**COMPROMISE AMENDMENT 1**

The CA 1 covers all articles, annexes and recitals of the Commission proposal (COM (2020)0823- 2020/0359 (COD)). If CA 1 is adopted, all amendments tabled (1-600) and related opinions (AFET 1-48, IMCO 1-156, TRAN 1-34 and LIBE 1-122) fall.

**Title**

All related AMs fall, meaning AM 92.

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union (***NIS 2 Directive***), repealing Directive (EU) 2016/1148
(Text with EEA relevance)

**Article 1 Subject matter (covers Article 1, paragraph 2 and recitals 1, 3, 5, 20 and 82)**

All related AMs fall, including AMs 209-212, 26, 93, 118, IMCO 42, AFET 1-3, AFET 6, TRAN 1 and IMCO 10, LIBE 1, LIBE 3, LIBE 4 and LIBE 13.

*Article 1*

***Subject matter***

1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union.

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 Annex I and important entities in Annex II;

(c) lays down obligations on cybersecurity information sharing***;***

***(ca) lays down supervision and enforcement obligations on Member States.***

**Recitals**[1]

(1) Directive (EU) 2016/1148 of the European Parliament and the Council[11], ***commonly known as the 'NIS directive'***, 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 ***security and to the effective functioning of its*** economy and society to function effectively.

(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. ***Moreover, cybersecurity is a key enabler for many critical sectors to successfully embrace the digital transformation and to fully grasp the economic, social and sustainable benefits of digitalisation.***

***(3a) Large-scale cybersecurity incidents and crises at Union level require coordinated action to ensure a rapid and effective response, because of the high degree of interdependence between sectors and countries. The availability of cyber-resilient networks and information systems and the availability, confidentiality and integrity of data are vital for the security of the Union within as well as beyond its borders, as cyber threats could originate from outside the Union. The Union's ambition to acquire a more prominent geopolitical role also rests on credible cyber defence and deterrence, including the capacity to identify malicious actions in a timely, effective manner and to respond adequately.***

(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. ***Ultimately, these divergences can lead to higher vulnerability of some Member States to cybersecurity threats, with potential spill over effects across the Union.*** 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 ***(NIS 2 Directive)***.

(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

[1] The present CAs include all those recitals modified (either text change or deletion). Those recitals of the Commission proposal that have not been modified are deemed to be approved.

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 ***intensified attacks against network and information systems during the*** COVID-19 pandemic ***have*** shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.

***(82b) This Directive creates new tasks for ENISA, thereby enhancing its role, and could also result in ENISA being required to carry out its existing tasks under Regulation (EU) 2019/881 of the European Parliament and of the Council[1a] to a higher standard than before. In order to ensure that ENISA has the necessary financial and human resources to carry out existing and new activities under its tasks, as well as to satisfy any higher standard resulting from its enhanced role, its budget should be increased accordingly. In addition, in order to ensure the efficient use of resources, ENISA should be given greater flexibility in the way that it is permitted to allocate resources internally, so as to enable it to carry out its tasks, and to satisfy expectations, effectively.***

**Article 2 Scope (covers Article 2 paragraphs 1, 2, 4 and 6, Annexes I and II, and recitals 6, 7, 8, 9, 10, 12, 14, 15, 19 and 69)**

All related AMs fall, including AMs 1-2, 27-31, 94-96, 213-241, 102-110, 117, 126-128, 193-196, 598-600, 91, AFET 4, AFET 5, IMCO 2-10, IMCO 12, IMCO 36, IMCO 43, IMCO 44, TRAN 2, TRAN 4, TRAN 5, TRAN 9, TRAN 17, TRAN 18, AFET 47, AFET 48, LIBE 47-54, LIBE 5-11, LIBE 39 and LIBE 122.

*Article 2*

***Scope***

1. This Directive applies to public and private ***essential and important*** entities of a type referred to as essential entities in Annex I and as important entities in Annex II ***that provide their services or carry out their activities within the Union***. This Directive does not apply to small ***enterprises or micro***enterprises within the meaning of ***Article 2(2) and (3) of the Annex to*** Commission Recommendation 2003/361/EC.[2] ***Article 3 (4) of the Annex of that Recommendation is not applicable***.

2. Regardless of their size, this Directive also applies to ***essential and important*** entities, where:

   (a) the services are provided by one of the following entities:

[2] 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).

(i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I;

(ii) trust service providers referred to point 8 of Annex I;

(iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I;

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

(c) the entity is the sole provider of a service in a Member State;

(d) a ~~potential~~ disruption of the service provided by the entity could have an impact on public safety, public security or public health;

(e) a ~~potential~~ disruption of the service provided by the entity could induce 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[3] [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 points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.~~

***2a. Member States shall establish a list of essential and important entities, including the entities referred to in paragraph 1 and the entities identified pursuant to points (b) to (f) and Article 24 (1), by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it.***

***2b. Member States shall ensure that essential and important entities submit at least the following information to competent authorities:***

***(a) the name of the entity;***

***(b) address and up-to-date contact details, including email addresses, IP ranges, telephone numbers; and***

***(c) the relevant sector(s) and subsector(s) referred to in Annexes I and II.***

***The essential and important entities shall notify any changes to the details submitted pursuant to the first subparagraph without delay, and, in any event, within two weeks from the date on which the change takes effect. To this end, the Commission, with the assistance of ENISA, shall without undue delay issue guidelines and templates regarding the obligations set out in this paragraph.***

***2c. By [6 months after the transposition deadline] and every two years thereafter, Member States shall notify:***

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

***(a) the Commission and the Cooperation Group of the number all essential and important entities identified for each sector and subsector referred to in Annexes I and II, and***

***(b) the Commission , the names of the entities identified pursuant to paragraph 2, points (b) to (f).***

3. This Directive is without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law.

4. This Directive applies without prejudice to Council Directive 2008/114/EC[4] and Directives 2011/93/EU[5], 2013/40/EU[6] ***and 2002/58/EC***[7] of the European Parliament and of the Council .

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

6. Where provisions of sector–specific acts of Union law require essential or important entities ~~either~~ to adopt cybersecurity risk management measures or to notify incidents, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply. ***The Commission shall without undue delay issue guidelines in relation to the implementation of the sector–specific acts of Union law in order to ensure that cybersecurity requirements established by this Directive are fulfilled by those acts and that there is no overlap or legal uncertainty. When preparing those guidelines, the Commission shall take into account the best practices and expertise of ENISA and the Cooperation Group.***

***6a. Essential and important entities, CSIRTs and providers of security technologies and services, shall process personal data, to the extent strictly necessary and proportionate for the purposes of cybersecurity and network and information security, to meet the obligations set out in this Directive. That processing of personal data under this Directive shall be carried out in compliance with Regulation (EU) 2016/679, in particular Article 6.***

---

4 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).

5 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).

6 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).

7 ***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 (OJ L 201, 31.7.2002)***

***6b. The processing of personal data pursuant to this Directive by providers of public electronic communications networks or providers of publicly available electronic communications referred to in point 8 of Annex I, shall be carried out in accordance with Directive 2002/58/EC.***

**Recitals**

(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 ***prevention,*** 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[14], are of relevance.

(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 ***risk management requirements and reporting obligations*** 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.

(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/EC15, 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.~~

(9) However, 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 it to the Commission.~~

***(9a new) Member States should establish a list of all essential and important entities. That list should include the entities that meet the generally applicable size-related criteria as well as the small enterprises and microenterprises that fulfil certain criteria that indicate a key role for the economies or societies of Member States. In order for CSIRTs and competent authorities to provide assistance and to warn entities about cyber incidents that could affect them, it is important that those authorities have the correct contact details of the entities.***

***Essential and important entities should therefore submit at least the following information to the competent authorities: the name of the entity, the address and up-to-date contact details, including email addresses, IP ranges, telephone numbers and relevant sector(s) and subsector(s) referred to in Annexes I and II. The entities should notify the competent authorities of any changes to this information. Member States should without undue delay, ensure that this information can be easily provided through a single entry point. To that end, ENISA, in cooperation with the Cooperation Group, should without undue delay issue guidelines and templates regarding the obligations set out in this paragraph. Member States should notify to the Commission and the Cooperation Group of the number of essential and important entities. Member States should also notify the Commission for the purpose of the review referred to in Article 35 of the names of the small enterprises and micro entities identified as essential and important, in order to enable the Commission to assess consistency among the Member States' approaches. This information should be handled as strictly confidential.***

(10) The Commission, in cooperation with the Cooperation Group ***and relevant stakeholders***, ~~may~~ ***should*** issue guidelines on the implementation of the criteria applicable to micro and small enterprises. ***The Commission should also ensure that appropriate guidance is given to all micro and small enterprises falling within the scope of this Directive. The Commission should, with the support of the Member States, provide microenterprises and small enterprises with information in this regard.***

***(10a) The Commission should also issue guidelines to support Member States in correctly implementing the provisions on the scope, and to evaluate the proportionality of the obligations set out by this Directive, especially as regards entities with complex business models or operating environments, whereby an entity may simultaneously fulfil the criteria assigned to both essential and important entities, or may simultaneously conduct activities that are some within and some outside the scope of this Directive.***

(12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors***. Sector-specific Union legal acts that require essential or important entities to adopt cybersecurity risk management measures or to report significant incidents, should, where possible, be consistent with the terminology and refer to the definitions laid down in this Directive***. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents***, and where those requirements are*** of at least an equivalent effect to the obligations laid down in this Directive ***and apply to the entirety of the security aspects of the operations and services provided by essential and important entities***, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission ***should*** issue ***comprehensive*** guidelines in relation to the implementation of the *lex specialis****, taking into account the relevant opinions, expertise and best practices of ENISA and the Cooperation Group***. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications ***that duly take into account the need for a comprehensive and consistent cybersecurity framework***. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy.

(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[17] and this Directive. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be 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 ***authorities within and between Member States,*** 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. Authorities under both Directives should cooperate and exchange information ***without undue delay*** ~~***on a regular basis***~~, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures taken by critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent authorities under this Directive should be allowed to exercise their supervisory and enforcement powers on an essential entity identified as critical. Both authorities should cooperate and exchange information ***where possible in real time,*** for this purpose.

(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 top-level-domain (TLD) name servers, ***publicly available recursive domain name resolution services for internet end-users and*** authoritative domain ***name resolution services***. ***This Directive does not apply to root*** name servers.

(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council18, 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 ***while taking into account the degree of their dependence on network and information systems.*** Transport services that are not undertaken in conjunction with one of those steps should fall outside of the scope of postal services.

(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by ***essential and important*** entities, CSIRTs and providers of security technologies and services***, is necessary for compliance with their legal obligations provided for in this Directive. Such processing of personal data might also be necessary for the purposes of the legitimate interests pursued by essential and important entities. Where this Directive requires the processing of personal data for the purpose of cybersecurity and network and information security in accordance with the provisions set out in Article 18, 20 and 23 of the Directive, that processing is considered to be necessary for compliance with a legal obligation as referred to in Article 6(1), point (c) of Regulation (EU) 2016/679. For the purpose of Articles 26 and 27 of this Directive, processing, as referred to in Article 6(1), point (f) of Regulation (EU) 2016/679, is considered to be necessary for the purposes of the legitimate interests pursued by the essential and important entities.*** Measures related to the prevention, detection, ***identification, containment,*** 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 require the processing of ***certain categories*** of personal data***, such as*** IP addresses, uniform resources locators (URLs), domain names, email

addresses***, time stamps, Operation System- or browser-related information, cookies or other information indicating the modus operandi***.

**Annexes**

Annex I, Transport (d) Road

| | | |
|---|---|---|
| 2. Transport | (d) Road | — Road authorities referred to in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 ([8]) responsible for traffic management control<br>***— Operators of smart charging services for electric vehicles*** |

Annex II – table – row 6 a (new)

| | | |
|---|---|---|
| ***6a. Education and research*** | | ***— Higher education institutions and research institutions*** |

**CA Article 3 Minimum harmonisation**

No AM tabled, Commission proposal remains unchanged.

*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.

[8] 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).

**CA Article 4 Definitions (covers Article 4, paragraphs 1, 2, 6, 11, 13-15 and recitals 38, 39 and 50)**

All related AMs fall, including AMs 7, 8, 29-33, 242-270, 144, 145, 164-166, IMCO 23, IMCO 45-49, LIBE 28 and LIBE 55-59.

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

(3) 'cybersecurity' means cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council[9];

(4) 'national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the security of network and information systems in that Member State;

***(4a) 'near miss' means an event which could have compromised the availability, authenticity, integrity or confidentiality of data, or could have caused harm, but was successfully prevented from producing their negative impact;***

(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 ***prevention,*** detection, analysis**,** and containment of and a response to an incident;

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

[9] 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).

***(7a) 'risk' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident;***

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

(9) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of i) a DNS service provider, a top-level domain (TLD) name registry, a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of 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[10];

(11) 'technical specification' means a technical specification ***as defined in*** Article ***2, point (20)*** of Regulation (EU) ***No 2019/881***;

(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 ***enables the identification of internet*** services and resources***, allowing end-user devices to utilise*** internet ***routing and connectivity services, to reach those services and resources***;

(14) 'DNS service provider' means an entity that provides***:***

***(a) open and public*** recursive domain name resolution services to internet end-users***; or***

***(b) authoritative domain name resolution services as a*** service ***procurable by third-party entities***;

(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***, irrespective of whether any of those operations are being performed by the entity or are outsourced***;

***(15a) 'domain name registration services' means services provided by domain name registries and registrars, privacy or proxy registration service providers, domain***

[10] 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).

***brokers or resellers, and any other services which are related to the registration of domain names;***

(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 [11];

(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[12];

(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[13];

(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;

(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 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;

---

11 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).

12 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).

13 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).

(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.

Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded.

***(23a) 'public electronic communications network' means a public electronic communications network as defined in Article 2, point (8) of Directive (EU) 2018/1972;***

***(23b) 'electronic communications service' means an electronic communications service as defined in Article 2, point (4) of Directive (EU) 2018/1972;***

(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;

(26) 'important entity' means any entity of a type referred to as an important entity in Annex II

**Recitals**

(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.~~

(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 ***to network security*** 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. ***However, as the attack surface continues to expand, number-independent interpersonal communications services including, but not limited to, social media messengers, are becoming popular attack vectors. Malicious actors use platforms to communicate and attract victims to open compromised web pages, therefore increasing the likelihood of incidents involving the exploitation of personal data, and by extension, the security of information systems***.

**CA Article 5 (covers Article 5, paragraphs 1-4)**

All related AMs fall, including AMs 34, 36, 93, 113, 115, 121, 122, 130, 131, 271-304, IMCO 13, IMCO 14, IMCO 49-60, AFET 19-24, TRAN 10, TRAN 19, AFET 19-24 and LIBE 60-67.

*Article 5*

***National cybersecurity strategy***

1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives***, the required technical, organisational, and financial resources to achieve those objectives, as well as the*** 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 ***State's*** strategy on cybersecurity;

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

   (ba) ***a framework allocating*** the roles and responsibilities of public bodies and entities as well as other relevant actors***, underpinning the cooperation and coordination, at the national level, between the competent authorities designated pursuant to Article 7(1) and Article 8(1), the single point of contact designated pursuant to Article 8(3), and the CSIRTs designated pursuant to Article 9***;

   (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***, including a cybersecurity single point of contact for SMEs that provides support for implementing the specific cybersecurity measures***;

   (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[14] [Resilience of Critical Entities Directive]***, both within and between Member States,*** for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks;

   ***(fa) an assessment of the general level of cybersecurity awareness amongst citizens.***

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

   ***(-a) a policy addressing cybersecurity for each sector covered by this Directive;***

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

(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) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement***, including encryption requirements and the use of open source cybersecurity products***;

(c) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6;

(d) a policy related to sustaining the general availability and integrity of the public core of the open internet***, including cybersecurity of undersea communications cables***;

***(da) a policy to promote and support the development and integration of emerging technologies, such as artificial intelligence, in cybersecurity-enhancing tools and applications;***

***(db) a policy to promote the integration of open-source tools and applications;***

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

(f) a policy on supporting academic and research institutions that develop***, enhance and deploy*** 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 ***promoting cybersecurity for*** SMEs, ***including*** those excluded from the scope of this Directive, ***addressing their specific needs and providing easily accessed*** guidance and support, ***including guidelines addressing supply chain challenges faced;***

***(ha) a policy to promote cyber hygiene comprising a baseline set of practices and controls and raising general cybersecurity awareness among citizens for cybersecurity threats and best practices;***

***(hb) a policy on promoting active cyber defence;***

***(hc) a policy to help authorities develop competences and understanding of the security considerations needed to design, build, and manage connected places;***

***(hd) a policy specifically addressing the ransomware threat and disrupting the ransomware business model;***

***(he) a policy, including relevant procedures and governance frameworks, to support and promote the establishment of cybersecurity PPPs.***

3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. Member States may exclude 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 at least every four 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 request, in the development of a national strategy and of key performance indicators for the assessment of the strategy. ***ENISA shall provide guidance to Member States in order to align their already formulated national cybersecurity strategies with the requirements and obligations set out in this Directive.***

**Recitals**

***(26a) Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software and online application security, and business or end-user data on which entities rely upon. Cyber hygiene policies comprising a common baseline set of practices including, but not limited to, software and hardware updates, password changes, management of new installs, limitation of administrator-level access accounts, and backing up of data, enable a proactive framework of preparedness and overall safety and security in the event of incidents or threats. ENISA should monitor and assess Member States' cyber hygiene policies, and explore Union wide schemes to enable cross-border checks ensuring equivalence independent of Member State requirements.***

***(26b) The use of artificial intelligence (AI) in cybersecurity has the potential of improving the detection and to stop attacks against network and information systems, enabling resources to be diverted towards more sophisticated attacks. Member States should therefore encourage in their national strategies the use of (semi-)automated tools in cybersecurity and the sharing of data needed to train and improve automated tools in cybersecurity. In order to mitigate risks of unduly interference with the rights and freedoms of individuals that AI-enabled systems might pose, the requirements of data protection by design and by default laid down in Article 25 of Regulation (EU) 2016/679 shall be applied. Integrating appropriate safeguards such as pseudonymisation, encryption, data accuracy and data minimisation could furthermore mitigate these risks.***

***(26c) Open-source cybersecurity tools and applications can contribute to a higher degree of transparency and can have a positive impact on the efficiency of industrial innovation. Open standards facilitate interoperability between security tools, benefitting the security of industrial stakeholders. Open-source cybersecurity tools and applications can leverage the wider developer community, enabling entities to pursue vendor diversification and open security strategies. Open security can lead to a more transparent verification process of cybersecurity related tools and a community-driven process of discovering vulnerabilities. Member States should therefore promote the adoption of open-source software and open standards by pursuing policies relating to the use of open data and open-source as part of security through transparency. Policies promoting the adoption and sustainable use of open-source cybersecurity tools are of particular importance for SMEs facing significant costs for implementation, which can be minimised by reducing the need for specific applications or tools.***

***(26d) Public-Private Partnerships (PPPs) in the field of cybersecurity can provide the right framework for knowledge exchange, sharing of best practices and the establishment of a common level of understanding amongst all stakeholders. Member States should adopt policies underpinning the establishment of cybersecurity-specific PPPs as part of their national cybersecurity strategies. Those policies should clarify, inter alia, the scope and stakeholders involved, the governance model, the available funding options, and the***

***interaction among participating stakeholders. PPPs can leverage the expertise of private sector entities to support Member States' competent authorities in developing state-of-the art services and processes including, but not limited to, information exchange, early warnings, cyber threat and incident exercises, crisis management, and resilience planning.***

***(27a) Member States should, in their national cybersecurity strategies, address specific cybersecurity needs of small and medium-sized enterprises (SMEs). SMEs represent, in the Union context, a large percentage of the industrial/business market and they are often struggling to adapt to new business practices in a more connected world, navigating the digital environment, with employees working from home and business increasingly being conducted online. Some SMEs face specific cybersecurity challenges such as low cyber-awareness, a lack of remote IT security, the high cost of cybersecurity solutions and an increased level of threat, such as ransomware, for which they should receive guidance and support. Member States should have a cybersecurity single point of contact for SMEs, which either provides guidance and support to SMEs or directs them to the appropriate bodies for guidance and support on cybersecurity related issues. Member States are encouraged to also offer services such as website configuration and logging enabling to small enterprises and microenterprises that lack those capabilities.***

***(27b) Member States should adopt policies on the promotion of active cyber defence as part of their national cybersecurity strategies. Active cyber defence is the proactive prevention, detection, monitoring, analysis and mitigation of network security breaches, combined with the use of capabilities deployed within and outside the victim network. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enabling a unity of effort in successfully detecting, preventing and addressing attacks against network and information systems. Active cyber defence is based on a defensive strategy that excludes offensive measures against critical civilian infrastructure.***

**CA Article 6 vulnerability disclosure/database (covers Article 6, paragraphs 1 and 2 and recitals 28-31)**

All related AMs fall, including AMs 5, 6, 37, 38, 305-313, 132-140, IMCO 61, IMCO 62, AFET 25, AFET 26, IMCO 15-18 and LIBE 68.

*Article 6*

***Coordinated vulnerability disclosure and a European vulnerability database***

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, ***upon request of the reporting entity***, 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, the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.

2. ENISA shall develop and maintain a European vulnerability ***database leveraging the global Common Vulnerabilities and Exposures (CVE)***. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures***, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the database,*** with a view in particular to enabling important and essential entities and their suppliers of network and information systems***, as well as entities which do not fall within the scope of this Directive, and their suppliers,*** to disclose and register vulnerabilities present in ICT products or ICT services. ***All interested parties shall be provided access to the information on the vulnerabilities contained in the database that have patches or mitigation measures available.*** The ***database*** 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. In the absence of available patches, guidance addressed to users of vulnerable ***ICT*** products and ***ICT*** services as to how the risks resulting from disclosed vulnerabilities may be mitigated ***shall be included in the database***.

**Recitals**

(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 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 provide guidance on vulnerability handling and vulnerability disclosure respectively. ***Strengthening the coordination*** between reporting entities and manufacturers or providers of ICT products or services is particularly important ***to facilitate the voluntary framework of vulnerability disclosure.*** 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.

***(28a) The Commission, ENISA and the Member States should continue to foster international alignment with standards and existing industry best practices in the area of risk management, for example in the areas of supply chain security assessments, information sharing and vulnerability disclosure.***

(29) Member States***, in cooperation with ENISA,*** should therefore take measures to facilitate coordinated vulnerability disclosure by establishing a relevant national policy. ***In that national policy, Member States should address problems which vulnerability researchers encounter. Entities and natural persons researching vulnerabilities may in some Member States be exposed to criminal and civil liability. Member States are therefore encouraged to issue guidelines for non-prosecution of information security research and an exception for civil liability for those activities.***

***(29a)*** 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***, which are likely to be affected by the vulnerability,*** 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 vulnerability disclosure). Where vulnerabilities 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.

***(30)*** Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. Sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also ***for*** national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability ***database*** where, essential and important entities and their suppliers, as well as entities which do not fall ***with***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. ***The aim of that database is to address the unique challenges posed by cybersecurity risks to European entities. Furthermore, ENISA should establish a responsible procedure regarding the publication process, in order to give entities the time to take mitigating measures as regards their vulnerabilities, and employ state of the art cybersecurity measures, as well as machine-readable datasets and corresponding interfaces (API). To encourage a culture of disclosure of vulnerabilities, a disclosure should be without detriment of the reporting entity.***

(31) ***The*** European vulnerability ***database maintained by ENISA should leverage the Common Vulnerabilities and Exposures (CVE)*** registry***, through the use of its framework for identification, tracking and scoring of vulnerabilities. Furthermore, ENISA should explore the possibility to enter into structured cooperation agreements with other similar***

***registries or databases under the third country jurisdictions, to avoid duplications of efforts and to seek complementarity.***

**CA Article 7 National cybersecurity crisis management framework (covers Article 7 paragraphs 2 and 4)**

All related AMs fall, including AMs 314-316, IMCO 63, IMCO 64, AFET 27, AFET 28 and LIBE 69.

*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 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.

***1a. Where a Member State designates more than one competent authority referred to in paragraph 1, it should clearly indicate which of those competent authorities shall serve as the coordinator for the management of large-scale incidents and crises.***

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

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) crisis management procedures and information exchange channels;

   (d) preparedness measures, including 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 ***to the EU-CyCLONe*** 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.

**CA Article 8 National competent authorities and single points of contact (covers Article 8, paragraphs 3 and 4)**

All related AMs fall, including AMs 39, 317 and 318.

*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 ***of the competent authorities referred to in paragraph 1 as a*** 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, ***the Commission and ENISA,*** 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.

**CA Article 9 CSIRTs (covers Article 9, paragraphs 2, 6 and 7, and recitals 24-26)**

All related AMs fall, including AMs 2, 40, 41, 124-131, 319-324, IMCO 12, IMCO 13, AFET 7, AFET 29-31 and LIBE 18.

*Article 9*

***Computer security incident response teams (CSIRTs)***

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

2. Member States shall ensure that each CSIRT has adequate resources ***and the technical capabilities necessary*** 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.

***6a. Member States shall ensure the possibility of effective, efficient and secure information exchange on all classification levels between their own CSIRTs and CSIRTs from third countries on the same classification level.***

***6b. CSIRTs shall, without prejudice to Union law, in particular Regulation (EU) 2016/679, cooperate with CSIRTs or equivalent bodies in candidate countries and in other third countries in the Western Balkans and the Eastern Partnership and, where possible, provide them with cybersecurity assistance.***

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

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

**Recitals**

(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 ***designate one or more computer security incident response teams (CSIRTs) under this Directive and*** ensure that they ***are*** well-

functioning, 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***. Member States may designate existing computer emergency response teams ('CERTs') as CSIRTs***. 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[19] as regards personal data, on behalf of and upon request by an entity under this Directive***, or in case of a serious threat to national security***, a proactive scanning of the network and information systems used for the provision of their services. 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***, including with CSIRTs from third countries where information exchange is reciprocal and beneficial to the security of citizens and entities,*** in addition to the CSIRTs network established by this Directive***, in order to contribute to the development of Union standards that can shape the cybersecurity landscape at international level. Member States could also explore the possibility of increasing cooperation with like-minded partner countries and international organisations with the aim to secure multilateral agreements on cyber norms, responsible state and non-state behaviour in cyberspace and effective global digital governance as well as to create an open, free, stable and secure cyberspace based in international law.***

**CA Article 10 Requirements and tasks of CSIRTs (covers Article 10, paragraphs 1, 2 and 4, and recital 35)**

All related AMs fall, including AMs 325-335, 42-48, 126 and 142, IMCO 22, IMCO 65-69 and LIBE 70.

*Article 10*

***Requirements, technical capabilities 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 ***classifying,*** routing***, and tracking*** requests, in particular, to facilitate effective and efficient handovers;

***(ca) CSIRTs shall have appropriate codes of conduct in place to ensure the confidentiality and trustworthiness of their operations;***

(d) CSIRTs shall be adequately staffed to ensure availability at all times ***and ensure appropriate training frameworks of their staff***;

(e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services***, including broad connectivity across networks, information systems, services and devices;***

(f) CSIRTs shall have the possibility to participate in international cooperation networks.

***1a. CSIRTs shall develop at least the following technical capabilities:***

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

***(b) the ability to support intrusion prevention and detection;***

***(c) the ability to collect and conduct complex forensic data analysis, and to reverse engineer cyber threats;***

***(d) the ability to filter malign traffic;***

***(e) the ability to enforce strong authentication and access privileges and controls; and***

***(f) the ability to analyse cyber threats.***

2. CSIRTs shall have the following tasks:

(a) monitoring cyber threats, vulnerabilities and incidents at national level ***and acquiring real-time threat intellingence***

(b) providing early warning, alerts, announcements and dissemination of information to essential and important entities as well as to other relevant interested parties on cyber threats, vulnerabilities and incidents, ***if possible near-real-time***;

(c) responding to incidents ***and providing assistance to the entities involved***;

(d) providing dynamic risk and incident analysis and situational awareness regarding cybersecurity

(e) providing, upon request of an entity ***or in the case of a serious threat to national security***, 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) providing, upon request of an entity enabling and configuration of network logging to protect data, including personal data from unauthorised exfiltration;***

***(fb) contributing to the deployment of secure information sharing tools pursuant to Article 9(3).***

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

4. In order to facilitate cooperation, CSIRTs shall promote ***automation of information exchange,*** 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.

**Recitals**

***(25a) CSIRTs should have the ability to, upon an entity's request, continuously discover, manage, and monitor all internet-facing assets, both on premises and off premises, to understand their overall organisational risk to newly discovered supply chain compromises or critical vulnerabilities. The knowledge whether an entity runs a privileged management interface, affects the speed of undertaking mitigating actions.***

(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes for officials from other Member States***, within structured rules and mechanisms underpinning the scope and, where applicable, the required security clearance of officials participating in such exchange schemes,*** in order to improve cooperation ***and strengthen trust among Member States***. 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 ***or CSIRT***.

**CA Article 11 Cooperation at national level (covers Article 11, paragraphs 2, 4 and 5)**

All related AMs fall, including AMs 336-340, IMCO 70, IMCO 71, AFET 33, LIBE 71 and LIBE 72.

*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 their CSIRTs receive notifications on ***significant*** incidents ***pursuant to Article 20*** and significant cyber threats and near misses ***pursuant to Article 27 through the single entry point referred to in Article 20(5a).***

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***,*** single points of contact***, CSIRTs,*** law enforcement authorities, ***national regulatory authorities or other competent authorities responsible for public electronic communications networks or for publicly available electronic communications services pursuant to Directive (EU) 2018/1972,*** data protection authorities, the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State ***in line with their respective competences***.

5. Member States shall ensure that their competent authorities regularly provide ***timely*** information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] on cybersecurity risks, cyber 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.

**CA Article 12 Cooperation Group (covers Article 12, paragraphs 3, 4 and 8 and recitals 33 and 34)**

All related AMs fall, including AMs 49, 50, 341-351, IMCO 72-81, AFET 34 and 35, and TRAN 11, TRAN 12, TRAN 20, TRAN 21, IMCO 21, LIBE 73-75, LIBE 20 and LIBE 21.

*Article 12*
***Cooperation Group***

1. In order to support and to facilitate strategic cooperation and the exchange of information among Member States in the field of application of the Directive, a Cooperation Group is established.

2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 6.

3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The ***European Parliament and the*** European External Action Service shall participate in the activities of the Cooperation Group as ***observers***. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(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, ***such as the EDPB and representatives of industry,*** 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, ***capacity*** building, standards and technical specifications ***as well as the identification of essential and important entities***;

***(ba) mapping the national solutions in order to promote compatibility of cybersecurity solutions applied to each specific sector across the Union;***

(c) exchanging advice and cooperating with the Commission on emerging cybersecurity policy initiatives ***and the overall consistency of sector-specific cybersecurity requirements***;

(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;

(f) discussing reports on the peer review referred to in Article 16(7)***, and drawing up conclusions and recommendations***;

***(fa) carrying out coordinated security risk assessments that may be initiated pursuant to Article 19(1), in cooperation with the Commission and ENISA;***

(g) discussing results from joint-supervisory activities in cross-border cases as referred to in Article 34;

(h) providing strategic guidance to the CSIRTs network on specific emerging issues;

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

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

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

***(ka) submitting to the Commission for the purpose of review referred to in Article 35 reports on the experience gained at a strategic and operational level;***

***(kb) providing a yearly assessment in cooperation with ENISA, Europol and national law enforcement institutions on which third countries are harbouring ransomware criminals.***

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 ***twice*** a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to ***facilitate*** strategic cooperation and information ***exchange***.

**Recitals:**

(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***, particularly on facilitating alignment in the transposition of this Directive among Member States,*** to be addressed through better implementation of existing rules. ***The Cooperation Group should also map the national solutions in order to promote compatibility of cybersecurity solutions applied to each specific sector across Europe. This is particularly relevant for the sectors that have an international and cross-border nature.***

(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 relevant*** Union bodies and agencies involved in cybersecurity policy, ***such as Europol***, the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work.

**CA Article 13 CSIRTs network (covers Article 13 paragraph 3 and recital 36)**

All related AMs fall, including AMs 51, 352-355, 143 and IMCO 82-87, AFET 9, AFET 36, LIBE 76 and LIBE 22.

*Article 13*

***CSIRTs network***

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

2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs 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;

   ***(aa) facilitating the sharing and transferring of technology and relevant measures, policies, best practices and frameworks among the CSIRTs;***

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

   ***(ba) ensuring interoperability with regard to information sharing standards;***

   (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 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.

**Recitals**

(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 ***Union's interests and*** adequate protection of data. ***This shall not preclude the right of Member States to cooperate with likeminded third countries on management of vulnerabilities and cyber security risk management, facilitating reporting and general information sharing in line with Union law.***

**CA Article 14 EU - CyCLONe (covers Article 14, paragraphs 1, 2 and 4 and recital 27)**

All related AMs fall, including AMs 356-362, AFET 8, AFET 37, AFET 38, IMCO 14, IMCO 88-90, LIBE 77, LIBE 78 and LIBE 19.

*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 ***relevant*** 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' crisis management authorities designated in accordance with Article 7, the Commission and ENISA. ENISA shall provide the secretariat of the ***EU - CyCLONe*** and support the secure exchange of information.
3. EU-CyCLONe shall have the following tasks:
   (a) increasing the level of preparedness of the management of large scale incidents and crises;
   (b) developing a shared situational awareness of relevant cybersecurity events;
   (c) coordinating large scale incidents and crisis management and supporting decision-making at political level in relation to such incidents and crisis;
   (d) discussing national cybersecurity incident and response plans referred to in Article 7(2).
4. EU-CyCLONe shall adopt its rules of procedure.
5. EU-CyCLONe shall regularly report to the Cooperation Group on ***large-scale*** incidents and ***crises, as well as*** 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.

**Recitals:**

(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20], 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 ***or posing serious public security and safety risks for entities or citizens in several Member States or the Union as a whole***. 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.

**CA Article 15 Report on the state of cybersecurity in the Union (covers Article 15, paragraphs 1 and 2)**

All related AMs fall, including AMs 52, 363-370, TRAN 22, IMCO 91-94 and LIBE 79-81.

*Article 15*

***Report on the state of cybersecurity in the Union***

1. ENISA shall issue, in cooperation with the Commission, a biennial report on the state of cybersecurity in the Union ***and submit and present it to the European Parliament***. The report shall ***be delivered in machine-readable format and shall*** in particular include an assessment of the following:

   (a) the development of cybersecurity capabilities across the Union;

   ***(aa) the general level of cybersecurity awareness and hygiene amongst citizens and entities, including SMEs , as well as the general level of security of connected devices;***

   (b) the technical, financial and human resources available to competent authorities and cybersecurity policies, and the implementation of supervisory measures and enforcement actions in light of the outcomes of peer reviews referred to in Article 16;

   (c) a cybersecurity index providing for an aggregated assessment of the maturity level of cybersecurity capabilities ***across the Union***, ***including the alignment of Member States national cybersecurity strategies.***

2. The report shall include in particular ***identification of obstacles and*** 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.

***2a. ENISA, in cooperation with the Commission and with guidance from the Cooperation Group and the CSIRTs network, shall prepare the methodology including the relevant variables of the cybersecurity index referred to in paragraph 1, point (c).***

**CA Article 16 Peer-reviews (covers Article 16, paragraphs 1, 3, 4, 6 and 7, and recital 79)**

All related AMs fall, including AMs 371-381, 204-206, TRAN 23, IMCO 39, IMCO 95, IMCO 96 and LIBE 44.

*Article 16*

**Peer-reviews**

1. The Commission shall establish, after consulting the Cooperation Group and ENISA, and at the latest ***[***by 18 months following the entry into force of this Directive***]***, the methodology and content of a peer-review system for assessing the effectiveness of the Member States' cybersecurity policies. The ***peer-***reviews shall be conducted ***in consultation with ENISA*** by cybersecurity technical experts drawn from ***at least two*** Member States, different than the one reviewed and shall cover at least the following:

   (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;

   (iii) the operational capabilities and effectiveness of CSIRTs ***in executing their tasks***;

   (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 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. ENISA and the Commission shall designate experts to participate as observers in 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 by the Commission, supported by ENISA, and, following consultation of the Cooperation Group, 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, including targeted issues specific to one or several Member States or one or several sectors. ***The designated experts carrying out the review shall communicate those targeted issues to the Member State under peer-review, prior to its commencement.***

***3a. Prior to the commencement of the peer-review process, the Member State under peer-review shall carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated experts.***

4. Peer reviews shall 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. ***The Commission, in cooperation with ENISA, shall develop***

***appropriate codes of conduct underpinning the working methods of designated experts.*** 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.

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 otherwise decided by the Commission, upon consultation with ENISA and the Cooperation Group.

6. Member State***s*** shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Member States, the Commission and ENISA***, before the commencement of the peer-review process.***

7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. ***The reports shall include recommendations to enable improvement on the aspects covered by the peer-review process.*** The reports shall be submitted to the Commission, the Cooperation Group, 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, ***excluding sensitive and confidential information.***

**Recitals**

(79) A peer-review mechanism should be introduced, allowing the assessment by ***independent*** experts designated by the Member States***,*** of the implementation of cybersecurity policies, including the level of Member States' capabilities and available resources. ***Peer-reviews can lead to valuable insights and recommendations strengthening the overall cybersecurity capabilities. In particular, they can contribute in facilitating the transfer of technologies, tools, measures and processes among the Member States involved in the peer-review, creating a functional path for the sharing of best practices across Member States with different levels of maturity in cybersecurity, and enabling the establishment of a high, common level of cybersecurity across the Union. The peer-review should be preceded by a self-assessment by the Member State under review, covering the reviewed aspects and any additional targeted issues communicated by the designated experts to the Member State under peer-review prior to the commencement of the process. The Commission, in cooperation with ENISA and the Cooperation Group, should develop templates for the self-assessment of the reviewed aspects in order to streamline the process and avoid procedural inconsistencies and delays, which Member States under peer-review should complete and provide to the designated experts carrying out the peer-review prior to the commencement of the peer-review process.***

**CA Article 17 Governance (covers Article 17, paragraph 2)**

All related AMs fall, including AMs 382-384, AFET 39 and LIBE 82.

*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 its implementation and be accountable for the non-compliance by the entities with the obligations under this Article.

2. Member States shall ensure that members of the management body ***of essential and important entities*** follow specific training***, and shall encourage essential and important entities to offer similar training to all employees***, 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 ***services provided by*** the entity.

**CA Article 18 Cybersecurity risk management measures (covers Article 18, paragraphs 1, 2, 4, 5 and 6, and recitals 40, 41, 43, 44, 45, 51, 53 and 54)**

All related AMs fall, including AMs 53-55, 385-418, 11, 13, 14, 15, 146-155, 167-176 and 405, IMCO 97-104, TRAN 24-27, AFET 40, and 9, AFET 11-14, IMCO 24, IMCO 27, IMCO 29, IMCO 30, LIBE 83-86, LIBE 24, LIBE 30 and LIBE 31.

*Article 18*

***Cybersecurity risk management measures***

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical***, operational*** and organisational measures to manage the risks posed to the security of network and information systems which those entities use ***for their operations or for*** the provision of their services ***and prevent or minimise the impact of incidents on recipients of their services and on other services***. Having regard to the state of the art ***and to European or international standards*** those measures shall ensure a level of security of network and information systems appropriate to the risk presented.

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 to incidents)~~*;*

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

(d) supply chain security including security-related aspects concerning the relationships between each entity and its 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 (***training,*** testing and auditing) to assess the effectiveness of cybersecurity risk management measures;

***(fa) basic computer hygiene practices and cybersecurity training;***

***(fb) the use of cryptography, such as encryption, where appropriate;***

***(fc) the use of multi-factor authentication or continious authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate;***

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.

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 ***appropriate and proportionate*** 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 of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.~~

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 ***as well as to supplement this Directive by laying down the technical and the methodological specifications of the measures referred to in paragraph 2***.

**Recitals**

(40) Risk-management measures should include measures to identify any risks of incidents, to prevent, detect***, respond to and recover from*** incidents and to mitigate their impact. The security of network and information systems should comprise the security of stored, transmitted and processed data. ***Those systems should provide for systemic analysis, breaking down the various processes and the interactions between subsystems and taking into account the human factor, in order to have a complete picture of the security of the information system.***

(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 the network and information system concerned, taking

into account the state of the art ***and to European or international standards, such as ISO31000 and ISA/IEC 27005,*** of such measures.

(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers, ***such as providers of data storage and processing services or managed security services***; is particularly important given the prevalence of incidents where entities have fallen victim to ***attacks against network and information systems*** 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 ***and resilience*** of products ***and services, the cybersecurity measures embedded in them, and the*** cybersecurity practices of their suppliers and service providers, including their secure development procedures. ***Entities should in particular be encouraged to incorporate cybersecurity measures into contractual arrangements with their first-level suppliers and service providers. Entities could consider cybersecurity risks stemming from other levels of suppliers and service providers.***

(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 ***prevent,*** detect, respond to ***or recover from*** 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.

(45) Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem***, including to counter industrial espionage and to protect trade secrets***. 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.

***(45a) Entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust architecture, software updates, device configuration, network segmentation, identity and access management or user awareness, and organise training for their staff regarding corporate email cyber threats, phishing or social engineering techniques. Furthermore, entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies driven by artificial intelligence or machine learning systems to automate their capabilities and the protection of network architectures.***

(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 ***all*** public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report ***significant*** incidents in relation thereto. ***Member States should ensure that the integrity and availability of those public electronic communications networks are maintained and should consider their protection from***

***sabotage and espionage of vital security interest. Information about incidents on, for example on submarine communication cables, should be shared actively between Member States.***

(53) Providers of public electronic communications networks or publicly available electronic communications services, should ***implement security by design and by default, and*** inform the service recipients of particular and significant cyber threats and of measures they can take to protect the security of their ***devices and*** communications, for instance by using specific types of ***encryption*** software or ***other data-centric security*** technologies.

(54) In order to safeguard the security of electronic communications networks and services, the use of ***encryption and other data-centric security technologies, such as***, ***tokenisation, segmentation, throttle access, marking, tagging, strong identity and access management, and automated access decisions***, 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. ***However, this should not lead to any efforts to weaken end-to-end encryption, which is a critical technology for effective data protection and privacy.***

***(54a) In order to safeguard the security and to prevent abuse and manipulation of electronic communications networks and services, the use of interoperable secure routing standards should be promoted to ensure the integrity and robustness of routing functions across the ecosystem of internet carriers.***

***(54b) In order to safeguard the functionality and integrity of the internet and to reduce security issues relating to DNS, relevant stakeholders including Union businesses, internet service providers and browser vendors should be encouraged to adopt a DNS resolution diversification strategy. Furthermore, Member States should encourage the development and use of a public and secure European DNS resolver service.***

**CA Article 19 EU coordinated risk assessments of critical supply chains (covers Article 19, paragraphs 1 and 2, and recitals 46 and 47)**

All related AMs fall, including AMs 419-423, 10, 137, 156-160, IMCO 105, AFET 41-43, TRAN 15, AFET 15, IMCO 25, IMCO 26, LIBE 87 and LIBE 26.

*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 ***and ICS*** services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.

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

**Recitals**

(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 supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21], with the aim of identifying per sector which are the critical ICT ***and ICS*** services, systems or products, relevant threats and vulnerabilities. ***Such risk assessments should identify measures, mitigation plans and best practices against critical dependencies, potential single points of failure, threats, vulnerabilities and other risks associated with the supply chain and should explore ways to further encourage their wider adoption by entities. Potential non-technical risk factors, such as undue influence by a third country on suppliers and service providers, especially in the case of alternative models of governance, include concealed vulnerabilities or backdoors and potential systemic supply disruptions, especially in case of technological lock-in or provider dependency.***

(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 ***throughout their entire lifecycle*** against disruptive events and (v) for emerging ICT services, systems or products, their potential future significance for the entities' activities. ***Furthermore, particular emphasis should be placed on ICT services, systems or products that are subject to specific requirements stemming from third countries.***

***(47a) The Stakeholder Cybersecurity Certification Group established pursuant to Article 22 of Regulation (EU) 2019/881 should issue an opinion on security risk assessments of specific critical ICT and ICS services, systems or products supply chains. The Cooperation Group and ENISA should take into account that opinion.***

**CA Article 20 Reporting obligations (covers Article 20, paragraphs 1-11 and recitals 52 and 55)**

All related AMs fall, including AMs 56-68, 424-485, 12, 16, 177-179, TRAN 28-30, IMCO 106-123, TRAN 16, IMCO 28, IMCO 31, LIBE 88-94 and LIBE 29.

*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 ***significant*** incident~~on the provision of their services~~. Member States shall ensure that those entities report, among others, any information enabling the CSIRT to determine any cross-border impact of the incident.

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 notification shall not make the notifying entity subject to increased liability.~~

   ***Where applicable, Member States shall ensure that essential and important entities inform the recipients of their services, without undue delay, of protective measures or remedies to particular incidents and known risks, which can be taken by the recipients. Where appropriate, the entities shall inform the recipients of their services of the incident or the known risk itself. Informing of recipients shall take place on a 'best efforts' basis and shall not subject the notifying entity to an increase in liability.***

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

   ~~(a) the incident has caused or has the potential to cause 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.~~

   ***In order to determine the significance of the incident, where available, the following parameters shall be taken into account:***

   ***(a) the number of recipients of the services affected by the incident;***

   ***(b) the duration of the incident;***

   ***(c) the geographical spread of the area affected by the incident;***

   ***(d) the extent to which the functioning and continuity of the service is affected;***

   ***(e) the extent of impact on economic and societal activities.***

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) ***an initial notification of the significant incident, which shall contain information available to the notifying entity on a best efforts basis as follows:***

***(i) with regard to incidents that significantly disrupt the availability of the services provided by the entity, the CSIRT shall be notified without undue delay and in any event within 24 hours of becoming aware of the incident;***

***(ii) with regard to incidents that have a significant impact on the entity other than on the availability of the services provided by that entity, the CSIRT shall be notified without undue delay and in any event within 72 hours of becoming aware of the incident;***

***(iii) with regard to incidents that have a significant impact on the services of a trust services provider as defined in Article 3, point (19) of Regulation (EU) No 910/2014 or on the personal data maintained by that trust service provider, the CSIRT shall be notified without undue delay and in any event within 24 hours of becoming aware of the incident;***

(b) ***an intermediate report on relevant status updates,*** upon the request of a CSIRT;

(c) a ***comprehensive*** report not later than one month after the submission of the ***initial notification***, 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.

***(ca) in the case of an ongoing incident at time of the submission of the comprehensive report referred to in point (c), a final report shall be provided one month after the incident has been resolved.***

Member States shall provide that in duly justified cases and in agreement with the the CSIRT, the entity concerned can deviate from the deadlines laid down in points (a***)(i) and (ii), point (c). Member States shall ensure the confidentiality and appropriate protection of sensitive information about incidents shared with CSIRTs, and shall adopt measures and procedures for sharing and reuse of incident information.***

***4a. Member States shall establish a single entry point for all notifications required under this Directive and other relevant Union law. ENISA, in cooperation with the Cooperation Group, shall develop and continuously improve common notification templates by means of guidelines to simplify and streamline the reporting information required under Union law and decrease the burdens on reporting entities.***

***4b. Essential and important entities referred to in Article 24(1) may meet the requirements of paragraph 1 of this Article by notifying the CSIRT of the Member State in which the entities have the main establishment within the Union, and by notifying the essential and important entities they provide services to of any significant incident that is known to impact the recipient of the services.***

5. The CSIRT shall provide, within 24 hours 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 ***the*** request of the entity, guidance ***and actionable advice*** on the implementation of possible mitigation measures. CSIRT shall provide additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the CSIRT shall also provide guidance on reporting the incident to law enforcement authorities. ***The CSIRT may share information on the incident with other important and essential entities, while ensuring the confiditionality of the information provided by the reporting entity.***

6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the CSIRT shall inform the other affected Member States and ENISA of the incident ***and provide relevant information***. In so doing, the 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.

***7a*** ***CSIRTs shall, without undue delay, provide the single point of contact and where relevant, the competent authorities, with the information on significant incidents notified in accordance with paragraph 1.***

8. At the request of 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, ***while ensuring confidentiality and appropriate protections of the information provided by the reporting entity.***

9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraph 1 ***of this Article*** ~~and 2~~ and 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.

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 paragraph 1 ***of this Article and Article 27*** ~~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 procedure of a notification submitted pursuant to paragraph 1 ***of this Article and Article 27*** ~~and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3.~~ Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

***11a.*** ***The Commission is empowered to adopt delegated acts, in accordance with Article 36, to supplement this Directive by specifying the type of information to be submitted***

***pursuant to paragraph 1 of this Article and by further specifying the parameters which are to be taken into account when determining the significance of an incident as referred to in paragraph 3 of this Article.***

**Recitals**

(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. ***This*** 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 ***and drafted in a language easily comprehensible***.

(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 72 hours~~, followed by a ***comprehensive*** report not later than one month after ***the submission of the initial notification***. ***The initial incident notification timeline should not preclude entities from reporting incidents earlier, therefore allowing them to seek support from CSIRTs swiftly enabling the mitigation and the potential spread of the reported incident. CSIRTs can request an intermediate report on relevant status updates, while taking into account the incident response and remediation efforts of the reporting entity.***

**(55a)** ***A significant incident may have an impact on the confidentiality, integrity or availability of the service. Essential and important entities should notify CSIRTs about significant incidents that have an impact on the availability of their service within 24 hours of becoming aware of the incident. They should notify CIRTs about significant incidents that breach the confidentiality and integrity of their services within 72 hours of becoming aware of the incident. The distinction between the types of incidents is not based on the seriousness of the incident, but on the difficulty for the reporting entity to assess the incident, its significance and the ability to report information that can be of use for the CSIRT.*** The initial notification should include the information ~~strictly~~ necessary to make the ~~competent authorities~~ ***CSIRT*** aware of the incident and allow the entity to seek assistance, if required. 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 72 hours~~ for the initial notification and ~~one month~~ for the ***comprehensive*** report.

**CA Article 21 Use of European cybersecurity certification schemes (covers Article 21, paragraphs 1-3)**

All related AMs fall, including AMs 486-500, 69, 70, IMCO 124, IMCO 125 and TRAN 31-34.

*Article 21*

***Use of European cybersecurity certification schemes***

1. Member States ***shall***, ***following guidance from ENISA, the Commission and the Cooperation Group, encourage*** essential and important entities to certify certain ICT products, ICT services and ICT processes***, either developed by the essential or important entity or procured from third parties,*** under European cybersecurity schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 ***or, if not yet available, under similar internationally recognised*** certification ***schemes. Furthermore, Member States shall encourage essential and important entities to use qualified trust services pursuant to Regulation (EU) No 910/2014.***

2. The Commission ***is*** empowered to adopt delegated acts, ***in accordance with Article 36, to supplement this Directive by specifying which categories of essential and important entities are required to obtain a certificate under specific European cybersecurity schemes pursuant to Article 49 of Regulation (EU) 2019/881. Such delegated acts shall be considered where insufficient levels of cybersecurity have been identified, shall be preceded by an impact assessment and shall provide for an implementation period.***

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

**CA Article 22 Standardisation (covers Article 22, paragraph 2)**

All related AMs fall, including IMCO 126, IMCO 127 and LIBE 95.

*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, ***and where appropriate after consulting relevant stakeholders,*** shall draw up advice and guidelines regarding the technical areas

to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.

***3. The Commission, in collaboration with ENISA, shall support and promote the development and implementation of standards set by relevant Union and international standardisation bodies for the convergent implementation of Article 18 (1) and (2). The Commission shall support the update of the standards in the light of technological developments.***

**CA Article 23 Database structure of domain names and registration data (covers Article 23, paragraphs 1-5 and recitals 59-62)**

All related AMs fall, including AMs 71-76, 501-508, IMCO 128-133, and 17-19, 180-185 and 187, IMCO 33, IMCO 34, LIBE 96-100, LIBE 35 and LIBE 36.

*Article 23*

***Database structure of domain names and registration data***

1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ***require*** TLD registries and entities providing domain name registration services to collect and maintain accurate***, verified*** and complete domain name registration data in a database ***structure operated for that purposes***.

2. Member States shall ensure that the ***database structure*** of domain name registration data referred to in paragraph 1 ***contains*** relevant information***, which shall include at least the registrants' name, their physical and email address as well as their telephone number,*** to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.

3. Member States shall ensure that TLD registries and entities providing domain name registration services have policies and procedures in place to ensure that the ***database structure includes*** accurate***, verified*** and complete information. Member States shall ensure that such policies and procedures are made publicly available.

4. Member States shall ensure that TLD registries and entities providing domain name registration services ***make publicly available***, without undue delay after the registration of a domain name, domain registration data which are not personal data. ***For legal persons as registrants, the domain registration data publicly available shall include at least the registrants' name, their physical and email address as well as their telephone number.***

5. Member States shall ***require*** TLD registries and entities providing domain name registration services ***to*** provide access to specific domain name registration data***, including personal data,*** upon duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ***require*** TLD registries and entities providing domain name registration services ***to*** reply without undue delay ***and in any event within 72 hours upon the receipt of the*** requests for

access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

**Recitals**

(59) Maintaining accurate***, verified*** and complete databases of domain names registration data (so called 'WHOIS 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, ***and for tackling illegal activities***. ***TLD registries and entities providing domain name registration services should therefore be required to collect domain name registration data, which should include at least the registrants' name, their physical and email address as well as their telephone number. In practice, the collected data may not always be thoroughly accurate, however TLD registries and entities providing domain name registration services should adopt and implement proportionate processes to verify that natural or legal persons requesting or owning a domain name have provided contact details on which they can be reached and are expected to reply. Using a 'best efforts' approach, these verification processes should reflect the current best practices used within the industry. Those best practices in the verification process should reflect the advances being made in the electronic identification process. The TLD registries and entities providing domain name registration services should make publicly available their policies and procedures to ensure the integrity and availability of the domain name registration data.*** Where processing includes personal data such processing shall comply with Union data protection law.

***(60)*** TLD registries and entities providing domain name registration services should ***be required to*** make publicly available domain name registration data ***that does not contain personal data. A distinction should be made between natural and*** legal persons[25]***. For legal persons, TLD registries and entities should make publicly available at least the registrants' name, their physical and email address as well as their telephone number. The legal person should be required to either provide a generic email address that can be made publicly available or give consent to the publication of a personal email address. The legal person should be able to demonstrate such consent at the request of TLD registries and entities providing domain name registration services.***

***(61) The availability and timely accessibility of the domain name registration data to legitimate access seekers is essential for cybersecurity purposes and tackling illegal activities in the online ecosystem.*** TLD registries and entities providing domain name registration services should ***therefore be required to enable*** lawful access to specific domain name registration data, ***including personal data,*** to legitimate access seekers, in accordance with Union data protection law. ***Legitimate access seekers should make a duly justified request to access domain name registration data on the basis of Union or national law, and could include competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, and national CERTs or CSIRTs***. Member States should ensure that TLD registries and entities providing domain name registration services should respond without undue delay ***and in any event within 72 hours*** to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and entities providing domain name registration services 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 tools to provide an efficient system for requesting

and accessing registration data. 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.

**CA Article 24 Jurisdiction and territoriality (covers Article 24, paragraph 2 and recitals 63 and 64)**

All related AMs fall, including AMs 509-516, 188, 189, AFET 44, IMCO 134, LIBE 101, LIBE 37 and LIBE 38.

*Article 24*

***Jurisdiction and territoriality***

1. DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery network providers referred to in point 8 of Annex I, as well as digital providers referred to in point 6 of Annex II shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union.

2. For the purposes of this Directive, entities referred to in paragraph 1 shall be deemed to have their main establishment in the Union in the Member State where the decisions related to the cybersecurity risk management measures are taken. If such decisions are not taken in any establishment in the Union, the main establishment shall be deemed to be in the Member State ***either*** where the entities have the establishment with the highest number of employees in the Union, ***or the establishment where cybersecurity operations are carried out.***

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.

**Recitals**

(63) All essential and important entities under this Directive should fall under the jurisdiction of the Member State where they provide their services ***or carry out their activities***. 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, 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 taken in the Union. This will typically correspond to the place of the companies' central administration in the Union. If such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States ***either*** where the entity has an establishment with the highest number of employees in the Union ***or the establishment where cybersecurity operations are carried out***. 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.

**CA Article 25 ENISA registry (covers Article 25, paragraph 1)**

All related AMs fall, including AMs 21 and 517-521, IMCO 135, AFET 44 and LIBE 102.

*Article 25*

***ENISA registry***

1. ENISA shall create and maintain a ***secure*** registry for essential and important entities referred to in Article 24(1)***, which shall include*** the following information:

   (a) the name of the entity;

   (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***, IP ranges,*** telephone numbers ***and relevant sector(s) and subsector(s) of the entities referred to in Annexes I and II***.

   ***By ... [12 months after the date of entry into force of this Directive], the essential and important entities shall submit the information refered to in the first subparagraph to ENISA.***

2. The entities referred to in paragraph 1 shall notify ENISA about any changes to the details they submitted under paragraph 1 without delay, and in any event, within two weeks from the date on which the change took effect.

3. Upon receipt of the information under paragraph 1, ENISA shall forward 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. 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.

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.

**Recitals**

***(65a) ENISA should create and maintain a registry containing information about essential and important entities that comprise DNS service providers, TLD name registries and providers of cloud computing services, data centre services, content delivery networks, online marketplaces, online search engines and social networking platforms. Those essential and important entities should submit to ENISA their names, addresses and up-to-date contact details. They should notify ENISA about any changes to those details without delay and, in any event, within two weeks from the date on which the change took effect. ENISA should forward the information to the relevant single point of contact. The essential and important entities submitting their information to ENISA are therefore not required to separately inform the competent authority within the Member State. ENISA should develop a simple publicly available application programme that those entities could use to update their information. Furthermore, ENISA should establish appropriate information classification and management protocols to ensure the security and confidentiality of disclosed information, and restrict the access, storage, and transmission of such information to intended users***.

**CA Article 26 Cybersecurity information sharing arrangements (covers Article 26, paragraphs 1-3)**

All related AMs fall, including AMs 77-81, 522-534, 537, 22, IMCO 136-138 and LIBE 103.

*Article 26*

***Cybersecurity information-sharing arrangements***

1. Member States shall ensure that essential and important entities ***and other relevant entities not covered by the scope of this Directive*** may exchange relevant cybersecurity information among themselves including information relating to cyber threats, ***near misses,*** vulnerabilities, techniques and procedures, ***metadata and***

***content data, indicators of compromise, adversarial*** tactics, ***modus operandi, actor specific information,*** cybersecurity alerts***, industrial espionage tactics*** and ***recommended security tool configurations***, 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***, containment and prevention*** techniques, mitigation strategies, response and recovery stages ***or promoting collaborative cyber threat research between public and private entities***.

2. Member States shall ***facilitate*** the exchange of information ***by enabling the establishment of*** trusted communities of essential and important entities ***and their service providers or, where relevant, other suppliers***. 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 ***facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by making*** operational elements (including the use of dedicated ICT platforms ***and automation tools***) ***and*** content ***available. Member States*** shall lay down the details of the involvement of public authorities in such arrangements ***and may impose certain conditions on the information made available by competent authorities or CSIRTs***. 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.

**CA Article 27 (covers Article 27 and recitals 66 and 68)**

All related AMs fall, including AMs 82, 535-539, 22, 23, 192, AFET 16, AFET 17, IMCO 35 and IMCO 140.

*Article 27*

***Voluntary notification of relevant information***

Member States shall ensure that ***notifications may be submitted to the CSIRT, on a voluntary basis, by:***

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

***(b)*** entities falling outside the scope of this Directive***, with regard to significant*** incidents, cyber threats or near misses.
~~, 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 ***such*** 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. ***Where necessary, CSIRTs shall provide the single point of contact and, where relevant, the competent authorities, with the information on notifications received pursuant this Article, while ensuring confidentiality and appropriate protections of the information provided by the reporting entity.*** Voluntary ***notification*** 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.

**Recitals**

(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. ***In addition, ENISA should have the infrastructure, procedures and rules in place to handle sensitive and classified information in compliance with the applicable security rules for protecting EU classified information.***

(68) Entities should be encouraged ***and supported by Member States*** 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, ***such as entities focusing on cybersecurity services and research,*** 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.

**Article 28 (covers Article 28, paragraph 2)**

All related AMs fall, including AM 540, IMCO 141, IMCO 142 and LIBE 104.

*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.

2. Competent authorities shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches. ***This shall be done in accordance with their competence and tasks pursuant to Regulation (EU) 2016/679.***

**CA Article 29 Supervision and enforcement for essential entities (covers Article 29, paragraphs 2, 4, 5, 7 and 9, and recitals 71, 72 and 76)**

All related AMs fall, including AMs 83-87, 541-571, IMCO 143-147, AFET 45, AMs 198-203, IMCO 38, LIBE 105-113, LIBE 40 and LIBE 42.

*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, have the power to subject those entities to:

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

   ***(aa) investigation of cases of non-compliance and the effects thereof on the security of the services;***

   ~~(b) regular audits;~~

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

   ***(b) annual and targeted security audits carried out by a qualified independent body or a competent authority;***

   ***(c) ad hoc audits in cases justified on the ground of a significant incident or non-compliance by the essential entity;***

   (d) security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria;

   (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.

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

***The results of any targeted security audit shall be made available to the competent autority. The costs of such an audit carried out by a qualified independent body shall be paid by the entity concerned.***

***2a. Where exercising their powers under points (a) to (d) in paragraph 2, the competent authorities shall minimise the impact on the business processes of the entity.***

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 to:

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

(b) issue binding instructions***, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation,*** or an order requiring 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 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 their 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;

~~(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 ***in accordance with*** national ***law*** 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)*** ***temporarily*** suspend or request a certification or authorisation body to ***temporarily*** suspend a certification or authorisation concerning part or all ***relevant*** services or activities provided by an essential entity

(b) ***as ultima ratio,*** ~~impose or~~ request the imposition by the relevant bodies or courts ***in accordance with*** national ***law*** 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.

***Temporary suspensions or bans pursuant to this paragraph*** shall be applied only until the entity ***concerned*** takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such sanctions were applied. ***The imposition of such temporary suspensions or bans 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.***

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.

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 damage caused or losses incurred***, including*** financial or economic losses, effects on other services ***and the*** number of users affected;

***(ca) any relevant previous infringements by the entity concerned;***

(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 inform the relevant competent authorities of ***all relevant*** Member ***States*** 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. Upon request of competent authorities under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], competent authorities may exercise their supervisory and enforcement powers on an essential entity identified as critical or equivalent.

***9a. Member States shall ensure that their competent authorities cooperate with the relevant competent authorities of the Member State concerned designated pursuant to Regulation (EU) XXXX/XXXX [DORA].***

**Recitals**

(71) In order to make enforcement effective, a minimum list of administrative ***penalties*** 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 ***penalties*** 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 penalties, including administrative fines, should ***be proportionate and their imposition 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, due process***, the presumption of innocence and the rights of defence***.

(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 ***if the infringement was intentional, negligent or the entity concerned had received notice of the entity's non-compliance***.

(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 ***a temporary*** suspension of a certification or authorisation concerning part or all ***relevant*** services provided by an essential entity and the ***request to impose*** a temporary ban from the exercise of managerial functions by a natural

person ***at chief executive officer or legal representative level***. ***Member States should develop specific procedures and rules concerning the temporary ban from the exercise of managerial functions by a natural person at chief executive officer or legal representative level in public administration entities. In the process of developing such procedures and rules, Member States should take into account the particularities of their respective levels and systems of governance within their public administrations.*** Given their severity and impact on the entities' activities and ultimately on their consumers, such ***temporary suspensions or bans*** 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 ***temporary suspensions or bans*** 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 ***temporary suspensions or bans*** were applied. The imposition of such ***temporary suspensions or bans*** 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.

**CA Article 30 Supervision and enforcement for important entities (covers Article 30, paragraphs 1, 2 and 4)**

All related AMs fall, including AMs 88, 89, 572-578, IMCO 148-150, AFET 46, LIBE 114 and LIBE 115.

*Article 30*

**Supervision and enforcement for important entities**

1. When provided with evidence or indication 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. ***Member States shall ensure that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.***

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

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

   ***(aa) investigation of cases of non-compliance and the effects thereof on the security of the services;***

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

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

(c) security scans based on objective***, non-discrimantory***, fair and transparent risk assessment criteria;

(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.

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

***The results of any targeted security audit shall be made available to the competent autority. The costs of such an audit carried out by a qualified independent body shall be paid by the entity concerned.***

3. Where exercising their powers pursuant to points (d) or (e) 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 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 any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;

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

(g) order those entities to make public aspects of non-compliance with their obligations laid down in this Directive in a specified manner;

~~(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 ***in accordance with*** national ***law*** 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 Annex II.

**CA Article 31 General conditions for imposing administrative fines on essential and important entities (covers Article 31, paragraph 2)**

All related AMs fall, including AMs 90, 579, 580, IMCO 151, LIBE 116 and LIBE 117.

*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 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.

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.

**CA Article 32 Infringements entailing a personal data breach (covers Article 32 paragraphs 1 and 3)**

All related AMs fall, including AMs 581-583, IMCO 152, IMCO 153 and LIBE 119.

*Article 32*

***Infringements entailing a personal data breach***

1. Where the competent authorities have indications that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 entails a personal data breach, as defined ***in*** Article 4, ***point*** (12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ~~not later than~~ ***without undue delay and in any event within 72 hours of becoming aware of a data breach.***

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(i) of that Regulation and impose an administrative fine, the competent authorities shall not impose an administrative fine for the same infringement 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 ***shall*** inform the supervisory authority established in the same Member State.

**CA Article 33 Penalties**

No AMs tabled, Commission proposal remains unchanged.

*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.

**CA Article 34 Mutual assistance**

All related AMs fall, including AM 584 and LIBE 120. Commission proposal remains unchanged.

*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 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 the requested assistance is not proportionate to the supervisory tasks of the competent authority carried out in accordance with Article 29 or Article 30.

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.

**CA Article 35 Review (covers Article 35, first paragraph and recitals 82 and 84)**

All related AMs fall, including AMs 584-586 and 596, LIBE 121 and LIBE 46.

*Article 35*
**Review**

***By ... [42 months after the date of entry into force of this Directive] and every 36 months thereafter,*** 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 ***the*** sectors, subsectors, size and type of entities referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. ***To that end*** and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level.

***The report shall be accompanied, where necessary, by a legislative proposal.***

**Recitals**

(82) The Commission should periodically review this Directive, in consultation with interested parties, in particular with a view to determining ***whether it is appropriate to propose amendments*** in the light of changes to societal, political, technological or market conditions. As part of th***ose*** review***s, the Commission should assess the relevance of the sectors, subsectors and types of entities referred to in the annexes for the functioning of the economy and society in relation to cybersecurity. The Commission should assess, inter alia, whether digital providers that are classified as very large online platforms within the meaning of Article 25 of Regulation (EU) XXXX/XXXX [Single Market For Digital Services (Digital Services Act) or as gatekeepers as defined in Article 2, point 1 of Regulation (EU) XXXX/XXXX [Contestable and fair markets in the digital sector (Digital Markets Act)], should be designated as essential entities under this Directive. Furthermore, the Commission should assess whether it is appropriate to amend Annex I to the Directive 2020/1828 of the European Parliament and of the Council[15] by adding a reference to this Directive.***

(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 includes the right to an effective remedy before a court for the recipients of services provided by essential and important entities.*** This Directive should be implemented in accordance with those rights and principles**.**

***[15] Directive 2020/1828 of the European Parliament and of the Council of 25 November 2020 on Representative Actions for the Protection of the Collective Interests of Consumers (OJ L 409, 4.12.2020, p. 1).***

**CA Article 36 Exercise of the delegation (covers Article 36, paragraphs 2 and 3 and recital 80)**

All related AMs fall, including AMs 587, 207, 208, IMCO 40 and IMCO 154-156.

*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)***, 20(11a)*** 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)***, 20(11a)*** 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), ***20(11a)*** 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.

**Recitals**

(80) In order to take into account 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 and reporting obligations*** required by this Directive. The Commission should also be empowered to adopt delegated acts establishing which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. 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-Making. 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.

**CA Article 37 Committee procedure (covers recital 81)**

All related AMs fall, including AM 588 and IMCO 41. Commission proposal remains unchanged.

*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.

**Recitals**

(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, 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.

**CA Article 38 Transposition**

All related AMs fall, including AMs 589 and 590. Commission proposal remains unchanged.

*Article 38*
**Transposition**

1. Member States shall adopt and publish, by … [18 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.

**CA Article 39 Amendment of Regulation (EU) No 910/2014**

All related AMs fall, including AMs 591 and 592. Commission proposal remains unchanged.

*Article 39*
**Amendment of Regulation (EU) No 910/2014**

Article 19 of Regulation (EU) No 910/2014 is deleted.

**CA Article 40 Amendment of Directive (EU) 2018/1972**

All related AMs fall, including AMs 593-596. Commission proposal remains unchanged.

*Article 40*
**Amendment of Directive (EU) 2018/1972**

Articles 40 and 41 of Directive (EU) 2018/1972 are deleted.

**CA Article 41 Repeal**

No AMs tabled. Commission proposal remains unchanged.

*Article 41*
**Repeal**

Directive (EU) 2016/1148 is repealed with effect from.. [ date of transposition deadline of the Directive].

References to Directive (EU) 2016/1148 shall be construed as references to this Directive and read in accordance with the correlation table set out in Annex III.

**CA Article 42 Entry into force**

All related AMs fall, including AM 597.

*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.

***However, Articles 39 and 40 shall apply from ... [18 months after the date of entry into force of this Directive].***

**CA Article 43 Addressees (covers recital 82a)**

All related AMs fall, including AM 25. Commission proposal remains unchanged.

*Article 43*
**Addressees**

This Directive is addressed to the Member States.

**Recital**

***82a*** ***This Directive lays down cybersecurity requirements in the area of cybersecurity for Member States as well as essential and important entities established in the Union. Those cybersecurity requirements should also be applied by the Union institutions, bodies, offices and agencies on the basis of a Union legislative act.***