~ompetent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way, **also with a view to facilitate, where appropriate, a timely response to incidents** ~~**in accordance with Article 10(2c)**~~ **and to provide a response to the notifying entity** ~~**in accordance with Article 20(5).**~~ The single points of contact should be tasked with forwarding incident notifications to the single points of contact of other affected Member States. At the level of Member States' authorities, to ensure one single entry point in every Member States, the single points of contacts should also be the addressees of relevant information on **major ICT** incidents **and significant cyber threats** concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX. **For that purpose, Member States can determine that competent authorities under this Directive or national CSIRTs are the addressees of the notifications in accordance with Regulation EU [of Regulation XXX DORA].** ~~which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive~~.

(23a) The sector-specific Union legal acts which require cybersecurity risk management measures or reporting obligations of at least equivalent effect with those laid down in this Directive could provide that their designated competent authorities ~~a~~exercise their supervisory and enforcement powers in relation to such measures or obligations with the assistance of the competent authorities designated in accordance with this Directive. The competent authorities concerned could establish cooperation arrangements for this purpose. Such cooperation arrangements could specify, amongst others, the procedures concerning the coordination of supervisory activities, including the procedures of investigations and on-site inspections in accordance with the national law and a mechanism for the exchange of relevant information between competent authorities on supervision and enforcement~~cyber issues~~, including access to cyber-related information requested by competent authorities designated in accordance with this Directive.

(24) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ensure that they have well-functioning CSIRTs, also known as computer emergency response teams ('CERTs'), complying with essential requirements in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. In view of enhancing the trust relationship between the entities and the CSIRTs, in cases where a CSIRT is part of the competent authority, Member States should consider functional separation between the operational tasks provided by CSIRTs, notably in relation to information sharing and support to the entities, and the supervisory activities of competent authorities.

(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[9] as regards personal data, on behalf of and upon request by an entity under this Directive, a proactive scanning of the network and information systems used for the provision of their services. **Where applicable,** Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.

(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive. **CSIRTs should be able to exchange information, including personal data, with national ~~CERTs and~~ CSIRTs of third countries for the purpose of their tasks and~~.~~ in accordance with Regulation (EU) 2016/679. In particular, t~~T~~he exchange of ~~such~~ personal information that is deemed necessary for the purposes of mitigating significant cyber threats and responding to an ongoing significant incident could be considered an important reason of public interest within the meaning of Article 49 (1) (d) of Regulation (EU) 2016/679.**

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[10], a large-scale incident should mean 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. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.

(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop **or administer** such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third parties. In this regard, international standards ISO/IEC 30111 and ISO/IEC ~~29417~~ **29147** provide guidance on vulnerability handling and vulnerability disclosure respectively. As regards vulnerability disclosure, coordination between reporting entities and manufacturers or providers of ICT products or services is particularly important. Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to organisations in a manner allowing the organisation to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also comprise coordination between the reporting entity and the organisation as regards the timing of remediation and publication of vulnerabilities.

---

10 Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

(29) Member States should therefore take measures to facilitate coordinated vulnerability disclosure by establishing a relevant national policy. In this regard, Member States should designate a CSIRT to take the role of 'coordinator', acting as an intermediary between the reporting entities and the manufacturers or providers of ICT products or services where necessary. The tasks of the CSIRT coordinator should in particular include identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure timelines, and managing vulnerabilities that affect multiple organisations (multi-party **coordinated** vulnerability disclosure). Where **the reported** vulnerabilit**y could potentially have significant impact on entities** ~~ies affect multiple manufacturers or providers of ICT products or services established~~ in more than one Member State, the designated CSIRTs ~~from each of the affected Member States~~ should cooperate within the CSIRTs Network **where appropriate**.

(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. In that regard, sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability registry where, essential and important entities and their suppliers, as well as entities which do not fall in the scope of application of this Directive may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures.

(31) Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A European vulnerability registry maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with similar registries in third country jurisdictions. **In particular, ENISA should explore the possibility of a close cooperation with the operators of the Common Vulnerabilities and Exposures (CVE) system, including the possibility to become a root ~~Common Vulnerabilities and Exposures (~~CVE~~)~~ numbering authority.**

(32) **The Cooperation Group should continue to support and facilitate strategic cooperation and the exchange of information, as well as to develop trust and confidence among Member States.** The Cooperation Group should establish a work programme every two years including the actions to be undertaken by the Group to implement its objectives and tasks. The timeframe of the first programme adopted under this Directive should be aligned with the timeframe of the last programme adopted under Directive (EU) 2016/1148 in order to avoid potential disruptions in the work of the Group.

(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations to be addressed through better implementation of existing rules.

(34) The Cooperation Group should remain a flexible forum and be able to react to changing and new policy priorities and challenges while taking into account the availability of resources. It should organize regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges. In order to enhance cooperation at Union level, the Group should consider inviting Union bodies and agencies involved in cybersecurity policy, such as the European Cybercrime Centre (EC3), the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work.

(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes for officials from other Member States in order to improve cooperation. The competent authorities should take the necessary measures to enable officials from other Member States to play an effective role in the activities of the host competent authority.

(35a) The CSIRTs network should countinue to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States.

(36) The Union should, 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 and the CSIRTs network. Such agreements should ensure adequate protection of data

(36a) In order to facilitate the effective implementation of provisions of this Directive such as the management of vulnerabilities, capability assessments, cybersecurity risk management, reporting measures and information sharing arrangements, Member States may cooperate with third countries and undertake activities that are deemed appropriate for that purpose, including information exchanges on threats, incidents, vulnerabilities, tools and methods, tactics, techniques and procedures, cyber crisis management preparedness and exercises, training, trust building, structured information sharing arrangements and involvement in peer reviews and capability assessments. Such cooperation agreements should ~~take into account the need to ensure adequate protection of data~~comply with Union law on data protection.

(37) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework set out in Recommendation (EU) 2017/1584 through the existing cooperation networks, notably the **European** Cyber Crisis Liaison Organisation Network (EU-CyCLONe), CSIRTs network and the Cooperation Group. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements defining the modalities of that cooperation **and avoid any duplication of tasks** ~~**with the CSIRTs network or the Cooperation Group**~~. The EU-CyCLONe's rules of procedures should further specify the modalities through which the network should function, including but not limited to roles, cooperation modes, interactions with other relevant actors and templates for information sharing, as well as means of communication. For crisis management at **political** Union level, relevant parties should rely on the Integrated Political Crisis Response (IPCR) arrangements. The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for this purpose. If the crisis entails an important external or Common Security and Defence Policy (CSDP) dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) should be activated.

(37a) EU-CyCLONe should work as an intermediary network between the technical and political level during large scale cybersecurity incidents and crises. It should enhance cooperation ~~on~~ at operational level, building on CSIRTs network findings and using own capabilities ~~and~~ to create impact analysis of the large-scale incidents and crises and supporting decision–making at political level.

~~(38) For the purposes of this Directive, the term 'risk' should refer to the potential for loss or disruption caused by a cybersecurity incident and should be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of said incident.~~

~~(39) For the purposes of this Directive, the term 'near misses' should refer to an event which could potentially have caused harm, but was successfully prevented from fully transpiring.~~

(39a) Responsibilities in ensuring the security of network and information system lie, to a great extent, with essential and important entities. A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed.

(40) Risk-management measures should **take into account the degree of dependence of the entity on network and information systems and** include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data.

(40a) As threats to the security of network and information systems can have different origins, this Directive applies an "all-hazard" approach that includes the protection of network and information systems and their physical environment from any event such as theft, fire, flood, telecommunications or~~,~~ power failures or from any unauthorised physical access and damage to and interference with the organisation's information and information processing facilities that could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems. The risk management measures should therefore also address the physical and environmental security by including measures to protect the entity's network and information systems from system failures, human error, malicious actions or natural phenomena in line with European or internationally recognised standards, such as those included in the ISO 27000 series. In this regard, entities should, as part of their risk management measures, also address human resources security and have in place appropriate access control policies. Those measures should be coherent with Directive XXXX [CER Directive].

(41) In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the cybersecurity risk management requirements should be proportionate to the risk presented ~~by~~ **to** the network and information system concerned, taking into account the state of the art of such measures **and the cost for their implementation**. **Due account should also be taken of the size of the entity, as well as the likelihood of occurance of incidents and their severity.**

(41a) As large-sized entities may have more resources at their disposal, they can be required to implement more enhanced cybersecurity risk management measures as compared to medium-, small- or micro-sized entities. With a view to easing regulatory burdens, the requirements for the implementation of cybersecurity risk management measures for medium-, small- or micro-sized entities should in principle be lighter, unless criticality criteria or national risk assessments would justify stricter requirements, in particular with regard to entities that meet the criticality-related criteria set out in this Directive~~.~~.

(42) Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those are primarily private network and information systems managed by their internal IT staff or the security of which has been outsourced. The cybersecurity risk management and reporting requirements pursuant to this Directive should apply to the relevant essential and important entities regardless of whether they perform the maintenance of their network and information systems internally or outsource it.

(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.

(44) Among service providers, managed security services providers (MSSPs) in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to detect and respond to incidents. Those MSSPs have however also been the targets of cyberattacks themselves and through their close integration in the operations of operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP.

(44a) National competent authorities, in the context of their supervisory tasks, may also benefit from MSSP services such as security audits and penetration testing. To assist entities, as well as national competent authorities, in selecting skilled and trustworthy MSSPs, the Commission, with the assistance of the Cooperation Group and ENISA, should consider the possibility of establishing relevant EU certification schemes, where appropriate under the Regulation 2019/881.

(45) Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem. In particular, entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of the entities, when relying on data transformation and data analytics services from third parties, the entities should take all appropriate cybersecurity measures.

(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[11], with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities.

(47) The supply chain risk assessments, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5G networks security and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated risk assessment, the following criteria should be taken into account: (i) the extent to which essential and important entities use and rely on specific critical ICT services, systems or products; (ii) the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, systems or products; (iv) the resilience of the overall supply chain of ICT services, systems or products against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities.

---

[11] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

(48) In order to streamline the legal obligations imposed on providers of public electronic communications networks or publicly available electronic communications services, and trust service providers related to the security of their network and information systems, as well as to enable those entities and their respective competent authorities to benefit from the legal framework established by this Directive (including designation of CSIRT responsible for risk and incident handling, participation of competent authorities and bodies in the work of the Cooperation Group and the CSIRT network), they should be included in the scope of application of this Directive. The corresponding provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council[12] and Directive (EU) 2018/1972 of the European Parliament and of the Council[13] related to the imposition of security and notification requirement**s** on th**o**se types of entities should therefore be repealed.

(48a) The security obligations laid down in this Directive should be considered complementary to the requirements imposed on trust service providers under Regulation (EU) No 910/2014 (eIDAS Regulation). Member States may assign the role of competent authorities for trust services to the eIDAS supervisory bodies in order to ensure the continuation of current practices and to build on the knowledge and experience gained in the application of the eIDAS Regulation. Where that role is assigned to a different body, the national competent authorities under this Directive should 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].

---

12 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

13 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

Where applicable, the national competent authority under this Directive should immediately inform the eIDAS supervisory body about any notified significant cyber threat or incident with impact on trust services as well as about any non-compliance of a trust service provider with the requirements under this Directive. For the purposes of reporting, Member States may use, where applicable, the single-entry point established to achieve a common and automatic incident reporting to both the eIDAS supervisory body and the competent authority under this Directive. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council[14].

(49) Where appropriate and to avoid unnecessary disruption, existing national guidelines ~~and national legislation~~ adopted for the transposition of the rules related to security measures laid down in Article**s** 40~~(1)~~ and 41 of Directive (EU) 2018/1972~~, as well as of the requirements of Article 40(2) of that Directive concerning the parameters related to the significance of an incident, should continue to be used by the competent authorities in charge of supervision and enforcement for the purposes of this Directive~~ **should be taken into account in transposition arrangements implemented by the Member States in relation to this Directive, thereby building on the knowledge and skills already acquired under Directive (EU) 2018/1972 concerning security risk management measures and incident notifications. ENISA can also develop guidance on security and reporting requirements for providers of public electronic communication networks or publicly available electronic communication services to facilitate harmonisation, transition and minimise disruption. Member States can assign the role of competent authorities for electronic communications to the national regulatory authorities in order to ensure the continuation of current practices and to build on the knowledge and experience gained in Directive (EU) 2018/1972.**

---

14 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

(50) Given the growing importance of number-independent interpersonal communications services, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. Providers of such services should thus also ensure a level of security of network and information systems appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission.

(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents in relation thereto.

(52) Where appropriate, entities should inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves. The requirement to inform those recipients of such threats should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats to the recipients should be free of charge.

~~**(52a) When adopting implementing acts on the significance of the cyber threat in accordance with this Directive, the Commission should take into account the severity and technical characteristics of the threat, as well as its potential cross-sectorial spillover effects.**~~

(53) In particular, providers of public electronic communications networks or publicly available electronic communications services, should inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their communications, for instance by using specific types of software or encryption technologies.

(54) In order to safeguard the security of electronic communications networks and services, the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory for providers of such services and networks in accordance with the principles of security and privacy by default and by design for the purposes of Article 18. The use of end-to-end encryption should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime.

(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within 24 hours, followed by a final report not later than one month after. The initial notification should only include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines of 24 hours for the initial notification and one month for the final report.

(56) Essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. In view of this and, for the purposes of simplifying the reporting of security incidents, Member States should establish *a single entry point* for all notifications required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. ENISA, in cooperation with the Cooperation Group should develop common notification templates by means of guidelines that would simplify and streamline the reporting information requested by Union law and decrease the burdens for companies.

(57) Where it is suspected that an incident is related to serious criminal activities under Union or national law, Member States should encourage essential and important entities, on the basis of applicable criminal proceedings rules in compliance with Union law, to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, and without prejudice to the personal data protection rules applying to Europol, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the EC3 and ENISA.

(58) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities should cooperate and exchange information on all relevant matters with data protection authorities and the supervisory authorities pursuant to Directive 2002/58/EC.

(59) Maintaining accurate**, verified** and complete databases of domain names and registration data (so called 'WHOIS data') and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law.

(60) The availability and timely accessibility of these data to public authorities, including competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs, (CSIRTs, and as regards the data of their clients to providers of electronic communications networks and services and providers of cybersecurity technologies and services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents. Such access should comply with Union data protection law insofar as it is related to personal data.

(61) In order to ensure the availability of accurate**, verified** and complete domain name registration data, TLD registries and the entities providing domain name registration services for the TLD (so-called registrars) should collect and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules.

(62) TLD registries and the entities providing domain name registration services for them should make publically available domain name registration data that fall outside the scope of Union data protection rules, such as data that concern legal persons[15]. TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and the entities providing domain name registration services for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. **Member States should ensure that all type of access to domain registration data (both personal and non-personal data) are ~~should be~~ free of charge.** With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board.

---

15 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL recital (14) whereby "this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person".

(63) All essential and important entities under this Directive should fall under the jurisdiction of the Member State where they provide their services. If the entity provides services in more than one Member State, it should fall under the separate and concurrent jurisdiction of each of these Member States. The competent authorities of these Member States should cooperate, provide mutual assistance to each other and where appropriate, carry out joint supervisory actions.

(64) In order to take account of the cross-border nature of the services and operations of DNS service providers, TLD name registries, **entities providing domain name registration services for the TLD,** content delivery network providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. Whether this criterion is fulfilled should not depend on whether the network and information systems are physically located in a given place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not decisive criteria for determining the main establishment. The main establishment should be the place where the decisions related to the cybersecurity risk management measures are **predominantly** taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If **the place where such decisions are predominantly taken cannot be determined or** such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where the entity has an establishment with the highest number of employees in the Union. Where the services are carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings.

(64a) In order to ensure a clear overview of DNS service providers, TLD name registries, entities providing domain name registration services for the TLD, content delivery network providers, cloud computing service providers, data centre service providers and digital providers providing services across the Union under the scope of this Directive, ENISA should create and maintain a registry for such entities, based on notifications received by Member States through their national mechanisms for self-notification. With a view to ensure accuracy and completeness of the information that should be included in this registry, Member States should ~~consider~~ submit~~ting~~ to ENISA, without undue delay, the information available in their national registries on these ~~same type of~~ entities. ENISA and the Member States should take measures to facilitate the interoperability of such registries, while ensuring protection of confidential or classified information.

(65) In cases where a DNS service provider, TLD name registry, content delivery network provider, cloud computing service provider, data centre service provider and digital provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such an entity is offering services within the Union, it should be ascertained whether it is apparent that the entity is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the entity's or an intermediary's website or of an email address and of other contact details, or the use of a language generally used in the third country where the entity is established, is as such insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the entity is planning to offer services within the Union. The representative should act on behalf of the entity and it should be possible for competent authorities or the CSIRTs to contact the representative. The representative should be explicitly designated by a written mandate of the entity to act on the latter's behalf with regard to the latter's obligations under this Directive, including incident reporting.

(66) Where information considered classified according to national or Union law is exchanged, reported or otherwise shared under the provisions of this Directive, the corresponding specific rules on the handling of classified information should be applied.

(67) With cyber threats becoming more complex and sophisticated, good detection and prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing between entities. Information sharing contributes to increased awareness on cyber threats, which, in turn, enhances the entities' capacity to prevent threats from materialising into real incidents and enables the entities to better contain the effects of incidents and recover more efficiently. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, notably uncertainty over the compatibility with competition and liability rules.

(68) Entities should be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules.

(69) ~~The processing of personal data, t~~**T**o the extent strictly necessary and proportionate for the purposes of ensuring network and information security**, the processing of personal data** by **essential and important** entities, ~~public authorities, CERTs, CSIRTs,~~ and providers of security technologies and services **could be considered necessary for compliance with a legal obligation or** ~~should~~ constitute a legitimate interest of the data controller concerned~~.~~, as referred to in Regulation (EU) 2016/679. That **could** ~~should~~ include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, ~~as well as~~ cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of ~~the following~~ **various** types of personal data**, such as**: IP addresses, uniform resources locators (URLs), domain names, and email addresses. **Processing of personal data by competent authorities, SPOCs and CSIRTs should be laid down in national law and considered necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, as referred to in Article 6(1) point (c) or (e) of Regulation (EU) 2016/679.**

(69a) Member States' laws may lay down rules allowing c~~C~~ompetent authorities, SPOCs and CSIRTs~~ can~~, to the extent that is strictly necessary and proportionate for the purpose of ensuring the security of network and information systems of essential and important entities, to process special categories of personal data in accordance with Article 9(1) of Regulation (EU) 2016/679, in particular by providing for suitable and specific measures to safeguard the fundamental rights and interests of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

(70) In order to strengthen the supervisory powers and actions that help ensure effective compliance, this Directive should provide for a minimum list of supervisory actions and means through which competent authorities **can** ~~may~~ supervise essential and important entities. In addition, this Directive should establish a differentiation of supervisory regime between essential and important entities with a view to ensuring a fair balance of obligations for both entities and competent authorities. Thus, essential entities should be subject to a fully-fledged supervisory regime (*ex-ante* and *ex-post*), while important entities should be subject to a light supervisory regime, *ex-post* only. For the latter, this means that important entities should not **be required to** ~~document~~ systematically **document** compliance with cybersecurity risk management requirements, while competent authorities should implement a reactive *ex -post* approach to supervision and, hence, not have a general obligation to supervise those entities. **For important entities, *ex-post* supervision may be triggered by evidence or any indication or information brought to the attention of competent authorities deemed by these authorities as suggesting potential non-compliance with the obligations laid down in this Directive. For example, such evidence, indication or information could be of the type provided to competent authorities by other authorities, entities, citizens, media or other sources, publicly available information, or may emerge from other activities conducted by the competent authorities in the fulfilment of their tasks.**

(70bis) In the exercise of *ex-ante* supervision, competent authorities should be able to decide on the prioritisation of the use of supervisory actions and means at their disposal in a proportionate manner. This entails that competent authorities can decide on such prioritisation based on supervisory methodologies which should follow a risk-based approach. More specifically, such methodologies could include criteria or benchmarks for the classification of essential entities into risk categories and corresponding supervisory actions and means recommended per risk category, such as use, frequency or type of on-site inspections or targeted security audits or security scans, type of information to be requested and level of detail of that information. Such supervisory methodologies can also be accompanied by work programmes and be assessed and reviewed regularly, including on aspects such as resource allocation and needs.

(71) In order to make enforcement effective, a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations provided by this Directive should be laid down, setting up a clear and consistent framework for such sanctions across the Union. Due regard should be given to the nature, gravity and duration of the infringement, the actual damage caused or losses incurred or potential damage or losses that could have been triggered, the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered, the degree of responsibility or any relevant previous infringements, the degree of cooperation with the competent authority and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection and due process.

(72) In order to ensure effective enforcement of the obligations laid down in this Directive, each competent authority should have the power to impose or request the imposition of administrative fines.

(73) Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine does not affect the application of other powers by the competent authorities or of other penalties laid down in the national rules transposing this Directive.

(74) Member States should be able to lay down the rules on criminal penalties for infringements of the national rules transposing this Directive. However, the imposition of criminal penalties for infringements of such national rules and of related administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

(75) Where this Directive does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of the obligations laid down in this Directive, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity and the imposition of a temporary ban from the exercise of managerial functions by a natural person. Given their severity and impact on the entities' activities and ultimately on their consumers, such sanctions should only be applied proportionally to the severity of the infringement and taking account of the specific circumstances of each case, including the intentional or negligent character of the infringement, actions taken to prevent or mitigate the damage and/or losses suffered. Such sanctions should only be applied as ultima ratio, meaning only after the other relevant enforcement actions laid down by this Directive have been exhausted, and only for the time until the entities to which they apply take the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. The imposition of such sanctions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter of Fundamental Rights of the European Union, including effective judicial protection, due process, presumption of innocence and right of defence.

(77) This Directive should establish cooperation rules between the competent authorities and the supervisory authorities in accordance with Regulation (EU) 2016/679 to deal with infringements related to personal data.

(78) This Directive should aim at ensuring a high level of responsibility for the cybersecurity risk management measures and reporting obligations at the level of the organisations. For these reasons, the management bodies of the entities falling within the scope of this Directive should approve the cybersecurity risk measures and supervise their implementation.

(79) A peer-review mechanism should be introduced **to help ~~build~~ strengthen mutual trust and learn from good practices and ~~challanges~~ experiences**, allowing the ~~assessment~~ **analysis** by experts designated by the Member States of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources. **When implementing the peer-review mechanism, particular consideration should be given to ensure that it does not place unnecessary or disproportionate burden on the relevant Member States' authorities. Furthermore, the mechanism should take account of the results of similar mechanisms, such as the peer-review system of the CSIRTs network, add value and avoid duplication. The implementation of the mechanism should be without prejudice to national and Union laws on protection of confidential and classified information. Prior to the commencement of the peer-review process, Member States can carry out a self-assessment of the reviewed aspects. Upon request from the Cooperation Group, the Commission, supported by ENISA, can provide guidance on the self assessment and relevant templates, where necessary. The publication of the peer review reports should be conditional of the consent of the ~~reviewed~~ Member State concerned~~s~~. ~~A~~ That ~~reviewed~~ Member State can refuse publication for national or public security considerations or in duly justified cases when the publication of such report is deemed to affect the protection of confidential or classified information. A ~~reviewed~~ Member State ~~could~~ can agree to the publication of a non-confidential version of ~~the~~ its respective peer-review report.**

~~(80) In order to take account of new cyber threats, technological developments or sectorial specificities, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the elements in relation to risk management measures required by this Directive. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making1 . In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.~~

(81) In order to ensure uniform conditions for the implementation of the relevant provisions of this Directive concerning the procedural arrangements necessary for the functioning of the Cooperation Group, the technical elements related to risk management measures or the type of information, the format and the procedure of incident notifications**, the significance of cyber threats, as well as the categories of entities that are to be required to use certain certified ICT products, services and processes ~~or obtain a certificate~~**, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.[16]

(82) The Commission should periodically review this Directive, in consultation with interested parties, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions.

---

[16] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

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

(84) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles,

HAVE ADOPTED THIS DIRECTIVE:

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 ~~as essential entities~~ in **the** Annex ~~I and important entities in **the** Annex I~~;

   (c) ~~**provides the a legal basis for and**~~ lays down **rules and** obligations on cybersecurity information sharing.

Article 2

Scope

1. This Directive applies to public and private entities of the type**s** ~~reffered to as~~ provided for in the Annex ~~I and as important entities in Annex II~~. This Directive does not apply to entities that qualify as micro **or** ~~and~~ small enterprises within the meaning of Commission Recommendation 2003/361/EC[17]. **Article 3 4 of the~~ate~~ Annex to ~~the~~ that Recommendation shall not apply.**

1a. Member States may ~~shall~~ establish national ~~registration~~ notification ~~mechanisms~~ for self-notification ~~which may~~ requiring all entities ~~of a type referred to as essential entities in the Annex~~ under the scope of this Directive ~~to which this Directive applies~~ to notify ~~register with~~ the competent ~~relevant~~ authorities under this Directive or bodies designated for this purpose by the Member States at the latest [6 months after the transposition deadline]. ~~Member States shall also include in these registries the public administration entities to which this Directive applies, in line with the definition and criteria provided for in Article 4(23) of this Directive and point 9 of the Annex to this Directive.~~

2. R~~However, r~~egardless of the~~ir~~ size **of the entities referred to in paragraph 1**, this Directive also applies to **the following** entities referred to in the Annex~~es I and II, 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 **the** Annex ~~I~~;

(ii) **qualified trust service providers referred to in point XX of the Annex;**

(iii) **non-qualified trust service providers ~~as~~ referred to in point XX of the Annex;**

(iv) top–level domain name registries ~~and domain name system (DNS)~~ referred to in point 8 of **the** Annex ~~I~~;

---

17 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).

(b) the entity is a public administration entity as defined in ~~point 23 of~~ Article 4**(23)**;

(c) the entity is the sole provider **in a Member State** of a service ~~in a Member State~~ **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 a~~n~~ **significant** impact on public safety, public security or public health;

(e) a potential disruption of the service provided by the entity could induce an **significant** systemic risks, in particular for the sectors where such disruption could have a cross-border impact;

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

(g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council[18] [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive.

Member States shall ~~establish a list of entities identified pursuant to point (b) (c) to (f) and~~ submit to the Commission **in relation to entities identified pursuant to point (b) to (e) at least relevant information ~~relating to the list, including~~on the number of identified entities, the sector they belong to or type of service they provide ~~ir type~~ as per the Annex, ~~their size~~ and ~~,~~ the specific provision(s) of Article 2(2) based on which they were identified by ~~and, where in accordance with national security rules, the names of the entities by~~ [6 months after the transposition deadline of this Directive].** ~~-~~Member States shall review ~~the list~~**this information**~~,~~ on a regular basis, and at least every two years thereafter and, where appropriate, update it.

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

2a. Entities of a type provided for in the Annex to this Directive which exceed the ceilings for medium-sized enterprises as defined in Commission Recommendation 2003/361/EC, as well as entities referred to in Article 2(2), points (a) ~~(i)~~, (ii) and (iv) and Article 2(2), points (b) and (g), of this Directive shall be considered essential entities.

2b. Entities of the type provided for in the Annex to this Directive which qualify as medium-sized ~~entreprises~~enterprises within the meaning of Commission Recommendation 2003/361/EC as well small and micro entities referred to in Article 2(2)(iii) and Article 2(2)(c) to (e~~f~~) shall be considered important entities. Member States may however establish, based on the criticality criteria referred to in Article 2(2)(c) to (e~~f~~), that medium-sized enterprises within the meaning of Commission Recommendation 2003/361/EC are essential entities. Member States may also establish that, based on ~~specific~~ national risk assessments, certain micro or small-sized entities within the meaning of Commission Recommendation 2003/361/EC identified pursuant to paragraph (2) points (c~~b~~) to (e~~f~~) of this article, are essential entities.

3. ~~This Directive is without prejudice to actions taken by the Member States and their responsibilities and their relevant competences in relation to safeguarding their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. These Such actions include activities, irrespective whether conducted by public entities or by private entities on behalf of public authorities, concerning the maintenance safeguarding of public security, defence and national security and activities in areas of criminal law, including the protection of information the disclosure of which Member states is consider contrary to the Member States' essential interests of their national security or defence, in compliance with Union law. Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security, as well as the judiciary and parliaments shall be excluded from of the scope of this Directive.~~ **This Directive is without prejudice to the responsibility of Member States to safeguard national security or to protect other essential State functions, in accordance with Union law.**

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 and defence, regardless of which entity is carrying out those activities and whether it is a public entity or a private entity acting at the request of a public entity;

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

This Directive shall be without prejudice to actions taken by Member States for the protection of information the disclosure of which is contrary to their essential interests of national security, public security or defence, in compliance with Union law.

3a. 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.

4. This Directive applies without prejudice to Council Directive 2008/114/EC[19] and Directives 2011/93/EU[20] and 2013/40/EU[21] of the European Parliament and of the Council.

---

19 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

20 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).

21 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).

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 2a

Sector-specific Union acts

1. ~~6.~~ Where ~~provisions of~~ sector–specific **Union legal** acts ~~of Union law~~ require essential or important entities ~~either~~ to adopt cybersecurity risk management measures or to notify **significant** incidents or ~~significant~~ 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 ~~above~~ in ~~this~~ paragraph 1 of this article shall be considered equivalent in effect to the obligations laid down in this Directive if:

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

(b) requirements to notify significant incidents and cyber threats are at least ~~, at a minimum,~~ equivalent in effect to those laid down in Article 20 (1) to ~~(4)~~ (6) and ~~include~~provide for ~~,~~

~~(i) where appropriate, automatic and direct~~ immediate access, where appropriate automatic and direct, to the incident notifications by the competent authorities under this Directive or the designated CSIRTs.

3. ~~6a.~~ The Commission shall periodically review the application of the equivalent effect requirement in paragraph 6 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, in accordance with this Directive, adopt or maintain provisions ensuring a higher level of cybersecurity.

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** compromise~~s~~ 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[22];

[22] 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).

(4) 'national **cybersecurity** strategy ~~on cybersecurity'~~ means a coherent framework of a Member State providing a governance to achieve strategic objectives and priorities **in the area of**~~on~~ **cybersecurity** ~~the security of network and information systems~~ 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 ~~related~~ services offered by, or accessible via, network and information systems;

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

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

(8a) 'near misses' means an event that could potentially have caused harm, 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 **the** 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[23];

(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** ~~to~~ **third-party usage** ~~internet end-users and other DNS service providers~~;

(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**;

---

23 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).

(15a) 'entities providing domain name registration services for the TLD' means TLD 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 [24];

(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[25];

(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[26];

(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 and distributed computing resources;

---

24 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).

25 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).

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

(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;

(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 in a Member State 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 **own** 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.

In accordance with the conditions laid down in Article 2(3), public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security**, as well as the judiciary and parliaments** are excluded. **Where public administration entities carry out activities in these areas only as part of their overall activities, they shall be excluded in their entirety**.

(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 ~~referred to as an essential entity in Annex I~~ **provided for in the Annex and designated as 'essential' in accordance with Article 2(2a)**;

(26) 'important entity' means any entity of the type ~~referred to as an essential entity in Annex II~~ **provided for in the Annex and designated 'important' in accordance with Article 2 (2b)**.

(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.

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) ~~a definition of~~ 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 ~~public bodies and entities as well as other relevant actors~~;

   (c) an assessment to identify relevant assets and 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) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;~~

(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[27] [Resilience of Critical Entities Directive] for the purposes of information sharing on **cybersecurity risks,** ~~incidents and~~ 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 ~~essential and important~~ entities for the provision of their services;

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

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

(d) a policy related to sustaining the general availability**,** ~~and~~ 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;

---

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

(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** ~~specific information from the notification where and to the extent that it is strictly necessary to preserve~~ national security.

4. Member States shall assess their national cybersecurity strategies on a regular basis and at least every ~~four~~ **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 and the manufacturer or provider of ICT products or ICT services. Where the reported vulnerability ~~concerns multiple manufacturers or providers of ICT products or ICT services across the Union~~ **could potentially have significant impact on entities in more than one Member State** , the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.

2. ENISA shall develop and maintain a European vulnerability registry. 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 ~~its~~ 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 ~~interested~~ 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 communicate to the Commission 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 ~~as referred to in paragraph 3~~ within three months from that designation and the adoption of those plans. Member States may exclude specific information from the plan where and to the extent that it is strictly necessary for their national security.

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 **the** 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).

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 reviews 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 **the** 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 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, upon request of an **essential or important** entity, a proactive scanning of the network and information systems used for the provision of their services;

(f) participating in the CSIRTs network and providing mutual assistance to other members of the network upon their request.

(fa) where applicable, acting as a coordinator for the purpose of coordinated vulnerability disclosure pursuant to Article 6 (1) that shall include in particular facilitating the interaction between the reporting entities and the manufacturer or provider of ICT products or ICT services in cases where this is necessery, identifying and contacting concerned entities, supporting reporting entities, negotiating disclosure time lines and managing vulnerabilities that affect multple 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 CERTs and 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** ~~responsible for critical infrastructure~~ 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,** ~~and~~ 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** ~~provide~~ information ~~to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]~~ on t**he 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 ~~by competent authorities~~ in response to those risks and incidents. **Member States shall also ensure that competent authorities under this Directive** ~~regularly exchange relevant information with~~ **and the competent authorities designated under Regulation (XXXX/XXXX)[DORA Regulation], Directive 2018/1972 and Regulation (EU) 910/2014 regularly exchange relevant information~~.~~.**

5a. For the purpose~~s~~ of simplifying the reporting of incidents, Member States ~~shall~~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 integrate notifications required under other sector-specific Union legal acts in the single-entry-point. 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** ~~and~~ **to strengthen** ~~develop~~ **trust and confidence** ~~in the field of application of the Directive~~, a Cooperation Group is established.

1a. The Cooperation Group established in accordance with Directive (EU) 2016/1148 shall be considered the Cooperation Group within the meaning of this Directive.

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) in accordance with Article 17(5) **point** (c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group.

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;

(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 ~~or delegated~~ 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 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 cyber 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**;**

(l) establish the peer review mechanism in accordance with Article 16 of this Directive.

5. The Cooperation Group may request from the CSIRT 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.

1a. The CSIRT Network established in accordance with Directive (EU) 2016/1148 shall be considered the CSIRT Network within the meaning of this Directive.

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;

(c) at the request of a representative of the CSIRT 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 representative of the CSIRT 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 ~~multiparty~~ 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);

(h) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (g), 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 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 reviews 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.

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**, the CERT-EU** and ENISA. ENISA shall provide the secretariat of the network and support the secure exchange of information **as well as provide necessery tools to support cooperation between Member States ensuring secure exchange of information.**

3. EU-CyCLONe shall have the following tasks:

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

   (b) developing a shared situational awareness of incidents that could be relevant for large scale cybersecuirty 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 ~~management~~ and supporting decision-making at political level in relation to such incidents and crisis;

   (d) **at a request of a Member State,** discussing national cybersecurity incident and **crisis** response plans referred to in Article 7(**3**~~2~~)**;**~~.~~

   (da) discussing and identifying further forms of cooperation such as mutual assitance in the event of large scale cybersecurity incidents and crisis where appropriate.

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**~~cyber threats, incidents and trends~~, 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 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, t**~~T~~he report shall ~~in particular~~ include ~~an assessment of~~ the following:

(aa) an~~a~~ **Union-level** ~~**strategic level EU**~~ **cybersecurity risk assessment, taking account of the threat landscape**~~**assessment,**~~ **;**

(a) ~~the~~ **an assessment of the** development of cybersecurity capabilities in the public and private sector across the Union;

(b) **an**~~the~~ **assessment of the** technical, financial and human resources available to competent authorities and cybersecurity policies, and the implementation of supervisory measures and enforcement actions**, taking also account, where possible,** ~~in light of~~ the outcomes of peer reviews referred to in Article 16 **and the mutual assistance provided on the basis of Article 34 of this Directive**;

(c) ~~a~~ **an aggregated assessment based on** cybersecurity ~~index~~ **quantitative and qualitative indicators,** providing for an ~~aggregated assessment~~ **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-reviews

1. **With a view to ~~building~~ strengthening mutual trust, achieving a high common level of cybersecurity and strengthening the Member States' cybersecurity capabilities and policies necessary for effectively implementing this Directive, t~~T~~he Cooperation Group~~Commission~~** shall establish, **with the support of the Commissiona and** after consulting ~~the Cooperation Group and~~ ENISA ~~and **upon endorsement by the Cooperation Group**~~, and at the latest by 18 months following the entry into force of this Directive, the methodology ~~and content of~~ for a**n objective, non-discriminatory and fair** peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. The reviews shall be conducted by cybersecurity ~~technical~~ experts drawn from Member States different than the one reviewed and shall cover ~~at least~~ the following aspects:

   (i) the effectiveness of the implementation of the cybersecurity risk management requirements and reporting obligations referred to in Articles 18 and 20;

   (ii) the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the national competent authorities **referred to in Article 8**;

   (iii) the operational capabilities and effectiveness of CSIRTs**, taking account of the peer review system of the CSIRTs network**;

   (iv) the effectiveness of mutual assistance referred to in Article 34;

   (v) the effectiveness of the information-sharing framework, referred to in Article 26 of this Directive.

2. **The criteria based on which Member States are to designate experts eligible to carry out the peer-reviews, as well as the system for the selection and the random allocation of these experts for each peer-review~~, shall be~~** ~~The methodology shall include~~ objective, non-discriminatory, fair and transparent ~~criteria on the basis of which the Member States shall designate experts eligible to carry out the peer reviews~~**and shall be included in the methodology referred to in paragraph 1 of this Article**. ENISA and the Commission shall designate experts to participate as observers in the peer-reviews. The methodology referred to in paragraph 1 **of this article** shall also include the rules to cover the costs of the peer-reviews. ~~The Commission, supported by ENISA, shall establish within the methodology as referred to in paragraph 1 an objective, non-discriminatory, fair and transparent system for the selection and the random allocation of experts for each peer review.~~

3. The organisational aspects of the peer reviews shall be ~~decided~~ **defined** by the ~~Commission~~**Cooperation Group**, supported by **the Commission and** ENISA~~, and with the endorsement ,following the consultation of of the Cooperation Group~~, **and** be based on criteria defined in the methodology referred to in paragraph 1. Peer reviews shall assess the aspects referred to in paragraph 1 for all Member States and sectors **and may also**~~,~~ includ~~e~~**e**~~ing~~ targeted issues specific to one or several Member States or one or several sectors.

3a A Member State may decline to be subject to or postpone the review of a particular aspect referred to in paragraph 1 of this Article, or sector or targeted issues referred to in paragraph 3 of this Article, on duly justified grounds, and in particular if:

(i). the review is disproportionate for that Member State at that time, taking account of available resources and the potential additional administrative burden on ongoing activities, or

(ii). the review concerns activities which are in conflict with that Member States's national or public security or defence.

These grounds shall be notified to the Cooperation Group.

3b. Prior to the commencement of the peer-review process, the Member State to be reviewed may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated experts conducting peer-review.

4. Peer reviews ~~shall~~ **may** entail actual or virtual on-site visits and off-site exchanges. In view of the principle of good cooperation, the Member States being reviewed shall provide the designated experts with the requested information necessary for the assessment of the reviewed aspects**, without prejudice to national and 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 review process shall be used solely for that purpose. The experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of that review to any third parties. **The reviewed Member State may object to the designation of particular experts for its review on duly justified grounds communicated to the Cooperation Group.Commission and ENISA.**

5. Once reviewed in a Member State, the same aspects shall not be subject to further peer review within that Member State during the two years following the conclusion of a peer review, **unless the Member State concerned agrees upon proposal** ~~otherwise decided~~ by the **Cooperation Group or the** Commission, upon consultation ~~of~~**with** ENISA ~~and **endorsement by** the Cooperation Group~~.

6. Member State shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Member States, the Commission and ENISA without undue delay.

7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. **The Member States reviewed shall be allowed to provide ~~factual~~ comments on the relevant draft reports.** The **final** reports shall be submitted to ~~the Commission,~~ the Cooperation Group~~,~~ **the Commission,** ~~the CSIRTs network~~ and ENISA~~. The reports shall be discussed in the Cooperation Group and the CSIRTs network. The reports may be published on the dedicated website of the Cooperation Group.~~**The reports shall not be made publicly available without the prior consent of the Member State subject to review.**

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, ~~supervise~~ **oversee** its implementation and ~~be~~ **can be held** accountable for the non-compliance by the entities with the obligations under this Article. ~~**For this purpose, the management bodies shall receive regular reports on the status of implementation.**~~

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

2. Member States shall ensure that **essential and important entities have expert staff at menegerial level who** ~~members of the management body~~ **are required to** follow ~~specific~~ 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. **For this purpose, the management bodies shall receive regular reports on the implementation of such trainings**.

Article 18

Cybersecurity risk management measures

1. **This Directive applies an "all-hazard" approach that includes the protection of network and information systems and the physical protection from relevant natural and man-made risks that could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems.**

   Member States shall ensure that essential and important entities ~~shall~~ take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network**,** ~~services~~ 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 given to the degree of the entity's exposure to risks, its size, as well as the likelihood of occurrence of incidents and their severity.**

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 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 ~~(testing and auditing)~~ to assess the effectiveness of cybersecurity risk management measures;

(g) ~~**appropriate**~~ **policy on** the use of cryptography and encryption~~**, including the management of cryptographic key and digital signitures**~~.

(ga) human resources security~~, and~~ 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 shall take into account the vulnerabilities specific to each 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 shall take into account coordinated risk assessments issued 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**. **Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).** When~~re~~ preparing ~~those~~ **such implementing** acts, the Commission shall ~~proceed in accordance with the examination procedure referred to in Article 37(2) and follow~~, to the greatest extent possible, **follow** international and European standards, as well as relevant technical specifications **and exchange advice with the Cooperation Group on the draft implementing act in accordance with Article 12(4)(d).**

~~6. The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities.~~

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 mere notification under this paragraph shall not make the notifying entity subject to increased liability.**

2. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident.

Where applicable, those 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 ~~**serious**~~ **severe** ~~substantial~~ operational disruption 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, 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 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, ~~within 24 hours~~ **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 paragraphs 1 and 2 to the single points of contact of other affected Member States.

9. The single point of contact shall submit to ENISA ~~on a monthly basis~~**every three months** a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraphs 1 and 2 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 regularly the Cooperation Group and the CSIRTs network abouts 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 **when a threat shall be considered significant pursuant to paragraph 2 and** the cases in which an incident shall be considered significant as referred to in paragraph 3. **When adopting implementing acts on the significance of the cyber threat in accordance with this Directive, the Commission should take into account the severity and technical characteristics of the threat, as well as its potential cross-sectorial spillover effects.** 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,** ~~ICT~~ **services and** ~~ICT~~ **processes certified** under specific European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881~~. The **in order to demonstrate compliance or establish a presumption of conformity with certain requirements.~~ **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 ~~shall be empowered to~~ adopt ~~delegated~~ **implementing** acts specifying which categories of essential **or important** entities **may** ~~shall~~ be required **to use certain certified ICT products, services and processes or** obtain a certificate ~~and~~ under which ~~specific~~ European cybersecurity certification schemes **adopted pursuant to Article 49 of Regulation (EU) 2019/881.** ~~pursuant to paragraph 1The delegated acts shall be adopted in accordance with Article 36.~~ **Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2). When preparing** ~~the~~ **such implementing acts, the Commission shall, in accordance with Article 56 of Regulation (EU) 2019/882:**

   (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;

   (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, particularly SMEs.

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 21a

Use of qualified trust services or notified electronic identification schemes

In order to demonstrate compliance with cybersecurity risk management measures referred to in Article 18, Member States may require essential and important entities to use qualified trust services or notified electronic identification schemes under Regulation (EU) No 910/2014.

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**, verified** and complete domain name registration data in a dedicated database facility with due diligence **in accordance with**~~subject to~~ 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) status of registration**~~

c~~**d**~~**) registrant data, including:**

(i)

~~**e)**~~ **for individuals - name, surname**~~**,**~~ **and address** **and e-mail address;**

(ii)

~~**f)**~~ **for legal persons**~~**registrants other than individuals**~~ **- name**~~**,**~~ ~~**and**~~ **address, and e-mail address.**

~~**(g) e-mail address for contact purposes**~~

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. All entities under this Directive shall be deemed to be under the jurisdiction of the Member State where they provide their services. If the entity provides services in more than one Member State, it shall fall under the separate and concurrent jurisdiction of each of these Member States.

1. **Without prejudice to paragraph 1a,** DNS service providers, TLD name registries~~,~~ **and entities providing domain name registration services for the TLD**~~-~~, cloud computing service providers, data centre service providers, and content delivery network providers referred to in point 8 of **the** Annex ~~I~~, as well as digital providers referred to in point **1**6 of the 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.

Article 25

Registry for essential and important entities

1. ~~ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1).~~ **Member States shall ensure that** t~~T~~he 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** ~~shall~~ submit**, where applicable through the national ~~notification~~ mechanisms of self-notification referred to in Article 2(1a),** the following information **to the relevant authorities or bodies designated for this purpose** ~~to ENISA~~ 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 the Annex 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 ~~.~~

2. **Member States shall ensure that t**~~T~~he entities referred to in paragraph 1 ~~shall notify ENISA about~~**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. ~~Upon receipt of the information under paragraph 1, ENISA~~ **The Member States' single points of contact** shall forward **the information referred to in paragraphs 1 and 2**~~it~~ to ~~the single points of contact depending on the indicated location of each entity's main establishment or, if it is not established in the Union, of its designated representative~~**ENISA**. ~~Where an entity referred to in paragraph 1 has besides its main establishment in the Union further establishments in other Member States, ENISA shall also inform the single points of contact of those Member States.~~

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 ~~national~~ competent authorities to ~~the registry referred to in paragraph 1~~the registry, while ensuring the necessary guarantees to protect confidentiality of information where applicable.

~~4. Where an entity fails to register its activity or to provide the relevant information within the deadline set out in paragraph 1, any Member State where the entity provides services shall be competent to ensure that entity's compliance with the obligations laid down in this Directive.~~ **~~ENISA shall inform the Member States concerned as soon as it becomes aware of the entity's non-compliance with the obligations set out in paragraph 1 of this Article.~~**

CHAPTER V

Information sharing

Article 26

Cybersecurity information-sharing arrangements

1. ~~Without prejudice to Regulation (EU) 2016/679,~~ 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 trusted 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 and in compliance with the rules of Union law referred to in paragraph 1.

3. Member States shall 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 shall 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. ~~In compliance with Union law,~~ 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 CSIRT any relevant incidents, cyber threats or near~~s~~ 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. 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 of 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 and 20. **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] and other competent authorities designated under sector-specific Union legal acts** when addressing cybersecurity incidents. ~~when addressing incidents resulting in personal data breaches.~~

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.

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, as well as compliance with the obligation to notify the ENISA pursuant to Article 25 (1) and (2);

(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) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with the~~ir~~ obligations provided for by Articles 18 and 20;

(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 diclosure does not lead to a harmful exposure of the vulnerabilities of the respective entity**;

(i) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;

(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.

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 ~~accountability~~ 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**, ~~**of the risk of actual or potential loss of life and physical, social, emotional and psychological well-being,**~~ 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.

9. Member States shall ensure that their competent authorities **under this Directive** inform the relevant competent authorities **within that same** ~~of the~~ Member State ~~concerned~~ 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,** ~~Upon request of~~ 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** ~~**on**~~ **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.

Article 30

Supervision and enforcement for important entities

1. When provided with evidence or indication **or information** that an important entity is 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, including documented cybersecurity policies, as well as compliance with the obligation to notify ENISA pursuant to Article 25(1) and (2);

(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 (f)** 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;

(fa) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with the obligations provided for by Articles 18 and 20;

(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 diclosure does not lead to a harmful exposure of the vulnerabilities of the respective entity**;

(h) make a public statement which identifies the legal and natural person(s) responsible for the infringement of an obligation laid down in this Directive and the nature of that infringement;

(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 the important entities listed in **the** Annex ~~II~~.

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 entites** 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 10 000 000 EUR or ~~up to~~ 2% of the total worldwide annual turnover of the undertaking to which the essential ~~or important~~ entity belongs in the preceding financial year, whichever is higher.

4a. Member States shall ensure that infringements by the impotant entites 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 5 000 000 EUR or ~~up to~~ 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 ~~indications~~ **become aware** that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 **of this Directive** 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 ~~within a reasonable period of time~~.

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 shall not impose an administrative fine for ~~the same~~**an** infringement **by the same deed of** ~~under~~ 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 has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or other establishment or of the representative, and the competent authorities of those other Member States 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 ~~and their follow up~~, in accordance with Articles 29 and 30;

(b) a competent authority may request another competent authority to take the supervisory or enforcement measures referred to in Articles 29 and 30;

(c) a competent authority shall, upon receipt of a justified request from another competent authority, provide the other competent authority with assistance **proportionate** ~~**appropriate**~~ **to the resources at its own disposal** so that the supervision or enforcement actions referred to in Articles 29 and 30 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, ENISA and the Commission, 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 in accordance with Article 29 or Article 30 ~~**or the request concerns information or entails activities which are in conflict with that Member State's national 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 referred to in Articles 29 and 30.

~~**3. The provisions of this Article shall also apply in relation to critical entities of particular European significance according to Art 14 of Directive (EU) XXXX/XXXX (Resilience of Critical Entities Directive) which are under the scope of this Directive.**~~

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 **the** Annex~~es I and II~~ for the functioning of the economy and society in relation to cybersecurity. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The first report shall be submitted by… [54 months after the date of entry into force of this Directive].

~~*Article 36*~~

~~***Exercise of the delegation***~~

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

~~2. The power to adopt delegated acts referred to in Articles 18(6) and 21(2) shall be conferred on the Commission for a period of five years from […]~~

~~3. The delegation of power referred to in Articles 18(6) and 21(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.~~

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

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

~~6. A delegated act adopted pursuant to Articles 18(6) and 21(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.~~

Article 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** … [~~18~~**24** months after the date of entry into force of this Directive**],** Member States shall adopt and publish~~, by … [18**24** months after the date of entry into force of this Directive]~~, 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 ~~of Regulation (EU) No 910/2014~~ 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 ~~of Directive (EU) 2018/1972~~ 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 II~~I~~.

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*

ANNEX ~~I~~

SECTORS, SUBSECTORS AND TYPES OF ENTITIES

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings referred to in point (57) of Article 2 of Directive (EU) 2019/944, which carry out the function of 'supply' referred to in point (12) of Article 2 of that Directive ([28])
		— Distribution system operators referred to in point (29) of Article 2 of Directive (EU) 2019/944
		— Transmission system operators referred to in point (35) of Article 2 of Directive (EU) 2019/944
		— Producers referred to in point (38) of Article 2 of Directive (EU) 2019/944
		— Nominated electricity market operators referred to in point 8 of Article 2 of Regulation (EU) 2019/943 ([29])
		— Electricity market participants referred to in point (25) of Article 2 of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services referred to in points (18), (20) and (59) of Article 2 of Directive (EU)

[28] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p.125).

[29] Regulation (EU) 2019/943 of the European Parliament and of the Council on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).

		2019/944
	(b) District heating and cooling	— District heating or district cooling referred to in point (19) of Article 2 of the Directive (EU) 2018/2001 ([30]) on the promotion of the use of energy from renewable sources
	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		— Central oil stockholding entities referred to in point (f) of Article 2 of Council Directive 2009/119/EC ([31])
	(d) Gas	— Supply undertakings referred to in point (8) of Article 2 of Directive (EU) 2009/73/EC ([32])
		— Distribution system operators referred to in point (6) of Article 2 of Directive 2009/73/EC
		— Transmission system operators referred to point (4) of Article 2 of Directive 2009/73/EC
		— Storage system operators referred to in point (10) of Article 2 of

[30] Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).

[31] Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p.9).

[32] Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

		Directive 2009/73/EC
		— LNG system operators referred to in point (12) of Article 2 of Directive 2009/73/EC
		— Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities
	(e) Hydrogen	Operators of hydrogen production, storage and transmission
2. Transport	(a) Air	— Air carriers referred to in point (4) of Article 3 of Regulation (EC) No 300/2008 ([33])
		— Airport managing bodies referred to in point (2) of Article 2 of Directive 2009/12/EC([34]), airports referred to in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 ([35]), and entities operating ancillary installations contained within airports
		— Traffic management control operators providing air traffic control (ATC) services referred to in

[33] Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p.72).

[34] Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p.11).

[35] Regulation (EC) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p.1).

		point (1) of Article 2 of Regulation (EC) No 549/2004 ([36])
	(b) Rail	— Infrastructure managers referred to in point (2) of Article 3 of Directive 2012/34/EU([37])
		— Railway undertakings referred to in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities referred to in point (12) of Article 3 of Directive 2012/34/EU
	(c) Water	— Inland, sea and coastal passenger and freight water transport companies, referred to for maritime transport in Annex I to Regulation (EC) No 725/2004 ([38]), not including the individual vessels operated by those companies
		— Managing bodies of ports referred to in point (1) of Article 3 of Directive 2005/65/EC ([39]), including their port facilities referred to in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports

[36] Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p.1).

[37] Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p.32).

[38] Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p.6).

[39] Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

		— Operators of vessel traffic services referred to in point (o) of Article 3 of Directive 2002/59/EC ([40])
	(d) Road	— Road authorities referred to in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 ([41]) responsible for traffic management control
		— Operators of Intelligent Transport Systems referred to in point (1) of Article 4 of Directive 2010/40/EU ([42])
3. Banking		Credit institutions referred to in point (1) of Article 4 of Regulation (EU) No 575/2013 ([43])
4. Financial market infrastructures		— Operators of trading venues referred to in point (24) of Article 4 of Directive 2014/65/EU ([44])
		— Central counterparties (CCPs) referred to in point (1) of Article 2

[40] Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p.10)

[41] Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU–wide real–time traffic information services (OJ L 157, 23.6.2015, p. 21).

[42] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

[43] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

[44] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

		of Regulation (EU) No 648/2012 ([45])
5. Health		— Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU ([46])
		— EU reference laboratories referred to in Article 15 of Regulation XXXX/XXXX on serious cross-border threats to health[47]
		— Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC ([48]) — Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 — Entities manufacturing medical devices considered as critical during a public health emergency ('the public health emergency critical devices list') referred to in Article 20 of Regulation XXXX[49]

45 Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

46 Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross–border healthcare (OJ L 88, 4.4.2011, p. 45).

47 [Regulation of the European Parliament and of the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU, reference to be updated once the proposal COM (2020)727 final is adopted]

48 Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p.67).

49 [Regulation of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal produces and medical devices, reference to be updated once the proposal COM(2020)725 final is adopted]

6. Drinking water		Suppliers and distributors of water intended for human consumption referred to in point (1)(a) of Article 2 of Council Directive 98/83/EC([50]) but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential or important services
7. Waste water		Undertakings collecting, disposing or treating urban, domestic and industrial waste water referred to in points (1) to (3) of Article 2 of Council Directive 91/271/EEC ([51])
8. Digital infrastructure		— Internet Exchange Point providers
		— DNS service providers
		— TLD name registries
		— Cloud computing service providers
		— Data centre service providers
		— Content delivery network providers
		— Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014([52])

[50] Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).

[51] Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p.40).

[52] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p.73).

		— Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972([53]) or providers of electronic communications services referred to in point (4) of Article 2 of Directive (EU) 2018/1972 where their services are publicly available
[8a. Managed ICT service providers		— **An entity providing services such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers' premises, in their own data centre (hosting) or in a third-party data centre]**
9. Public administration		— Public administration entities of central governments
		— Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003 ([54])
		— Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003
		— **Any other public administration entities at regional or local levels which have jurisdiction over a territory of at least 200,000 inhabitants.**
10. Space		Operators of ground-based infrastructure, owned, managed and operated by Member States or by

[53] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communication Code (OJ L 321, 17.12.2018, p. 36).

[54] Regulation (EC) No 1059/2003 of the European Parliament and of the Council of 26 May 2003 on the establishment of a common classification of territorial units for statistics (NUTS) (OJ L 154, 21.6.2003, p. 1).

		private parties, that support the provision of space-based services, excluding providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972
11. Postal and courier services		**Postal service providers referred to in point (1a) of Article 2 of Directive 97/67/EC ([55])and providers of courier services**
12. Waste management		**Undertakings carrying out waste management referred to in point (9) of Article 3 of Directive 2008/98/EC ([56]) but excluding undertakings for whom waste management is not their principal economic activity**
13. Manufacture, production and distribution of chemicals		**Undertakings carrying out the manufacture, production and distribution of substances and articles referred to in points (4), (9) and (14) of Article 3 of Regulation (EC) No 1907/2006 ([57])**

[55] Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of the quality of service (OJ L 15, 21.1.98, p.14)**, as amended by Directive 2008/6/EC of the European Parliament and of the Council of 20 February 2008 amending Directive 97/67/EC with regard to the full accomplishment of the internal market of Community postal services (OJ L 52, 27.2.2008, p. 3).**

[56] Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3)

[57] Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning registration, evaluation, authorisation and restriction of chemicals (REACH), establishing a European Chemicals Agency amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155.EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1).

14. Food production, processing and distribution		**Food businesses referred to in point (2) of Article 3 of Regulation (EC) No 178/2002 ([58])**
15. Manufacturing	**(a) Manufacture of medical devices and in vitro diagnostic medical devices**	**Entities manufacturing medical devices referred to in Article 2 point 1 of Regulation (EU) 2017/745([59]), and entities manufacturing in vitro diagnostic medical devices referred to in Article 2 point 2 of Regulation (EU) 2017/746 ([60]) with exception of entities manufacturing medical devices mentioned in Annex 1, point 5.**
	(b) Manufacture of computer, electronic and optical products	**Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2**
	(c) Manufacture of electrical equipment	**Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2**
	(d) Manufacture of machinery and equipment n.e.c.	**Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2**
	(e) Manufacture of motor vehicles, trailers and semi-trailers	**Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2**
	(f) Manufacture of	**Undertakings carrying out any of the**

58 Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p.1).

59 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p.1)

60 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p.176)

	other transport equipment	**economic activities referred to in section C division 30 of NACE Rev. 2**
16. Digital providers		**— Providers of online marketplaces**
		— Providers of online search engines
		— Providers of social networking services platform

ANNEX II

IMPORTANT ENITIES:

SECTORS, SUBSECTORS AND TYPES OF ENTITIES

Sector	Subsector	Type of entity
1. Postal and courier services		Postal service providers referred to in point (1) of Article 2 of Directive 97/67/EC ([61])and providers of courier services
2. Waste management		Undertakings carrying out waste management referred to in point (9) of Article 3 of Directive 2008/98/EC ([62]) but excluding undertakings for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		Undertakings carrying out the manufacture, production and distribution of substances and articles referred to in points (4), (9) and (14) of Article 3 of Regulation (EC) No 1907/2006 ([63])

[61] Directive 97/67/EC of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of the quality of service (OJ L 15, 21.1.98, p.14).

[62] Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives (OJ L 312, 22.11.2008, p. 3)

[63] Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning registration, evaluation, authorisation and restriction of chemicals (REACH), establishing a European Chemicals Agency amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155.EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, p. 1).

~~4. Food production, processing and distribution~~		~~Food businesses referred to in point (2) of Article 3 of Regulation (EC) No 178/2002 ([64])~~
~~5. Manufacturing~~	~~(a) Manufacture of medical devices and in vitro diagnostic medical devices~~	~~Entities manufacturing medical devices referred to in Article 2 point 1 of Regulation (EU) 2017/745([65]), and entities manufacturing in vitro diagnostic medical devices referred to in Article 2 point 2 of Regulation (EU) 2017/746 ([66]) with exception of entities manufacturing medical devices mentioned in Annex 1, point 5.~~
	~~(b) Manufacture of computer, electronic and optical products~~	~~Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2~~
	~~(c) Manufacture of electrical equipment~~	~~Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2~~
	~~(d) Manufacture of machinery and equipment n.e.c.~~	~~Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2~~
	~~(e) Manufacture of motor vehicles, trailers and semi-trailers~~	~~Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2~~
	~~(f) Manufacture of other~~	~~Undertakings carrying out any of the economic activities referred to in~~

~~64~~ Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 1.2.2002, p.1).

~~65~~ Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p.1)

~~66~~ Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p.176)

	~~transport equipment~~	~~section C division 30 of NACE Rev. 2~~
~~6. Digital providers~~		~~— Providers of online marketplaces~~
		~~— Providers of online search engines~~
		~~— Providers of social networking services platform~~