Conseil de
l'Union européenne

Bruxelles, le 17 juin 2022
(OR. fr, en)

10193/22

Dossier interinstitutionnel:
2020/0359(COD)

LIMITE

CYBER 219
TELECOM 271
CSC 262
CSCI 84
DATAPROTECT 190
JAI 884
MI 472
CODEC 907

NOTE

Origine:	la présidence
Destinataire:	Comité des représentants permanents
Nº doc. préc.:	10356/22
N° doc. Cion:	14150/20 + ADD 1
Objet:	Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 - Analyse du texte de compromis final en vue d'un accord

I. INTRODUCTION

1. Le 16 décembre 2020, la Commission a adopté la proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (ci-après dénommée "directive NIS 2")[1], dans le but de remplacer l'actuelle directive sur la sécurité des réseaux et des systèmes d'information (ci-après dénommée "directive NIS")[2].

[1] 14150/20 + ADD 1, COM(2020) 823 final.
[2] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, OJ L 194 du 19 juillet 2016, p. 1.

2. Cette proposition était l'une des mesures prévues dans la stratégie de cybersécurité de l'UE pour la décennie numérique[3] en vue de faire en sorte que les citoyens et les entreprises bénéficient de technologies numériques dignes de confiance.

3. La proposition est fondée sur l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE) et a pour objectif d'améliorer la résilience et les capacités de réaction aux incidents des entités publiques et privées, des autorités compétentes et de l'Union dans son ensemble.

4. Le Contrôleur européen de la protection des données a rendu son avis le 11 mars 2021[4].

5. Le 3 février 2021, le Coreper a décidé de consulter le Comité européen des régions sur la proposition[5]. Le 20 avril 2021 le Comité européen des régions a décidé de ne pas rendre son avis[6].

6. Le Comité économique et social européen a adopté son avis le 28 avril 2021.

7. Au Parlement européen, la commission de l'industrie, de la recherche et de l'énergie (ITRE), compétente pour la proposition, a adopté son rapport le 28 octobre 2021[7].

8. Le Conseil a adopté une orientation générale le 3 décembre 2021[8].

---

3 14133/20.
4 7151/21.
5 5573/21.
6 8491/21.
7 A9-0313/2021.
8 14337/21.

II. NEGOCIATIONS AVEC LE PARLEMENT

9. Les discussions interinstitutionnelles sur la proposition ont débuté le 13 janvier 2022 avec un trilogue politique. Depuis lors, 28 réunions techniques ont eu lieu et deux autres trilogues politiques, le 17 février et le 12 mai 2022. Un accord provisoire a été trouvé entre les co-législateurs le 12 mai sur le texte figurant à l'annexe de la présente note. Ce texte a été finalisé au niveau technique le 16 juin 2022. En substance, le texte correspond en grande partie au mandat révisé approuvé par le Coreper le 11 mai qui incluait également une marge de flexibilité sur certains points. De nouvelles formulations ont été convenues concernant les points suivants :

- le champ d'application (article 2) et plus particulièrement l'approche proportionnée (art. 18(1)), la clause d'exclusion et l'inclusion des administrations publiques,
- le mécanisme de notification (article 2a),
- l'introduction du concept « active cyber protection » (article 5),
- le rôle de la Commission dans CyCLONe (article 14),
- les revues par les pairs (article 16(3a)),
- les obligations de notification (article 20(4)(a)),

– la mise en place d'un point d'entrée unique pour la notification d'incidents (article 11(5a)),

– les sanctions (article 31(4)),

– l'intégration des secteurs « recherche » et « opérateurs de services de recharge intelligente pour les véhicules électriques » (annexe),

– les actes d'exécution pour les articles 18 et 20, les actes délégués pour la certification (article 21),

– le délai de transposition (article 38).

III. CONCLUSION

10. À la lumière de ce qui précède, le Comité des représentants permanents est invité à :

(a) confirmer son accord sur le texte de compromis final qui figure à l'annexe de la présente note;

(b) autoriser la Présidence à adresser une lettre au Président de la Commission ITRE du Parlement européen confirmant que, si le Parlement européen adoptait sa position en première lecture, conformément à l'article 294, paragraphe 3, du traité, dans les termes du compromis figurant dans le texte de compromis figurant en annexe (sous réserve de mise au point par les juristis-linguistes par les deux institutions), le Conseil approuverait, conformément à l'article 294, paragraphe 4 du traité, la position du Parlement européen et l'acte serait adopté dans la formulation qui correspond à la position du Parlement européen.

PE-CONS – 2020/0359(COD)

DIRECTIVE (EU) 2022/...
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of ....

on measures for a high common level of cybersecurity across the Union *(NIS 2 Directive)*, repealing Directive (EU) 2016/1148

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[9],

Having regard to the opinion of the Committee of the Regions[10],

Acting in accordance with the ordinary legislative procedure,

[9] OJ C , , p. .
[10] OJ C , , p. .

Whereas:

(1) Directive (EU) 2016/1148 of the European Parliament and the Council[11]***, 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 ▌.

(2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national ▌strategies ***on security of network and information systems***, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group[12] and ***the*** network of national Computer Security Incident Response Teams ('CSIRTs network')[13]. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges.

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

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

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

(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence and cause major damage to the Union economy and society. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market. ***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 and for the protection of its people, businesses and institutions against cyber incidents and threats, as well as for enhancing the trust of individuals and organisations in the EU's ability to promote and protect a global, open, free, stable and secure cyberspace grounded in human rights, fundamental freedoms, democracy and the rule of law.

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

(5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different ***measures. Ultimately, those divergences could 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)***.

(5a) Ensuring adequate resources to fulfill the objectives of this Directive and to carry out the tasks foreseen for competent authorities and CSIRTs is essential. The Member States can introduce at the national level financing mechanism to cover necessary expenditure in relation to the conduct of tasks of public entities responsible for cybersecurity in the Member State pursuant to this Directive. Such mechanism should comply with Union law and should be proportionate, non-discriminatory and take into account different approaches to providing secure services.

(6) ▌Member States ***should be able*** 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***.*** ***For that purpose, Member States may decide that specific essential and important entities that carry out activities or provide services in these areas should not be obliged to comply with the legal obligations laid out in this Directive as regards those activities or those services. Where an essential or important entity provides an exclusive service to a public administration that is excluded from the scope of this Directive, Member States may decide that this entity is not obliged to comply with legal obligations under this Directive in regards to the exclusive service. Furthermore,*** no Member State ***should*** be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. ▌National ***or*** Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[14], are of relevance.

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

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

(6b) The exclusion of public administration entities from the scope of this Directive should apply to those entities whose activities are predominantly carried out in the areas of defence, national security, public security, or law enforcement. Public administration entities whose activities are only marginally related to such areas should still be covered by this Directive. For the purpose of this Directive, entities with regulatory competences are not considered as carrying out activities in the area of law enforcement and, therefore, are not excluded on these grounds from the scope of this Directive. Public administration entities that are jointly established with a country outside the EU in accordance with an international agreement, are not within the scope of this Directive. This Directive does not apply to Member States' diplomatic and consular missions in third countries and to their network and information systems, insofar as such systems are located in the premises of the mission or are operated for users in a third country. Given the intensification and increased sophistication of cyber threats, Member States should strive to ensure that entities that are excluded from the scope of this Directive achieve a high level of cybersecurity, and to support the implementation of equivalent cybersecurity risk management measures that reflect the sensitive nature of these entities.

(6c) Although the Directive applies to entities carrying out activities in the production of electricity from nuclear power plants, certain activities may be linked to national security. In that case, a Member State should be able to exercise its responsibility to safeguard its national security with respect to those activities, including activities within the nuclear value chain, in accordance with the Treaties.

(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. ***In particular this Directive*** should ***aim to overcome the shortcomings of the differentiation between*** operators of essential services ***and*** digital service providers***, which*** 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/EC[15], that operate within the sectors or provide the type of services covered by this Directive, fall within its scope. ▌

[15] 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).

(8a) ***In order to avoid entities having partner enterprises or linked enterprises from being disproportionately considered as essential or important entities, Member States, when applying Article 6(2) of the Annex to Commission Recommendation 2003/361/EC, are able to take into account the degree of independence an entity enjoys in relation to its partner and linked enterprises. In particular, Member States are able to take into account the fact that the entity is independent from its partner or linked enterprises in terms of the network and information systems that they use in the provision of their services and in terms of the services an entity provides. On that basis, where appropriate, a Member State is able to consider such an entity as not meeting or exceeding the threshold for medium-sized enterprises laid down in Article 2 of the Annex to that Recommendation, if, after taking into account the degree of independence, that entity would not have been considered as meeting or exceeding that threshold if only its data had been considered. This leaves unaffected the obligations under this Directive of partner and linked enterprises which fall within scope of that Directive.***

(8b) ***In order to ensure a clear overview of the entities falling within the scope of this Directive, Member States should be able to establish national mechanisms for self-registration that require relevant entities that are subject to this Directive to submit at least the following information to the competent authority under this Directive: 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 sub-sector(s) referred to in Annex I and II, or the type of service they provide and, where applicable, a list of Member States where the entity provides their services. To that end, the Commission, with the assistance of ENISA, should without undue delay issue guidelines and templates regarding the notification obligations. Member States can decide on the appropriate mechanisms where registers exist at national level, that allow for the identification of entities falling within the scope of this Directive. Member States should also establish that certain micro or small entities fulfilling specific criteria that indicate a key role for the economies or societies or for particular sectors or types of services, should also be covered by this Directive, either as essential or important entities. Member States should be responsible for submitting to the Commission at least the number of all essential and important entities for each sector and subsector, as well as relevant information on the number of identified entities and the specific criteria based on which they were identified. Member States are encouraged to exchange with the Commission information on essential and important entities and in the case of a large scale cybersecurity incident, relevant information such as the name of the entity targeted.***

(9a) Member States should be able to establish that entities identified before the entry into force of this Directive as operators of essential services in accordance with Directive (EU) 2016/1148 are to be considered essential entities.

(9b) Some entities perform activities in the field of national security, defence or law enforcement while also providing trust services. Trust services which are included in the scope of the Regulation (EU) No 910/2014 ("eIDAS Regulation") should be included in the scope of this Directive in order to secure the same level of security requirements and supervision as that previously laid out by the eIDAS Regulation. In line with the exclusion of certain specific services from the eIDAS Regulation, this Directive should not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.

(10) The Commission, in cooperation with the Cooperation Group ***and in consultation with relevant stakeholders, should*** issue guidelines on the implementation of the criteria applicable to ***microenterprises*** 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, make information available to microenterprises and small enterprises in that regard.***

(10a) The Commission could provide guidance to support Member States in implementing the provisions on the scope, and evaluating the proportionality of the measures to be taken pursuant to this Directive, in particular 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.

(11) ▌Entities falling within the scope of this Directive should be classified into two categories**,** essential and important ***reflecting*** the level of criticality of the sector or of the type of ***services they provide***, as well as ***their size***. ***In this regard, due account should also be taken of any relevant sectoral risk assessments or guidance by competent authorities, where applicable.*** The supervisory and penalty regimes between these two categories of entities should be differentiated to ensure a fair balance between ***risk based*** requirements and obligations on one hand, and the administrative burden stemming from the supervision of compliance on the other hand.

(12) ***This Directive sets out the baseline for cybersecurity risk management measures and reporting obligations across all sectors that fall within its scope. In order to avoid fragmentation of cybersecurity provisions of*** Union legal ***acts, when additional sector-specific legislation pertaining to*** cybersecurity risk management measures ***and reporting*** obligations ***are considered necessary to ensure a high level of cybersecurity, the Commission should assess whether such provisions could be stipulated in an implementing act under the empowerment provided for*** in this Directive**. *Should such acts not be suitable for that purpose,*** sector-specific ***legislation could contribute to ensuring a high level of cybersecurity, while taking full account of the specificities and complexities of the sectors concerned. To this end,*** 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.

(12a) Where a sector–specific Union legal act contains provisions requiring essential or important entities to adopt measures of at least equivalent effect to the obligations laid down in this Directive related to cybersecurity risk management and obligations to notify significant incidents, those sector-specific provisions, including on supervision and enforcement, should apply. If the sector-specific provisions of a Union legal act do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive should continue to apply to the entities not covered by those sector-specific provisions.

(12b) Future sector-specific Union legal acts should take due account of the definitions outlined in this Directive and the supervisory and enforcement framework laid down in Chapter VI of this Directive.

(12c) Where sector-specific provisions of Union legal acts require essential or important entities to adopt measures of at least equivalent effect to the reporting obligations laid down in this Directive, coherence and effectiveness of handling of incident notifications should be ensured. For that purpose, the sector specific provision on reporting should provide the competent authorities under this Directive with an immediate access to the notifications submitted in accordance with the sector-specific legislation. In particular, such immediate access can be ensured if notifications are being forwarded without undue delay to the CSIRT, the competent authority or the single point of contact under this Directive. For that purpose, where appropriate, Member States should put in place automatic and direct reporting mechanism that ensures systematic and immediate sharing of information with the relevant authorities and CSIRTs concerning the handling of such notifications. For the purposes of simplifying reporting and of implementing the common, automatic and direct reporting mechanism, Member States may, in accordance with sector-specific legislation, use a single point of entry.

(12d) Where sector-specific provisions of Union legal acts require or incentivise entities to notify significant cyber threats, Member States should also encourage the sharing of cyber threats to the CSIRTs, or where relevant competent authorities under this Directive, in order to provide such authorities with enhanced level of awareness about the threat landscape and enable them to respond effectively and in a timely manner should the cyber threats materialise.

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

(13a) In order to avoid gaps between or duplications of cybersecurity obligations imposed on entities in the aviation sector referred to in point 2 (a) of Annex I, national authorities designated under Regulations (EC) No 300/2008[16] and (EU) 2018/1139[17] of the European Parliament and of the Council and competent authorities under this Directive should cooperate in relation to the implementation of cybersecurity risk management measures and the supervision of those measures at national level. The compliance of an entity with the cybersecurity risk management measures under this Directive could be considered by the national authorities designated under Regulations (EC) No 300/2008 and (EU) 2018/1139 as compliant with the requirements laid down in those, and the relevant delegated and implementing acts adopted pursuant to those Regulations.

---

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

17 ***Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).***

(14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council ▌ and this Directive. To achieve this, Member States should ensure that critical entities, ***[***and equivalent entities***]***[*], pursuant to Directive (EU) XXX/XXX are considered ***as*** essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent ***authorities within 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. ***Competent*** authorities under both Directives should cooperate and exchange information ***without undue delay***, particularly in relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents ***as well as on non-cyber risks, threats and incidents*** affecting critical entities ***[or entities equivalent to critical entities][*], including*** the cybersecurity ***and physical*** measures taken by critical entities ***and the results of supervisory activities carried out with regard to such entities***. ***Furthermore, in order to streamline supervisory activities between the competent authorities designated under both Directives and in order to minimise the administrative burden for the entities concerned, competent authorities should endeavour to harmonise incident notification templates and supervisory processes. Where appropriate,*** competent authorities under Directive (EU) XXX/XXX, ***can request*** competent authorities under this Directive ▌ to exercise their supervisory and enforcement powers ***in relation to*** an essential entity identified as critical. Both authorities should cooperate and exchange information ***where possible in real time,*** for this purpose.

[*] ***The wording to be adapted to the text of Directive (EU) .../... on the resilience of critical entities, PE-CONS …/... (2020/0365(COD)).***

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

(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to ▌ 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.***

(16) Cloud computing services should cover services that allow on-demand and broad remote access to a scalable and elastic pool of shareable and distributed computing resources. Those computing resources include resources such as networks, servers or other infrastructure, operating systems, software, storage, applications and services. ***The service models of cloud computing include, amongst others, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) and Network as a Service (NaaS).*** The deployment models of cloud computing should include private, community, public and hybrid cloud. The aforementioned service and deployment models have the same meaning as the terms of service and deployment models defined under ISO/IEC 17788:2014 standard. The capability of the cloud computing user to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the cloud computing service provider could be described as on-demand administration. The term 'broad remote access' is used to describe that the cloud capabilities are provided over the network and accessed through mechanisms promoting use of heterogeneous thin or thick client platforms (including mobile phones, tablets, laptops, workstations). The term 'scalable' refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term 'elastic pool' is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment. The term 'distributed' is used to describe those computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing.

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

(18) Services offered by data centre service providers may not always be provided in a form of cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to the security of network and information systems, this Directive should cover also providers of such data centre services that are not cloud computing services. For the purpose of this Directive, the term 'data centre service' should cover provision of a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term 'data centre service' does not apply to in-house, corporate data centres owned and operated for own purposes of the concerned entity.

(19) Postal service providers within the meaning of Directive 97/67/EC of the European Parliament and of the Council[18], ***including*** courier ▌ 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 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.

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

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

(20a) For the purpose of achieving and maintaining a high level of cybersecurity, the national cybersecurity strategies required by this Directive should consist of coherent governance frameworks in the area of cybersecurity. These strategies can be composed of one or several documents of legislative or non-legislative nature.

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

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

(23) ***The single point of contact should ensure effective cross-border cooperation with relevant authorities of other Member States and ENISA.*** The single points of contact should ***therefore*** be tasked with forwarding ***of*** notifications ***of incidents with cross-border impact*** to the single points of contact***, CSIRTs or competent authorities*** of other affected Member States ***upon request***. At the level of Member States' authorities, [redacted] the single points of contact should ***enable smooth cross-sectorial cooperation with other competent national authorities. They could*** also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which ***the single points of contact*** should be able to forward, as appropriate, to the ***CSIRTs or the competent*** national competent authorities [redacted] under this Directive.

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

(24) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ***designate one or more*** CSIRTs ***under this Directive and ensure adequate resources and technical capabilities. They should comply*** 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 ***may*** 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] ▌, on behalf of and upon request by an entity under this Directive, a proactive scanning of the network and information systems used for the provision of their services. ***Where applicable,*** Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.

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

(25a) CSIRTs should have the ability to, upon an entity's request, monitor the internet-facing assets, both on premises and off premises, to discover, understand and manage their overall organisational risk to newly discovered supply chain compromises or critical vulnerabilities. The entity should be encouraged to communicate to the CSIRT whether it runs a privileged management interface, as this could affect the speed of undertaking mitigating actions.

(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive. ***Therefore, for the purpose of carrying out their tasks, CSIRTs and competent authorities should be able to exchange information, including personal data, with CSIRTs of third countries or their authorities provided the conditions under Union data protection law for transfers of personal data to third countries are met, for example those of Article 49 of Regulation (EU) 2016/679.***

(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 analyse Member States' cyber hygiene policies.

(26b) Cybersecurity awareness and cyber hygiene are essential to enhance the level of cybersecurity within the EU, in particular in light of the growing number of connected devices that are increasingly used in attacks. Efforts should be deployed to enhance the overall awareness of cyber risks related to such devices, while assessments at an EU level could help ensure a common understanding of these risks within the Internal market.

(26c) Member States should encourage the use of any innovative technology, including artificial intelligence (AI), the use of which could improve the detection and prevention of attacks against network and information systems, enabling resources to be diverted towards cyber attacks more effectively. Member States should therefore encourage in their national strategies activities in research and development to facilitate the use of such technologies, in particular relating to (semi-)automated tools in cybersecurity and where relevant the sharing of data needed to train and improve them. The use of any innovative technology, including artificial intelligence (AI) should be used in full respect of EU data protection law, including on the data protection principles of data accuracy, data minimisation, fairness and transparency, data security, such as state -of –the-art encryption. The requirements of data protection by design and by default laid down in Regulation (EU) 2016/679 should be fully exploited.

(26d) Open-source cybersecurity tools and applications can contribute to a higher degree of openness 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 diversification of suppliers. Open source can lead to a more transparent verification process of cybersecurity related tools and a community-driven process of discovering vulnerabilities. Member States should therefore be able to 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 small and medium-sized enterprises (SMEs) facing significant costs for implementation, which could be minimised by reducing the need for specific applications or tools.

(26e) Cities are increasingly connecting their utilities to their digital networks, to improve urban transport networks, upgrade their water supply and waste disposal facilities and make the heating of lights and buildings in the city more efficient. These digitalized utilities are vulnerable for cyber-attacks and run the risk to, in case of a successful attack, harm citizens at a large scale due to their interconnectness. Member States should develop a policy that addresses the development of these connected (or Smart) cities, and their potential effects on society, as part of their national strategy.

(26f) In recent years, Europe has faced an exponential increase in ransomware attacks, in which malware encrypt company data and systems and demand a ransom payment for release. The increasing frequency and severity of ransomware incidents can be driven by several factors, such different attack patterns, criminal business model around 'ransomware as a service' and cryptocurrencies, ransom demands, and the rise of supply chain attacks. Member States should develop a policy addressing the rise of ransomware attacks as part of their national strategy.

(26g) 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 among all stakeholders. Member States should promote policies underpinning the establishment of cybersecurity-specific PPPs. 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.

(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 ▌ whose disruption exceeds a Member State's capacity to respond to it ***or with a significant impact on at least two Member States***. 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.

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

(27a) Member States should, in their national cybersecurity strategies, address the specific cybersecurity needs of SMEs. SMEs represent, in the Union context, a large percentage of the industrial and business market and they often struggle 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. SMEs are increasingly becoming the target of supply chain attacks due to their less rigorous cybersecurity measures and attack management, and availability of dedicated security resources. Such supply chain attacks do not only impact SMEs and their operations in isolation but can also have a cascading effect for larger attacks on entities that they supply to. Member States should, through their national cybersecurity strategies, help SME's to address the challenges faced in their supply chains. Member States should have a point of contact for SMEs at national or regional level, 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 also encouraged to offer services such as website configuration and logging enabling to small enterprises and microenterprises that lack those capabilities.

(27b) ***As part of their national cybersecurity strategies, Member States should adopt policies on the promotion of active cyber protection as part of a wider defensive strategy. Rather than responding reactively, active cyber protection is the prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner, combined with the use of capabilities deployed within and outside the victim network. This could include Member States offering free services or tools to eligible entities, including self-service checks, detection tools and takedown services. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enable a unity of effort in successfully detecting, preventing, addressing and blocking attacks against network and information systems. Active cyber protection is based on a defensive strategy that excludes offensive measures.***

(28) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying those vulnerabilities is an important factor in reducing cybersecurity risk. Entities that develop ***or administer*** such systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and reported (disclosed) by third parties (reporting entities), the manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from third parties. In this regard, international standards ISO/IEC 30111 and ISO/IEC ***29147*** 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. ***As part of their national policy***, Member States should ***aim to address, to the extent possible, the challenges faced by vulnerability researchers, including their potential exposure to criminal liability, in accordance with their national legal order. Given that*** entities and ***natural persons researching*** vulnerabilities ***could in some*** Member ***States be exposed to criminal and civil liability,*** Member States ***are encouraged to issue guidelines as regards the non-prosecution of information security research and an exemption from 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 coordinated vulnerability disclosure). Where the reported vulnerability could potentially have significant impact on entities in more than one Member State, the designated CSIRTs should cooperate within the CSIRTs network, where appropriate.

(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an enhanced cybersecurity risk management. ▌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 ***within*** the scope of application of this Directive***, as well as competent authorities, CSIRTs,*** 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) Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A European vulnerability ***database*** maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with similar registries ***or databases*** in third country jurisdictions***, to avoid duplications of efforts and to seek complementarity***. ***In particular, ENISA should explore the possibility of a close cooperation with the operators of the Common Vulnerabilities and Exposures (CVE) system.***

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

(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations***, in particular as regards facilitating the alignment in the transposition of this Directive among Member States,*** to be addressed through better implementation of existing rules. ***The Cooperation Group could also map the national solutions in order to promote compatibility of cybersecurity solutions applied to each specific sector across the Union. 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 ***could organise*** regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the ***Cooperation*** Group and gather ***data and*** input on emerging policy challenges. ***Additionally, the Cooperation Group should carry out a regular assessment of the state of play of current cyber threats or incidents, such as ransomware.*** In order to enhance cooperation at Union level, the ***Cooperation*** Group should consider inviting ***relevant*** Union ***institutions,*** bodies and agencies involved in cybersecurity policy, such as the European ***Parliament, Europol***, ***the European Data Protection Board,*** the European Union Aviation Safety Agency (EASA) and the European Union Agency for Space Programme (EUSPA) to participate in its work.

(35) The competent authorities and CSIRTs should be empowered to participate in exchange schemes for officials from other Member States***, within a framework 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***.

(35a) The CSIRTs network should continue to contribute to strengthening confidence and trust and to promote swift and effective operational cooperation among Member States. In order to enhance operational cooperation at Union level, the CSIRTs network should consider inviting Union bodies and agencies involved in cybersecurity policy, such as Europol to participate in its work.

(35b) CSIRTs are tasked with incident handling. This includes the processing of large volumes of, sometimes sensitive, data. Member States should ensure that CSIRTs have an infrastructure for information-sharing and processing, as well as well-equipped staff, which ensures the confidentiality and trustworthiness of their operations. CSIRTs could also set up codes of conduct in this respect.

(36) The Union ***can***, 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***, EU-CyCLONe*** and the CSIRTs network. Such agreements should ensure ***Union's interests and*** adequate protection of data. ***This should not preclude the right of Member States to cooperate with third countries on management of vulnerabilities and cyber security risk management, facilitating reporting and general information sharing in accordance with Union law.***

(36a) In order to facilitate the effective implementation of provisions of this Directive such as the management of vulnerabilities, cybersecurity risk management, reporting measures and information sharing arrangements, Member States may cooperate with third countries and undertake activities that are deemed appropriate for that purpose, including information exchanges on threats, incidents, vulnerabilities, tools and methods, tactics, techniques and procedures, cyber crisis management preparedness and exercises, training, trust building and structured information sharing arrangements.

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

(37a) EU-CyCLONe should work as an intermediary between the technical and political level during large-scale cybersecurity incidents and crises and should enhance cooperation at operational level and support decision–making at political level. In cooperation with the Commission in regards to its competences in the area of crisis management, the network should build on the CSIRTs network findings and use its own capabilities to create impact analysis of the large-scale incidents and crises.

(37b) Cyberattacks are cross border in nature, and a significant cyber incident can disrupt and damage critical information infrastructures on which the smooth functioning of the internal market depends. Commission Recommendation 2017/1584 on coordinated response to large-scale cybersecurity incidents and crises addresses the role of all relevant actors. Furthermore, the Commission is responsible, within the framework of the Union Civil Protection Mechanism [DECISION No 1313/2013/EU, Article 8] for general preparedness actions including managing Emergency Response Coordination Centre and Common Emergency Communication and Information System, maintaining and further developing situational awareness and analysis capability, and establishing and managing the capability to mobilise and dispatch expert teams in the event of a request for assistance from a Member State or third country. The Commission is also responsible for providing analytical reports for the Integrated Political Crisis Response mechanism under Council Implementing Decision (EU) 2018/1993 on the EU Integrated Political Crisis Response Arrangements, including in relation to cybersecurity situational awareness and preparedness, as well as for situational awareness and crisis response in the areas of agriculture, adverse weather conditions, conflict mapping and forecasts, early warning systems for natural disasters, health emergencies, infection disease surveillance, plant health, chemical incidents, food and feed safety, animal health, migration, customs, nuclear and radiological and energy.

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

(40) Risk-management measures should ***take into account the degree of dependence of the entity on network and information systems and*** include measures to identify any risks of incidents, to prevent, detect***, 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 measures should provide for systemic analysis, and taking into account the human factor, in order to have a complete picture of the security of the information system.***

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

(40b) For the purposes of demonstrating compliance with cybersecurity risk management measures and in the absence of appropriate European cybersecurity certification schemes adopted in accordance with Regulation (EU) 2019/881, Member States should promote, in consultation with the Cooperation Group and the European Cybersecurity Certification Group, the use of appropriate European or international standards by the essential and important entities or may require entities to use certified ICT products, services and processes.

(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 ***to*** the network and information system concerned, taking into account the state of the art of such measures ***and the cost for their implementation***. ***Due account should also be taken of the size of the entity, as well as the likelihood of occurrence of incidents and their severity.***

(41a) Cybersecurity risk management measures should be proportionate to the degree of the entity's exposure to risks and to the societal and economic impact that an incident on the entity would have on the Member States. When defining sets of cybersecurity risk management measures adapted to essential and important entities, due account should be taken of the divergent risk exposure of essential and important entities, such as the criticality of the entity, risks including societal risks, the likelihood of occurrence of incidents, their severity, and the societal and economic impact an incident would have on the Member State.

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

(42a) Taking account of their cross-border nature, the DNS service providers, TLD name registries and entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, and managed security service providers should be subject to a higher degree of harmonisation at Union level. The implementation of cyber security measures should therefore be facilitated by an implementing act.

(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 and software editors,*** 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 direct 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.

(44a) National competent authorities, in the context of their supervisory tasks, may also benefit from cybersecurity services such as security audits and penetration testing or incident response.

(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) Research activities play a key role in the development of new products and processes. Many of these activities are carried out by entities that share, disseminate or exploit the results of their research, for commercial purposes. These entities can therefore be important players in value chains, which makes the security of their network and information systems an integral part of the overall cybersecurity of the internal market. Research organisations should be understood to encompass those entities focus the essential part of their activities on the conduct of applied research or experimental development, within the meaning of 2015 Guidelines for Collecting and Reporting Data on Research and Experimental Development (Frascati Manual) of the Organisation for Economic Cooperation and Development (OECD), in view of the results being used for commercial exploitation, such as the manufacturing and marketing of a product, process or the provision of a service.

(45b) Entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, and organise training for their staff, and raise awareness concerning 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, such as artificial intelligence or machine learning systems to enhance their capabilities and the protection of networks.

(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, ***and where appropriate in consultation with relevant stakeholders including from the industry,*** 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 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, in particular in the case of alternative models of governance, include concealed vulnerabilities or backdoors and potential systemic supply disruptions, in particular in case of technological lock-in or provider dependency.***

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

(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.***

(48) In order to streamline the legal obligations imposed on providers of public electronic communications networks or publicly available electronic communications services, and trust service providers related to the security of their network and information systems, as well as to enable those entities and their respective competent authorities to benefit from the legal framework established by this Directive (including designation of CSIRT responsible for risk and incident handling, participation of competent authorities and bodies in the work of the Cooperation Group and the CSIRT network), they should be included in the scope of application of this Directive. The corresponding provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council[22] and Directive (EU) 2018/1972 of the European Parliament and of the Council[23] related to the imposition of security and notification requirement on these types of entities should therefore be repealed. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council[24].

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

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

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

(48a) The security obligations laid down in this Directive should be considered complementary to the requirements imposed on trust service providers under Regulation (EU) No 910/2014 (eIDAS Regulation). Trust-service providers should be requested to take all appropriate and proportionate measures to manage the risks posed to their services, including in relation to customers and relying third parties, and to report security incidents under this Directive. Such security and reporting obligations should also concern the physical protection of the service provided. Article 24 of Regulation (EU) 910/2014 continues to apply.

(48b) Member States may assign the role of competent authorities for trust services to the eIDAS supervisory bodies in order to ensure the continuation of current practices and to build on the knowledge and experience gained in the application of the eIDAS Regulation. Where that role is assigned to a different body, the national competent authorities under this Directive should cooperate closely, in a timely manner, by exchanging the relevant information in order to ensure effective supervision and compliance of trust service providers with the requirements set out in this Directive and Regulation [XXXX/XXXX]. Where applicable, the CSIRT or national competent authority under this Directive should immediately inform the eIDAS supervisory body about any notified significant cyber threat or incident with impact on trust services as well as about any non-compliance of a trust service provider with the requirements under this Directive. For the purposes of reporting, Member States may use, where applicable, the single-entry point established to achieve a common and automatic incident reporting to both the eIDAS supervisory body and the CSIRT or the competent authority under this Directive. The rules on reporting obligations should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council[25].

---

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

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

(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.***

(51) The internal market is more reliant on the functioning of the internet than ever ▌. The services of ***almost*** 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 providers of*** public electronic ***communication*** networks ▌have appropriate cybersecurity measures in place and report significant incidents in relation thereto. ***Member States should ensure that the security of the public electronic communication networks is maintained and that their vital security interests are protected from sabotage and espionage. Given that international connectivity supports and accelerates the competitive digitalisation of the EU and its economy any incidents affecting undersea communication cables should be reported to the relevant CSIRT or competent authority. The national cybersecurity strategy of Member States should, when relevant, take into account the cybersecurity of undersea communication cables and include a mapping of potential security risks and mitigation measures to secure the highest level of their protection.***

(52) Where ***applicable***, entities should inform their service recipients of particular ▌measures they can take to mitigate the resulting risk ***from a significant cyber threat*** to themselves. ***The entities should, where appropriate and in particular in cases where the significant cyber threat can materialise, notify also their service recipients of the threat itself.*** The requirement to inform those recipients of such threats should ***be done on a best effort basis and*** 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 ***cyber*** threats to the recipients should be free of charge ***and drafted in an easily comprehensible language***.

(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 software or encryption technologies.

(54) In order to safeguard the security of electronic communications networks and services, the use of encryption ***technologies***, ▌ in particular end-to-end encryption ***as well as data-centric security concepts, such as cartography, segmentation, tagging, access policy and access management, and automated access decisions***, should be promoted***.*** Where necessary, ***the use of encryption and in particular end-to-end encryption*** should be mandatory for ***the*** providers of ***electronic communications networks and*** services ▌ 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 weaken*** end-to-end ▌ encryption***, which is a critical technology for effective data protection and*** privacy and security of communications ▌ .

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

(54b) In order to safeguard the functionality and integrity of the internet and to promote security and resilience of DNS, relevant stakeholders including Union private sector entities, providers of electronic communication services, in particular internet access service providers and providers of online search engines 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.

(55) This Directive lays down a ***multiple-stages*** 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. ***In this regard, the Directive should also include reporting of incidents that, based on an initial assessment performed by the entity, may be assumed to lead to severe operational disruption or financial losses or affect other natural or legal persons by causing considerable material or non-material losses. Such initial assessment should take into account, amongst other, the affected network and information systems and in particular their importance in the provision of the entity's services, the severity and technical characteristics of a cyber threat and any underlying vulnerabilities that are being exploited as well as the entity's experience with similar incidents. Indicators such as the extent to which the functioning of the service is affected, the duration of an incident or the number of affected recipients of services could play an important role in defining whether the operational disruption of the service is of severe nature.***

(55a) Where entities become aware of a significant incident, they should be required to submit an early warning without undue delay and in any case within 24 hours. This early warning should be followed by an incident notification to be submitted without undue delay and in any case within 72 hours after having become aware of the incident, aimed in particular at updating information submitted through the early warning and share an initial assessment of the incident, its severity and impact, including where available indicators of compromise. A final report should be submitted no later than one month after the incident notification. The early warning should only include the information strictly necessary to make the competent authority aware of the incident and allow the entity to seek assistance, if required. Such early warning, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action, and whether it may have any cross-border impact. Member States should ensure that the requirement to submit this early warning, or the subsequent incident notification, does not divert the reporting entity's resources from activities related to incident handling that should be prioritised to prevent that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect. In cases of ongoing incidents at the time of the submission of the final report, Member States should ensure that entities provide a progress report at that time, and a final report within one month after the incident has been handled.

(55b) ***A proactive approach to cyber threats is a vital component of cybersecurity risk management that should enable competent authorities to effectively prevent cyber threats from materialising into actual incidents that may cause considerable material or non-material losses. For that purpose, the notification of significant cyber threats is of key importance. To that end, entities are encouraged to report on a voluntary basis cyber threats.***

(56) ***In order to simplify the reporting information required under this Directive as well as to decrease the administrative burden for entities, Member States should provide technical means such as a single entry point, automated systems, online forms, user-friendly interfaces, templates, dedicated platforms for the use of entities, whether inside or outside the scope of this Directive, for the submission of the relevant reporting information. EU funding supporting the implementation of this Directive, in particular within the DIGITAL Europe programme[26], could in particular include support for single entry points. Furthermore,*** essential and important entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional burdens and may also lead to uncertainties with regard to the format and procedures of such notifications. ***When a single entry point is established, Member States are encouraged to use this single entry point also for notifications*** of security incidents ***required under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC. The use of such*** single entry point for ***reporting of security incidents*** under ***Regulation (EU) 2016/679 and Directive 2002/58/EC should not affect the application of the provisions of*** Regulation (EU) 2016/679 and Directive 2002/58/EC***, in particular those relating to independent supervisory authorities***. ENISA, in cooperation with the Cooperation Group***,*** should develop common notification templates by means of guidelines ***to*** simplify and streamline the reporting information ***required under*** Union law and decrease the ***burden on reporting entities***.

---

[26] ***Regulation (EU) 2021/6994.***

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

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

(59) Maintaining accurate and complete databases of domain names ▌ registration data (so called 'WHOIS data') and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. ***For this specific purpose, TLD registries and the entities providing domain name registration services should be required to process certain data necessary to achieve that purpose.*** Such processing ***should constitute a legal obligation within in the meaning of Article 6(1)(c) of Regulation 2016/679. This obligation is without prejudice to the possibility to collect domain name registration data for other purposes, for example based on contractual arrangements or legal requirements established in other*** Union ***or national laws. This obligation aims at achieving a complete and accurate set of registration data per each TLD and it should not result in collecting and storing the same data multiple times. The TLD name registries and the entities providing domain name registration services should cooperate in order to avoid the duplication of the tasks laid down in Article 23.***

(60) The availability and timely accessibility of ***the domain name registration*** data to ***legitimate access seekers, is essential to prevent and combat Domain Name System abuse, to prevent, detect and respond to cybersecurity incidents. Legitimate access seekers mean any legal or natural person making a request based on Union or national law. They include but are not limited to*** competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, ***and national*** CERTs, ***or*** CSIRTs ▌. ***TLD registries and the entities providing domain name registration services should be required to enable lawful access to specific domain name registration data, which are strictly necessary for the purpose of the access request, to legitimate access seekers in accordance with Union and national law. The request from legitimate*** access ***seekers*** should ***be accompanied with a statement of reasons permitting the assessment of the necessity of access*** to ***the*** data.

(61) In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the entities providing domain name registration services ▌ should collect and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules. ***These policies and procedures should take into account to the extent possible the standards developed by the multi-stakeholder governance structures at international level. The TLD registries and the entities providing domain name registration services should adopt and implement proportionate processes to verify such registration data. These processes should reflect the current best practices used within the industry and, to the extent possible, the progress being made in the field of electronic identification. Examples of verification processes may include both ex ante controls, performed at the time of the registration, and ex post controls, performed after the registration. The TLD registries and the entities providing domain name registration services should in particular verify at least one means of contact of the registrant.***

(62) TLD registries and the entities providing domain name registration services ▌ should ***be required to*** make ***publicly*** available domain name registration data that fall outside the scope of Union data protection rules, such as data that concern legal persons[27]. ***For legal persons, the TLD name registries and the entities providing domain name registration services should make publicly available at least the name of the registrant, and the contact telephone number. The contact email address should also be published provided that it does not contain any personal data. This can be achieved through various technical means, including the use of email aliases, functional accounts or similar systems.*** TLD registries and the entities providing domain name registration services ▌ should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should ensure that TLD registries and the entities providing domain name registration services ▌ should respond without undue delay to requests ▌ for the disclosure of domain name registration data ***from legitimate access seekers.*** TLD registries and the 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. ***These policies and procedures should take into account, to the extent possible any guidance and the standards developed by the multi-stakeholder governance structures at international level.*** The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. ***Member States should ensure that all types of access to domain name registration data (both personal and non-personal data) are free of charge.*** With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board ***and take into account to the extent possible the standards developed by the multi-stakeholder governance structures at international level***.

---

27 Regulation (EU) 2016/679 of the European Parliament and of the Council recital (14) whereby "this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person".

(63) ▌Essential and important entities under this Directive should fall under the jurisdiction of the Member State where they ***are established. Providers of public electronic communications networks or providers of publicly available electronic communications services should be deemed to be under the jurisdiction of the Member State in which they*** provide their services. If the entity provides services ***or is established*** 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. ***Where Member States exercise jurisdiction, they should avoid that the same conduct is sanctioned more than once for the infringement of the obligations laid down in this Directive, in line with the principle of ne bis in idem. DNS service providers, TLD name registries, and entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, and managed security service providers, as well as digital providers should be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union. Public administration entities should fall under the jurisdiction of the Member State which established them.***

(63a) For the purpose of ensuring compliance of the entities with their obligations under this Directive, Member States should cooperate and assist each other in the performance of supervisory and enforcement measures, notably when services are provided in more than one Member State or when the network and information systems are located in a different Member State than the ones where services are provided. When providing assistance, the competent authority the assistance of which was requested should carry out supervisory or enforcement measures in accordance with its national law. In order to ensure the smooth functioning of the mutual assistance mechanism established under this Directive, competent authorities should use the Cooperation Group as a forum to discuss cases and particular requests for assistance.

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

(64a) When a publicly available recursive DNS service is provided by a provider of public electronic communications networks or publicly available electronic communications services only as a part of the internet access service, the entity should be deemed to be under the jurisdiction of all the Member States where its services are provided.

(64b) In order to ensure a clear overview of DNS service providers, TLD name registries, entities providing domain name registration services, content delivery network providers, cloud computing service providers, data centre service providers, managed service providers and managed security service providers and digital providers providing services across the Union under the scope of this Directive, ENISA should create and maintain a registry of such entities, based on information received by Member States, where applicable through their national mechanisms for self-registration. The single point of contact of the Member States should forward to ENISA information. Any changes to the information should also be forwarded to ENISA. With a view to ensure accuracy and completeness of the information that should be included in this registry, Member States should submit to ENISA the information available in their national registries on these entities. ENISA and the Member States should take measures to facilitate the interoperability of such registries, while ensuring protection of confidential or classified information. 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.

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

(66) Where information considered classified ***in accordance with*** 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.***

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

(68) Entities should be encouraged ***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.

(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, ***could be considered legitimate to comply with legal obligation subject to the requirements of Article 6(1)(c) and (3) of Regulation (EU) 2016/679,*** of the data controller concerned ▌ as referred to in Regulation (EU) 2016/679. ***Processing of personal data might also be necessary for legitimate interests pursued by essential and important entities, as well as providers of security technologies and services acting on behalf of these entities, pursuant to Article 6(1)(f) of Regulation (EU) 2016/679, including where such processing is necessary for cybersecurity information sharing arrangements or the voluntary notification of relevant information as laid down in this Directive.*** 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 ▌ may require the processing of ***certain categories*** of personal data***, such as*** IP addresses, uniform resources locators (URLs), domain names, ***email addresses, time stamps – where those reveal personal data. Processing of personal data by competent authorities, SPOCs and CSIRTs, could be considered necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or could constitute a legal obligation, pursuant to Article 6(1) point (c) or (e) and Article 6(3) of Regulation (EU) 2016/679 or for pursuing a legitimate interest of the essential and important entities, as referred to in Article 6(1)(f) of Regulation (EU) 2016. Furthermore, Member States' laws may lay down rules allowing competent authorities, SPOCs and CSIRTs, to the extent that is strictly necessary and proportionate for the purpose of ensuring the security of network and information systems of essential and important entities, to process special categories of personal data in accordance with Article 9 of Regulation (EU) 2016/679, in particular by providing for suitable and specific measures to safeguard the fundamental rights and interests of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued***.

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

(70a) The execution of supervisory tasks by the competent authorities should not unnecessarily hamper the business activities of the subject entity. Where competent authorities execute their supervisory tasks in relation to essential entities, including the conduction of on- and off-site supervision, the investigation of cases of non-compliance, the conduction of security audits or security scans, they should minimise the impact on the business processes of the entity.

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

(70c) When exercising their supervisory tasks in relation to essential and important entities, competent authorities should ensure that these tasks are conducted by trained professionals. Trained professionals should have the necessary skills to carry out the tasks conferred on competent authorities by this Directive, in particular in regards to conducting on-site and off-site inspections including the identification of weaknesses in databases, hardware, firewalls, encryption and networks. Inspections should be conducted in an objective manner.

(70d) In duly justified cases where the competent authority is aware of a significant cyber threat or a pending risk, the competent authority should be able to take immediate enforcement decisions with the aim to prevent or respond to an incident.

(71) In order to make enforcement effective, a minimum list of administrative sanctions for breach of the cybersecurity risk management and reporting obligations provided by this Directive should be laid down, setting up a clear and consistent framework for such sanctions across the Union. Due regard should be given to the nature, gravity and duration of the infringement, the ▌damage caused or losses incurred▌, 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 ***(the 'Charter')***, including effective judicial protection***,*** due process***, the presumption of innocence and the rights of defence***.

(71a) The provisions relating to the liability of natural persons holding certain responsibilities within an entity for breach of their duty to ensure compliance with the obligations laid down in this Directive do not require Member States to ensure criminal prosecution or civil liability for damages caused by such breach to third parties.

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

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

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

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

(76) In order to further strengthen the effectiveness and dissuasiveness of the penalties applicable to infringements of obligations laid down pursuant to this Directive, the competent authorities should be empowered to apply ***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***. 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 ▌, including effective judicial protection, due process, presumption of innocence and right of defence.

(76a) In order to ensure effective supervision and enforcement, notably in cases with a cross-border dimension, Member States that have received a request for mutual assistance should, to the extent of the request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has the network and information system on their territory.

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

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

(79) A peer-review ▌ should be introduced ***to help learn from best practices, strengthen mutual trust and achieve a high common level of cybersecurity***. ***Peer-reviews can lead to valuable insights and recommendations strengthening the overall cybersecurity capabilities, creating another functional path for the sharing of best practices across Member States and contributing to enhance the Member States' levels of maturity in*** cybersecurity***. Furthermore, the peer-review should take account of the results of similar mechanisms, such as the peer-review system of the CSIRTs network, add value and avoid duplication. The implementation of the peer-review should be without prejudice to national or Union laws on protection of confidential and classified information.***

(79a) ***The Cooperation Group should establish a self-assessment methodology aiming to cover factors such as the level of implementation of the cybersecurity risk management requirements and reporting obligations, the level of capabilities and the effectiveness of the exercise of the tasks of the national competent authorities, the operational capabilities of the CSIRTs, the level of implementation of mutual assistance, the level of implementation of the information-sharing framework, or specific issues of cross-border or cross-sector nature. Member States should be encouraged to regularly carry out a self-assessment, and to present and discuss the results of their self-assessment within the Cooperation Group.***

(80) In order to ***ensure a high common level of cybersecurity within the Union on the basis of this Directive***, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect ***of supplementing this Directive by specifying*** which categories of essential ***or important*** entities ***are to*** be required to ***use certain certified ICT products, services and processes or*** obtain a certificate ▌ under ***a*** European cybersecurity certification ***scheme***. 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[28]. 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.

[28] OJ L 123, 12.5.2016, p. 1.

(81) In order to ensure uniform conditions for the implementation ▌ of this Directive***,*** ***implementing powers should be conferred on the Commission to lay down*** the procedural arrangements necessary for the functioning of the Cooperation Group ***and*** the technical ***and methodological as well as sectorial requirements concerning the cybersecurity*** risk management measures***, as well as to further specify*** the type of information, the format and the procedure of incident***, cyber threat and near miss*** notifications ***and of significant cyber threat communications, as well as cases in which an incident is to be considered to be significant***. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[29].

(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 those reviews, 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), could be designated as essential entities under this Directive.***

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

(82a) ***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 to a higher level 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 meet any higher level of execution of these tasks 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.***

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

(84) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter ▌, 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,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. This Directive lays down measures ***aiming to achieve*** a high common level of cybersecurity within the Union***, while aiming at improving the functioning of the internal market***.

2. To that end, this Directive:

   (a) lays down obligations on Member States to adopt national cybersecurity strategies, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs);

   (b) lays down cybersecurity risk management and reporting obligations for entities of a type referred to ▌ in ***Annexes*** I and ▌ II;

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

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

Article 2

Scope

1. This Directive applies to public and private ***essential and important*** entities of a type referred to ▌ in Annex I and ▌ Annex II ***that provide their services or carry out their activities within the Union and which meet or exceed the threshold for medium-sized*** enterprises within the meaning of Commission Recommendation 2003/361/EC[30]. ***Article 3(4) of the Annex to that Recommendation shall not apply for the purposes of this Directive.***

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

   (a) the services are provided by ▌:

      (i) ***providers of*** 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;

   ▌

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

[30] 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).

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

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

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

(g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council[31] [Resilience of Critical Entities Directive], ***[***or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive***]***[*].

▌

2a. Regardless of their size, this Directive also applies to:

– ***public administration entities of central governments recognised as such in a Member State in accordance with national law and referred to in point 9 of Annex I;***

– ***public administration entities at regional level referred to in point 9 of Annex I as defined by Member States, in accordance with national law, which following a risk based assessment, provide services the disruption of which could have a significant impact on critical economic or societal activities.***

Member States may establish that this Directive also applies to public administration entities at local level.

---

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

* ***The wording to be adapted to the text of Directive (EU) .../... on the resilience of critical entities, PE-CONS …/... (2020/0365(COD)).***

2b. Member States may decide to apply this Directive to education institutions in particular when carrying out critical research activities.

3. This Directive is without prejudice to the ▌Member ***States' responsibilities to safeguard*** national security ***or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order***.

3a. This Directive does not apply to public administration entities that carry out their activities in the areas of defence, national security, public security, or law enforcement, including the investigation, detection and prosecution of criminal offences.

3b. Member States may decide that specific essential and important entities which carry out activities in the areas of defence, national security, public security or law enforcement, including activities relating to the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 3a are not obliged to comply with the obligations laid down in Article 18 or Article 20 as regards those activities or those services. In such case, the supervision and enforcement measures referred to in Chapter VI shall not apply in relation to those specific activities or services. In cases when these essential and important entities exclusively carry out activities or exclusively provide services of the type referred to in this paragraph, Member States may decide for these entities to be also exempted from the notification obligations laid down in Article 2a and Article 25.

3c. Paragraphs 3a and 3b shall not apply when entities act as trust service providers referred to in Annex I, point 8.

3d. This Directive does not apply to entities which Member State have exempted from the scope of Regulation (EU) XXXX/XXXX of the European Parliament and of the Council [the DORA Regulation] in accordance with Article 2 paragraph 4 of that Regulation.

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

4. This Directive applies without prejudice to Council Directive 2008/114/EC[32] and Directives 2011/93/EU[33] and 2013/40/EU[34] of the European Parliament and of the Council, ***Regulation (EU) 2016/679 and Directive 2002/58/EC***[35].

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

---

32 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).

33 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).

34 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).

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

I

6a. Essential and important entities, CSIRTs, SPOCs and competent authorities shall process personal data to the extent necessary for the purposes of this Directive in compliance with Regulation (EU) 2016/679, in particular such processing shall rely on Article 6 thereof.

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 Annex I, point 8, shall be carried out in accordance with the applicable Union law on protection of personal data and privacy and in particular Directive 2002/58/EC.

Article 2a

Essential and important entities

1. For the purposes of this Directive, essential entities shall be considered all entities of the type listed in Annex I which exceed the ceilings for medium-sized enterprises as well as the following entities:

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

(b) providers of public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I meeting the ceiling for medium-sized enterprises;

(c) public administration entities referred to in Article 2(2a), first subparagraph;

(d) any other entities of the types listed in Annex I and Annex II established by a Member State on the basis of national risk assessments following the criteria laid down in Article 2(2)(c) to (f);

(e) entities identified as a critical entity pursuant to Directive (EU) X/X of the European Parliament and of the Council [Resilience of Critical Entities Directive], referred to in Article 2(2)(g);

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

2. For the purpose of this Directive, all entities of the type listed in Annexes I and II which do not qualify as essential pursuant to paragraph 1 shall be considered important entities. This includes entities designated by Member States on the basis of Article 2(2)(c) to (f).

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

4. For the purpose of establishing the list referred to in paragraph 3, Member States shall require that the 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;

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

(d) where applicable, the list of Member States where they provide services subject to this Directive.

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 that end, the Commission, with the assistance of ENISA, shall without undue delay issue guidelines and templates regarding the obligations set out in this paragraph.

5. For the purpose of establishing and updating the list referred to in paragraph 3, Member States may establish national mechanisms requiring entities to register themselves.

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

(a) the Commission and the Cooperation Group of the number of all essential and important entities listed pursuant to paragraph 3 for each sector and subsector referred to in the Annexes, and

(b) the Commission of relevant information on the number of identified entities, the sector they belong to or type of service they provide as per the Annexes, and the specific provision(s) of Article 2(2) based on which the essential and important entities were identified, pursuant to paragraph 2, points (c) to (f).

7. By ... [6 months after the transposition of deadline] and upon request of the Commission, Member States may notify the Commission of the names of the essential and important entities referred to in paragraph 6, point (b).

Article 2b

Sector-specific Union acts

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

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

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

   (b) ***the sector specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the designated CSIRTs, the competent authorities under this Directive or the single point of contact and if requirements to notify significant incidents are at least equivalent in effect to those laid down in Article 20(1) to (6).***

3. ***The Commission shall within six months after the entry into force of this Directive, issue guidelines clarifying the application of paragraphs 1 and 2. The Commission shall review the guidelines on a regular basis. When preparing those guidelines, the Commission shall take into account the views of the Cooperation Group and ENISA.***

Article 3

Minimum harmonisation

This Directive shall not preclude Member States ***from adopting or maintaining*** provisions ensuring a higher level of cybersecurity***, provided that such provisions are consistent with their obligations under Union law***.

Article 4

Definitions

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

(1) 'network and information system' means:

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

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

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

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

(3) 'cybersecurity' means cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council[36];

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

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

(4a) 'near miss' means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but was successfully prevented from transpiring or did not materialise;

(5) 'incident' means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the ▌services offered by, or accessible via, network and information systems;

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

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

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

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

(7b) '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 ***ICT products or ICT services*** 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, ***entities providing domain name registration services,*** a cloud computing service provider, a data centre service provider, a content delivery network provider***, managed service provider or managed security service provider*** as referred to in point 8 ***and 8a*** 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[37];

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

(12) 'internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

[37] 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).

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

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

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

(15a) 'entities providing domain name registration services' means registrars and agents acting on behalf of registrars, such as privacy or proxy registration service providers or resellers;

(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[38];

(16a) 'trust services' means trust services within the meaning of Article 3(16) of Regulation (EU) No 910/2014, excluding those exclusively used within closed systems as referred to in Article 2(2) of that Regulation;

[38] 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).

(16b) 'trust service provider' means a trust service provider within the meaning of Article 3(19) of Regulation (EU) No 910/2014;

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

(17) 'online marketplace' means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council[39];

(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[40];

(19) 'cloud computing service' means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable ***computing resources, including when those are*** distributed ***over several locations***;

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

(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;

---

39 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).

40 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).

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

(23) ‘public administration entity’ means an entity ***recognised as such*** in a Member State ***in accordance with national law,*** that complies with the following criteria:

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

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

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

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

(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 a 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;

▌

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

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

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

(26d) 'managed service provider' means any entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via support or active administration performed either on customer's premises or remotely;

(26e) 'managed security service provider' means a managed service provider that performs or supports cybersecurity risk-management related activities;

(26f) 'research organisation': means an entity, excluding education institutions, which has as its primary goal to conduct applied research, or experimental development in view of the exploitation of the results of that research for commercial purpose.

CHAPTER II

COORDINATED CYBERSECURITY REGULATORY FRAMEWORKS

Article 5

National cybersecurity strategy

1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives***, the required 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) ▌objectives and priorities of the Member ***State's*** strategy on cybersecurity ***covering in particular the sectors listed in Annexes I and II***;

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

(ba) a governance framework clarifying the roles and responsibilities of relevant actors at national level, underpinning the cooperation and coordination at the national level between the CSIRTs, the single points of contact, and the competent authorities designated under this Directive, as well as the coordination and cooperation between these authorities and competent authorities designated under sector-specific legislation;

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

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

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

(f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council[41] [Resilience of Critical Entities Directive] for the purposes of information sharing on ***cybersecurity risks, cyber threats and*** incidents ***as well as on non-cyber risks,*** threats ***and incidents*** and the exercise of supervisory tasks***, as appropriate;***

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

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

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

(b) ***a policy*** regarding the inclusion and specification of cybersecurity-related requirements for ICT products and ***services*** in public procurement***, including cybersecurity certification as well as encryption requirements and the use of open-source cybersecurity products***;

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

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

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

(da) a policy to promote the development and integration of relevant advanced technologies aiming to implement of state-of-the-art cybersecurity measures;

(e) a policy on promoting and developing cybersecurity ***education and training,*** skills, awareness raising and research and development initiatives***, as well as guidance on good cyber hygiene prevention practices and controls, aimed at citizens, stakeholders and businesses***;

(f) a policy on supporting academic and research institutions to develop***, enhance and promote the deployment of*** 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 ***to strengthen the cyber resilience and cyber hygiene baseline*** of SMEs, in particular those excluded from the scope of this Directive, ***by providing easily accessible*** guidance and support ***for their specific needs;***

(ha) a policy on promoting active cyber protection.

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

4. Member States shall assess their national cybersecurity strategies ***on a regular basis and*** at least every ***five*** years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon ***their*** request, in the development ***or the update*** of a national strategy and of key performance indicators for the assessment of the strategy***, in order to align it with the requirements and obligations set out in this Directive***.

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, where necessary, the interaction between the reporting entity and the manufacturer or provider of ***the potentially vulnerable*** ICT products or ICT services ***upon request of either party***.

Any natural or legal person may report, possibly anonymously, a vulnerability referred to in Article 4(8) to the designated CSIRT. The designated CSIRT shall ensure a diligent follow-up of the report and the confidentiality of the identity of the person who reports the vulnerability. Where the reported vulnerability ***could potentially have significant impact on entities in more than one Member State***, the designated CSIRT of each Member State concerned shall***, where appropriate,*** cooperate with ***other designated CSIRTs within*** the ***CSIRTs*** network.

2. ENISA shall develop and maintain***, in consultation with the Cooperation Group,*** a European vulnerability ***database***. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures***, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the 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***, on a voluntary basis, publicly known*** 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. 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 and, in the absence of available patches, guidance ***issued by national competent authorities or CSIRTs*** addressed to users of vulnerable ***ICT*** products and ***ICT*** services as to how the risks resulting from disclosed vulnerabilities may be mitigated.

Article 7

National cybersecurity crisis management frameworks

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

1a. Where a Member State designates more than one competent authority referred to in paragraph 1, it shall clearly indicate which of those competent authorities is to 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) ***cybersecurity*** crisis management procedures***, including their integration into the general national crisis management framework*** and information exchange channels;

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

   (e) relevant public and private ▌parties and infrastructure involved;

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

4. Member States shall ***inform*** the Commission ***about*** the designation of their competent authorities referred to in paragraph 1***. They shall*** submit ***to the Commission and EU-CyCLONe relevant information relating to the requirements of paragraph 3 of this Article about*** their national cybersecurity incident and crisis response plans ▌within three months from that designation and the adoption of those plans. Member States may exclude specific information ▌where and to the extent that it is ▌necessary for their national security.

Article 8

National competent authorities and single points of contact

1. Each Member State shall designate one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VI of this Directive. Member States may designate to that effect an existing authority or existing authorities.

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

3. Each Member State shall designate one national single point of contact on cybersecurity ('single point of contact'). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact for that Member State.

4. Each single point of contact shall exercise a liaison function to ensure cross–border cooperation of its Member State's authorities with the relevant authorities in other Member States, ***and, where appropriate, 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.

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. CSIRTs may establish cooperation relationships with national CSIRTs of third countries. As part of such cooperation relationships, Member States shall facilitate effective, efficient and secure information exchange with CSIRTs of third countries, using relevant information sharing protocols, including the Traffic Light Protocol. CSIRTs may exchange relevant information with CSIRTs of third countries, including personal data in accordance with Union law on data protection.

6b. CSIRTs may cooperate with CSIRTs or equivalent bodies in third countries, in particular with an aim to 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.

Article 10

Requirements***, capabilities*** and tasks of CSIRTs

1. CSIRTs shall comply with the following requirements:

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

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

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

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

   (d) CSIRTs shall be adequately staffed to ensure availability at all times ***and shall ensure that their staff is trained appropriately***;

(e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services;

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

1a. Member States shall ensure that their CSIRTs jointly have the technical capabilities necessary to perform the tasks referred to in paragraph 2. Member States shall ensure that sufficient resources are allocated to CSIRTs to ensure adequate staffing levels to enable CSIRTs to develop their technical capabilities.

2. CSIRTs shall have the following tasks:

(a) monitoring ***and analysing*** cyber threats, vulnerabilities and incidents at national level ***and, upon request, providing support to entities regarding real-time or near real-time monitoring of their networks and information systems***;

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

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

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

(e) providing, upon ***the*** request of an entity, a proactive scanning of the network and information systems ***of the entity concerned to detect vulnerabilities with a potential significant impact. CSIRTs may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential or important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned. Such scanning shall not have any negative impact on the functioning of*** their services;

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

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

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

When carrying out these tasks, CSIRTs may prioritise particular tasks based on a risk-based approach.

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 the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following:

   (a) incident handling procedures;

   (b) cybersecurity crisis management;

   (c) coordinated vulnerability disclosure.

Article 11

Cooperation at national level

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

2. Member States shall ensure that ▌ their CSIRTs ***or, where relevant, the competent authority,*** receive notifications on ***significant*** incidents ***pursuant to Article 20***, ▌ cyber threats and near misses ▌ pursuant to Article ***27***.

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. ***In order to ensure that*** tasks and obligations ***of competent authorities, CSIRTs and single point of contacts are carried out effectively,*** Member States ***should*** ensure appropriate cooperation between ***them*** and law enforcement authorities, data protection authorities ▌ and the ***competent*** authorities ***designated*** pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive]***, the competent authorities under Commission Implementing Regulation 2019/1583, the national regulatory authorities designated in accordance with Directive (EU) 2018/1972, the supervisory bodies designated in accordance with Regulation (EU) No 910/2014,*** the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council ▌ [the DORA Regulation]***, as well as competent authorities designated by other sector-specific Union legal acts,*** within that Member State.

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

[*] ***The wording to be adapted to the text of Directive (EU) .../... on the resilience of critical entities, PE-CONS …/... (2020/0365(COD)).***

5a. Member States shall simplify the reporting through technical means for all notifications referred to in Articles 20 and 27.

CHAPTER III

COOPERATION ***AT UNION AND INTERNATIONAL LEVEL***

Article 12

Cooperation Group

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

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

3. The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) ***and the competent authorities designated under*** Regulation (EU) XXXX/XXXX [the DORA Regulation] may participate in the activities of the Cooperation Group ***in accordance with Article 42(1) of Regulation (EU) XXXX/XXXX [the DORA Regulation]***.

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

   The Commission shall provide the secretariat.

4. The Cooperation Group shall have the following tasks:

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

(aa) providing guidance in relation to the development and implementation of policies on coordinated vulnerability disclosure as referred to in Article 5(2) (c) and Article 6(1);

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

(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;

(ea) exchanging views on the implementation of sectorial legislation with cybersecurity aspects;

(f) ***where relevant*** 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 in accordance with Article 19(1);

(g) discussing ***cases of mutual assistance, including experiences and*** results from ***cross-border*** joint-supervisory activities ▌ as referred to in Article 34;

(ga) upon request of one or more Member States concerned, discussing particular requests for mutual assistance referred to in Article 34;

(h) providing strategic guidance to the CSIRTs network ***and EU–CyCLONe*** on specific emerging issues;

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

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

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

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

(ka) establish the methodology and organisational aspects for the peer review, as well as for the self assesment in accordance with Article 16 of this Directive with the support of the Commission and ENISA;

(kb) preparing reports for the purpose of the review referred to in Article 35 on the experience gained at a strategic level and from peer reviews;

The reports shall be submitted to the Commission, the European Parliament and the Council.

(kc) discussing and carrying out on a regular basis an assessment of the state of play of current cyber threats or incidents, such as ransomware.

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.

The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first subparagraph of this paragraph in accordance with Article 12(4), point (d). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

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

Article 13

CSIRTs network

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

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

3. The CSIRTs network shall have the following tasks:

   (a) exchanging information on CSIRTs' capabilities;

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

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

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

   (bb) ensuring interoperability with regard to information sharing specifications and protocols;

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

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

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

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

(g) discussing and identifying further forms of operational cooperation, including in relation to:

(i) categories of cyber threats and incidents;

(ii) early warnings;

(iii) mutual assistance;

(iv) principles and modalities for coordination in response to cross–border risks and incidents;

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

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

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

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

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

(l) ***where relevant,*** 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.

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

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' ***cyber*** crisis management authorities designated in accordance with Article 7, ***as well as, in cases where a potential or ongoing large scale cybersecurity incident has or is likely to have significant impacts on services and activities falling within the scope of this Directive,*** the Commission ▌. ***In other cases, the Commission shall participate in the activities of EU-CyCLONe as an observer.*** ENISA shall provide the secretariat of ***EU-CyCLONe*** and support the secure exchange of information ***as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information***.

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

3. EU-CyCLONe shall have the following tasks:

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

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

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

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

(d) discussing national cybersecurity incident and ***crisis*** response plans referred to in Article 7(***3***). ***A national cybersecurity incident and crisis response plan of a Member State shall be discussed only at its request.***

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

5. EU-CyCLONe shall regularly report to the Cooperation Group on ***the management of large-scale cybersecurity*** incidents and ***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 ***provided for in Article 13(6)***.

6a. EU-CyCLONe shall submit to the European Parliament and the Council a report assessing its work by ... [18 months after the date of entering into force of this Directive] and every 18 months thereafter.

Article 14a

International cooperation

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

Article 15

Report on the state of cybersecurity in the Union

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

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

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

(aa) an assessment of the general level of cybersecurity awareness and hygiene among citizens and entities, including SMEs;

(b) ***an aggregated assessment on*** the outcomes of peer reviews referred to in Article 16;

(c) ▌ an aggregated assessment of the maturity level of cybersecurity capabilities ***and resources across the Union, including sector-specific, including the alignment of Member States national cybersecurity strategies***.

2. The report shall include particular policy recommendations***, in view of addressing shortcomings and*** 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, the Cooperation Group and the CSIRTs network, shall develop the methodology, including the relevant variables, such as quantitative and qualitative indicators of the aggregated assessment referred to in paragraph 1, point (c).

Article 16

Peer-reviews

1. The ***Cooperation Group*** shall establish, ***with the support of the Commission*** and ENISA, and ***where relevant the CSIRT network*** at the latest by ***... [24*** months following the entry into force of this Directive***]***, the methodology and ***organisational aspects*** of a peer-review ***with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing*** Member States' cybersecurity ***capabilities and*** policies ***necessary to implement this Directive***. ***Participation in the peer-reviews is voluntary.*** The ***peer-reviews*** shall be conducted by cybersecurity ▌experts ***assigned by at least two*** Member States***,*** different ***from the Member State being*** reviewed and shall cover at least ***one of*** the following:

   (i) the ***level of*** 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 ▌of CSIRTs;

   (iv) the ***level of implementation*** of mutual assistance referred to in Article 34;

   (v) the ***level of implementation*** of the information-sharing framework, referred to in Article 26***;***

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

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

3. ▌Member States ***may identify specific issues mentioned in paragraph 1, point (va) to be reviewed***. ***The scope of the review, including identified issues, shall be communicated to the participating Member States prior to the commencement of the peer review.***

3a. Prior to the commencement of the peer-review, Member State may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated experts. The methodology for the self-assessment shall be defined by the Cooperation Group, with the support of the Commission and ENISA.

4. Peer reviews shall entail ***physical*** or virtual on-site visits and off-site exchanges. In view of the principle of good cooperation, the Member ***State subject to the peer review*** shall provide the designated experts with the ▌information necessary for the assessment***, without prejudice to national or Union laws concerning protection of confidential or classified information or to safeguard essential State functions, such as national security. The Cooperation Group, in cooperation with the Commission and ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated 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 ***subject to a peer-review***, the same aspects ***reviewed in a Member State,*** shall not be subject to further ▌review ***in*** that Member State ***for*** the two years following the conclusion of ***the*** peer review, unless otherwise ***requested*** by the ***Member State or agreed upon after a proposal by*** the Cooperation Group.

6. Member ***States*** shall ensure that any risk of conflict of interests concerning the designated experts are revealed to the other Member States, ***the Cooperation Group,*** the Commission and ENISA***, before the commencement of the peer-review***. ***The Member State subject to the peer-review may object to the designation of particular experts on duly justified grounds communicated to the designating Member State.***

7. Experts participating in peer reviews shall draft reports on the findings and conclusions of the reviews. ***Member States shall be allowed to provide comments on their respective draft*** reports***, which*** shall be ***attached*** to the ***reports. The reports shall include recommendations to enable improvement on the aspects covered by the peer-review.*** The reports shall be ***presented to*** the Cooperation Group and the CSIRTs network ***when relevant. The Member State under review may decide to make its report, or a redacted version of its report, publicly available.***

CHAPTER IV

CYBERSECURITY RISK MANAGEMENT AND REPORTING OBLIGATIONS

Section I

Cybersecurity risk management and reporting

Article 17

Governance

1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities in order to comply with Article 18, ***oversee*** its implementation and ***can*** be ***held liable*** for the non-compliance by the entities with the obligations under this Article.

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

2. Member States shall ensure that ***the*** members of the management body ***of essential and important entities are required to*** follow ***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.

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 to 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, where applicable, relevant European and international standards***, ***as well as the cost of implementation***, those measures shall ensure a level of security of network and information systems appropriate to the risk presented. ***When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, its size, the likelihood of occurrence of incidents and their severity, including their societal and economic impact.***

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

   (a) risk analysis and information system security policies;

   (b) incident handling ▌;

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

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

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

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

(fa) basic computer hygiene practices and cybersecurity training;

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

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

(gb) the use of multi-factor authentication or continuous 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 ▌ take into account the vulnerabilities specific to each ***direct*** supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. ***Member States shall also ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities are required to take into account the results of the coordinated risk assessments carried out in accordance with Article 19(1).***

4. Member States shall ensure that where an entity finds that respectively its services or tasks are not in compliance with the requirements laid down in paragraph 2, it shall, without undue delay, take all necessary***, appropriate and proportionate*** corrective measures to bring the service concerned into compliance.

5. ***The Commission shall, by ... [21 months after the date of entry into force of this Directive], adopt implementing acts laying down the technical and the methodological requirements of the measures referred to in paragraph 2 of this Article with regard to entities referred to in Article 24(1), point (b), and trust service providers.***

The Commission may adopt implementing acts ***laying*** down the technical and the methodological ***requirements, as well as sectoral requirements, as necessary,*** of the ***measures*** referred to in paragraph 2 ***of this Article with regard to entities other than those referred to in Article 24(1), point (b) and trust service providers***.

When preparing ***implementing*** acts ***referred to in the first and the second subparagraphs of this paragraph,*** the Commission shall ▌, to the greatest extent possible, ***follow*** international and European standards, as well as relevant technical specifications. ***The Commission shall exchange advice and cooperate with the Cooperation Group and ENISA on the draft implementing acts in accordance with Article 12(4), point (d)***. ***Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).***

▌

Article 19

EU coordinated risk assessments of critical supply chains

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

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

Article 20

Reporting obligations

1. Member States shall ensure that essential and important entities notify, without undue delay, ***the CSIRT or, where relevant,*** the competent ***authority*** in accordance with paragraphs 3 and 4 of any incident having a significant impact on the provision of their services. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of ***those*** incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, ***inter alia***, any information enabling ***the CSIRT and*** the competent ***authority*** to determine any cross-border impact of the incident. ***The mere act of notification shall not subject the notifying entity to increased liability.***

Where the entities concerned do not notify the CSIRT in accordance with paragraph 4, Member States shall ensure that the competent authority forward the notification to the CSIRT upon receipt.

In the case of a cross-border or cross-sectorial incident, Member States shall ensure that the single point of contact is provided in due time with relevant information notified in accordance with paragraph 4.

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

▌

3. An incident shall be considered significant if:

(a) the incident has caused or ***is capable of causing severe*** operational disruption ***of the service*** or financial losses for the entity concerned;

(b) the incident has affected or ***is capable of affecting*** other natural or legal persons by causing considerable material or non-material losses.

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

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

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

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

(c) a final report not later than one month after the submission of the ***incident notification*** under point (***aa***), 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***;***

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

(ca) in cases of ongoing incidents at the time of the submission of the final report referred to in point (c), Member States shall ensure that entities provide a progress report at that time and a final report within one month after the incident has been handled.

With regard to incidents impacting the provision of the services of a trust service provider, the CSIRT or, where relevant, the competent authority, shall, by derogation from paragraph 4, point (aa), be notified without undue delay and in any event within 24 hours of becoming aware of the incident.

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

6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, ***the CSIRT,*** the competent authority, or the ***Single Point of Contact*** shall inform***, without undue delay,*** the other affected Member States and ENISA of the incident. ***Such information shall include at least the type of information received in accordance with paragraph 4.*** In so doing, the ***CSIRTs***, competent ***authority,*** 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 CSIRT or*** the competent authority ▌, and where appropriate ***the CSIRTs or*** the ***competent*** authorities ▌ of other Member States concerned***,*** may, after consulting the entity concerned, inform the public about the incident or require the entity to do so.

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

9. The single point of contact shall submit to ENISA ***every three months*** a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with paragraphs 1 and 2 ***of this Article*** and in accordance with Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report. ***ENISA shall inform every six months the Cooperation Group and the CSIRTs network about its findings on notifications received.***

10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with ***paragraph 1 and Article 27*** by ▌entities identified as critical entities, ***[***or as entities equivalent to critical entities,***]***[*] pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].

11. The Commission ▌may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraph 1 ***of this Article and Article 27 and of a communication submitted pursuant to paragraph 2 of this Article***.

With regard to entities referred to in Article 24(1), point (b), the Commission ***shall, by ... [21 months after the date of entry into force of this Directive], adopt*** implementing acts ▌further ***specifying*** the cases in which an incident shall be considered ***to be*** significant as referred to in paragraph 3 ***of this Article***. ***The Commission may adopt such implementing acts with regard to entities other than those referred to in Article 24(1), point (b).***

The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first and second subparagraphs of this paragraph in accordance with Article 12(4), point (d).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

[*] ***The wording to be adapted to the text of Directive (EU) .../... on the resilience of critical entities, PE-CONS …/... (2020/0365(COD)).***

Article 21

Use of European cybersecurity certification schemes

1. In order to demonstrate compliance with certain requirements of Article 18, Member States may require***,*** entities to ***use particular*** ICT products, ▌services and ▌processes***, either developed by the essential or important entity or procured from third parties, that are certified*** under ▌European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. ***Furthermore, Member States shall encourage*** essential ***and*** important ***entities to use qualified trust services 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 ***or important*** entities shall be required to ***use certain certified ICT products, services and processes or*** obtain a certificate ▌under ***a*** European cybersecurity certification ***scheme adopted*** pursuant to ***Article 49 of Regulation (EU) 2019/881***. ***Those*** delegated acts shall be adopted ***where insufficient levels of cybersecurity have been identified and shall include an implementation period***.

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

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

Article 22

Standardisation

1. In order to promote the convergent implementation of Article 18(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

2. ENISA, in collaboration with Member States***, 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.

Article 23

Database 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*** that TLD ***name*** registries and the entities providing domain name registration services ▌ collect and maintain accurate and complete domain name registration data in a dedicated database ▌ with due diligence ***in accordance with*** Union data protection law as regards data which are personal data.

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

   a. the domain name,

   b. the date of registration,

   c. the registrants' name,

   d. the registrant's contact email address,

   e. the registrant's contact telephone number,

   f. f. the contact email address and telephone number of the point of contact administering the domain name in case it is different from the registrant's.

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

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

5. Member States shall ***require*** that the TLD ***name*** registries and the entities providing domain name registration services ▌ provide access to specific domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ***require*** that the TLD ***name*** registries and the entities providing domain name registration services ▌ reply without undue delay ***and in any event within 72 hours*** to all requests for access. Member States shall ***require*** that policies and procedures to disclose such data are made publicly available.

5a. Compliance with the obligations laid down in paragraph 1 to 5 shall not result in a duplication of collecting and maintaining domain name registration data. To that effect, Member States shall require that TLD name registries and the entities providing domain name registration services cooperate for the purposes of ensuring compliance with this Article.

Section II

Jurisdiction and Registration

Article 24

Jurisdiction and territoriality

1. ***Entities under this Directive shall be deemed to be under the jurisdiction of the Member State in which they are established, except:***

   (a) providers of public electronic communications networks or providers of electronic communications services referred to in point 8 of Annex I which shall be deemed to be under the jurisdiction of the Member State in which they provide their services;

(b) DNS service providers, TLD name registries, ***and entities providing domain name registration services,*** cloud computing service providers, data centre service providers***,*** content delivery network providers***, managed service providers, and managed security service providers*** referred to in point 8 ***and point 8a*** of Annex I, as well as digital providers referred to in point 6 of Annex II ***which*** shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union***;***

(c) public administration entities referred to in point 9 of Annex I which shall be deemed under the jurisdiction of the Member State which established them.

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

3. If an entity referred to in paragraph 1***, point (b)*** is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such 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***, point (b)***, shall be without prejudice to legal actions, which could be initiated against the entity itself.

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

Article 25

Registry ***of*** essential and important entities

1. ENISA shall create and maintain a registry for essential and important entities referred to in Article 24(1), ***point (b), based on the information received from the Member States' single points of contacts according to paragraph 1a, except point (d), and 2***. ***Upon request, ENISA shall enable access of competent authorities to the registry, while ensuring the necessary guarantees to protect the confidentiality of*** information ***where applicable.***

1a. Member States shall require entities referred to in Article 24(1), point (b), to submit the following information to the competent authorities [3 months after the transposition deadline]:

(a) the name of the entity;

(aa) relevant sector, subsector and type of entity as referred to in Annex I and II;

(b) the address of its main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 24(3);

(c) up-to-date contact details, including email addresses and telephone numbers of the ***entity and where applicable, its representative designated pursuant to Article 24(3)***.

(ca) all the Member States where the entity provides services;

(d) IP ranges.

1b. Where applicable, this information shall be submitted through the national mechanism of self-notification referred to in Article 2a(5). The single point of contact in the Member State concerned shall forward the information to ENISA without undue delay after its receipt.

2. ***Member States shall ensure that*** the entities referred to in paragraph 1 ▌notify ***the competent authority*** about any changes to the details they submitted under paragraph ***1a*** without delay, and in any event, within three months from the date on which the change took effect. ***Without undue delay after its receipt, this information except the information referred to in paragraph 1a, point (d) shall be forwarded by the single point of contact of the Member State concerned to ENISA.***

▌

CHAPTER V

INFORMATION SHARING

Article 26

Cybersecurity information-sharing arrangements

1. ▌Member States shall ensure that essential and important entities ***and, where relevant, other relevant entities not covered by the scope of this Directive*** may exchange ***on a voluntary basis*** relevant cybersecurity information among themselves including information relating to cyber threats, ***near misses,*** vulnerabilities, ***techniques and procedures,*** indicators of compromise, ***adversarial*** tactics, ***threat actor specific information,*** cybersecurity alerts and ***recommendations regarding*** configuration ***of cybersecurity*** tools ***to detect cyber attacks***, 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, or response and recovery stages ***or promoting collaborative cyber threat research between public and private entities***.

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

3. Member States shall ***facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2. Such arrangements may specify*** operational elements (including the use of dedicated ICT platforms ***and automation tools***), content and conditions of the information sharing arrangements ▌. ***In laying*** down the details of the involvement of public authorities in such arrangements ***Member States may impose 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. ▌ENISA shall support the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by providing best practices and guidance.

Article 27

Voluntary notification of relevant information

1. Member States shall ensure that ▌ notifications ***may be submitted to the CSIRTs or where relevant competent authorities***, on a voluntary basis, ***by:***

(a) ***essential and important entities with regard to*** cyber threats***,*** near misses ***and relevant incidents which do not meet the criteria pursuant to Article 20(3);***

(b) ***entities falling outside the scope of this Directive, with regard to significant incidents, cyber threats or near misses.***

2. When processing notifications, Member States shall act in accordance with the procedure laid down in Article 20. Member States may prioritise the processing of mandatory notifications over voluntary notifications.

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. Without prejudice to the investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the reporting entity to which it would not have been subject had it not submitted the notification.

CHAPTER VI

SUPERVISION AND ENFORCEMENT

Article 28

General aspects concerning supervision and enforcement

1. Member States shall ensure that competent authorities effectively monitor and take the measures necessary to ensure compliance with ***the obligations under*** this Directive [redacted].

1a. Member States may allow competent authorities to prioritise supervision, which shall be based on a risk-based approach. For this purpose, where exercising their supervisory tasks provided for in Article 29 and Article 30, competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.

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

2a. Without prejudice to national legislative and institutional frameworks, Member States shall ensure that, in the supervision of compliance of public administration entities with this Directive and the enforcement of potential sanctions for non-compliance, the competent authorities have the appropriate powers to conduct such tasks with operational independence vis-à-vis the entities supervised. Member States may decide on the imposition of appropriate, proportionate and effective measures of supervision and enforcement in relation to these entities in accordance with the national frameworks and legal order.

Article 29

Supervision and enforcement for essential entities

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

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

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

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

   (c) ***ad hoc*** audits***, including 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***, where necessary, with the cooperation of the entity concerned***;

   (e) requests of information necessary to assess the cybersecurity measures adopted by the entity, including documented cybersecurity policies, as well as compliance with the obligation to notify the ***competent authorities*** pursuant to Article 25 ▌;

   (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 authority. The costs of such targeted security audit carried out by an independent body shall be paid by the entity concerned, except in duly justified cases when the competent authority decides otherwise.

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

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

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

   (b) issue binding instructions***, 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 ***the nature of the threat, as well as*** any possible protective or remedial measures which can be taken by those natural or legal person(s) in response to that threat;

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

(g) designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance with 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;

▌

(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 ***any of*** the measures referred to in points (a) to (h) 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 ***or courts according to national laws*** to ***temporarily*** suspend a certification or authorisation concerning part or all ***relevant*** services or activities provided by an essential entity;

(b) ▌ 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, ▌ 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, including effective judicial protection, due process, presumption of innocence and right of defence.***

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

6. Member States shall ensure that any natural person responsible for or acting as a representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the powers to ensure its compliance with the obligations laid down in this Directive. Member States shall ensure that those natural persons may be held liable for breach of their duties to ensure compliance with the obligations laid down in this Directive. ***As regards public administration entities, this provision shall be without prejudice to the Member States' laws as regards the liability of public servants and elected and appointed officials.***

7. Where taking any of the enforcement actions or applying any sanctions pursuant to paragraphs 4 and 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of:

(a) the seriousness of the infringement and the importance of the provisions breached. Among the infringements that should be considered as serious: repeated violations, failure to notify or remedy incidents with a significant disruptive effect, failure to remedy deficiencies following binding instructions from competent authorities obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement, providing false or grossly inaccurate information in relation to risk management requirements or reporting obligations set out in Articles 18 and 20.

(b) the duration of the infringement ▌;

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

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

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

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

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

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

8. The competent authorities shall set out a detailed reasoning for their enforcement decisions. Before taking such decisions, the competent authorities shall notify the entities concerned of their preliminary findings***. They shall also*** allow a reasonable time for those entities to submit observations***, except in duly justified cases where this could impede immediate action to prevent or respond to incidents***.

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

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

[*] ***The wording to be adapted to the text of Directive (EU) .../... on the resilience of critical entities, PE-CONS …/... (2020/0365(COD)).***

Article 30

Supervision and enforcement for important entities

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

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

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

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

   (d) requests for any information necessary to assess ex-post the cybersecurity measures, including documented cybersecurity policies, as well as compliance with the obligation to notify ***competent authorities*** pursuant to Article 25 ▌;

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

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

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

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

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

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

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

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

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

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

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

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

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

▌

(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 ***any of*** the measures referred to in points (a) to (***g***) of this paragraph, depending on the circumstances of each individual case.

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

Article 31

General conditions for imposing administrative fines on essential and important entities

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

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

3. Where deciding whether to impose an administrative fine and deciding on its amount in each individual case due regard shall be given, as a minimum, to the elements provided for in Article 29(7).

4. Member States shall ensure that infringements ***by essential entities*** of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 10 000 000 EUR or ▌2% of the total worldwide annual turnover of the undertaking to which the ▌ entity belongs in the preceding financial year, whichever is higher.

4a. Member States shall ensure that infringements by the important entities of the obligations laid down in Article 18 or Article 20 shall, in accordance with paragraphs 2 and 3 of this Article, be subject to administrative fines of a maximum of at least 7 000 000 EUR or 1.4 % of the total worldwide annual turnover of the undertaking to which the important entity belongs in the preceding financial year, whichever is higher.

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

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

6a. Where the legal system of the Member State does not provide for administrative fines, Member States shall ensure that this Article may be applied in such a manner that the fine is initiated by the competent authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by the competent authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by the date of transposition of this Directive and, without delay, any subsequent amendment law or amendment affecting them.

Article 32

Infringements entailing a personal data breach

1. Where***, in the course of supervision or enforcement,*** the competent authorities have ***become aware*** that the infringement by an essential or important entity of the obligations laid down in Articles 18 and 20 ***of this Directive may entail*** a personal data breach, as defined by Article 4(12) of Regulation (EU) 2016/679 which shall be notified pursuant to Article 33 of that Regulation, they shall***, without undue delay,*** inform the supervisory authorities competent pursuant to Articles 55 and 56 of that Regulation ▌.

2. Where the supervisory authorities competent in accordance with Articles 55 and 56 of Regulation (EU) 2016/679 decide to exercise their powers pursuant to Article 58***(2)***(i) of that Regulation and impose an administrative fine, the competent authorities ***referred to in Article 8 of this Directive*** shall not impose an administrative fine for ***an*** infringement ***by the same deed of*** Article 31 of this Directive. The competent authorities may, however, apply the enforcement actions or exercise the sanctioning powers provided for in points (a) to (h) of Article 29(4), Article 29 (5), and points (a) to (g) 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.

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 ***twenty four months*** following the entry into force of this Directive, notify the Commission of those rules and of those measures and shall notify it, without undue delay of any subsequent amendment affecting them.

Article 34

Mutual assistance

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

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

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

(c) a competent authority shall, upon receipt of a justified request from another competent authority, provide the other competent authority with assistance ***proportionate to the resources at its own disposal so that the supervision or enforcement actions*** can be implemented in an effective, efficient and consistent manner. Such mutual assistance may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed may not refuse that request unless, after an exchange with the other authorities concerned, ▌ and***, upon request of one of the Member States concerned, with*** the Commission ***in consultation with ENISA***, it is established that ▌ 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 ***or the request concerns information or entails activities which are in conflict with that Member State's national security or public security or defence***.

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

CHAPTER VII

TRANSITIONAL AND FINAL PROVISIONS

Article 35

Review

By ... [36 months after the transposition deadline of this Directive] and every 36 months thereafter, the Commission shall ▌review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of ***the*** 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***.

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 ***Article*** 21(2) shall be conferred on the Commission for a period of five years from [***the date of entry into force of this Directive***].

3. The delegation of power referred to in ***Article*** 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 ***Article*** 21(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 37

Committee procedure

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

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

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

Article 38

Transposition

1. ▌By … [*21* months after the date of entry into force of this Directive], ***Member States shall adopt and publish*** the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from … [one day after the date referred to in the first subparagraph].

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

Article 39

Amendment of Regulation (EU) No 910/2014

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

Article 40

Amendment of Directive (EU) 2018/1972

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

Article 41

Repeal

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

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

Article 42

Entry into force

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

Article 43

Addressees

This Directive is addressed to the Member States.

Done at ...,

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

ANNEX I

SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings referred to in point (57) of Article 2 of Directive (EU) 2019/944, which carry out the function of 'supply' referred to in point (12) of Article 2 of that Directive([42])
		— Distribution system operators referred to in point (29) of Article 2 of Directive (EU) 2019/944
		— Transmission system operators referred to in point (35) of Article 2 of Directive (EU) 2019/944
		— Producers referred to in point (38) of Article 2 of Directive (EU) 2019/944
		— Nominated electricity market operators referred to in point 8 of Article 2 of Regulation (EU) 2019/943([43])
		— Electricity market participants referred to in point (25) of Article

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

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

Sector	Subsector	Type of entity
		2 of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services referred to in points (18), (20) and (59) of Article 2 of Directive (EU) 2019/944 — ***Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider***
	(b) District heating and cooling	— District heating or district cooling referred to in point (19) of Article 2 of the Directive (EU) 2018/2001([44]) on the promotion of the use of energy from renewable sources
	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		— Central oil stockholding entities

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

Sector	Subsector	Type of entity
		referred to in point (f) of Article 2 of Council Directive 2009/119/EC([45])
	(d) Gas	— Supply undertakings referred to in point (8) of Article 2 of Directive (EU) 2009/73/EC([46])
		— Distribution system operators referred to in point (6) of Article 2 of Directive 2009/73/EC
		— Transmission system operators referred to point (4) of Article 2 of Directive 2009/73/EC
		— Storage system operators referred to in point (10) of Article 2 of Directive 2009/73/EC
		— LNG system operators referred to in point (12) of Article 2 of Directive 2009/73/EC
		— Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities

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

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

Sector	Subsector	Type of entity
	(e) Hydrogen	— Operators of hydrogen production, storage and transmission
2. Transport	(a) Air	— Air carriers referred to in point (4) of Article 3 of Regulation (EC) No 300/2008([47]) ***used for commercial purposes***
		— Airport managing bodies referred to in point (2) of Article 2 of Directive 2009/12/EC([48]), airports referred to in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013([49]), and entities operating ancillary installations contained within airports
		— Traffic management control operators providing air traffic control (ATC) services referred to in point (1) of Article 2 of Regulation (EC) No 549/2004([50])

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

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

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

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

Sector	Subsector	Type of entity
	(b) Rail	— Infrastructure managers referred to in point (2) of Article 3 of Directive 2012/34/EU([51])
		— Railway undertakings referred to in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities referred to in point (12) of Article 3 of Directive 2012/34/EU
	(c) Water	— Inland, sea and coastal passenger and freight water transport companies, referred to for maritime transport in Annex I to Regulation (EC) No 725/2004([52]), not including the individual vessels operated by those companies
		— Managing bodies of ports referred to in point (1) of Article 3 of Directive 2005/65/EC([53]), including their port facilities referred to in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained

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

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

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

Sector	Subsector	Type of entity
		within ports
		— Operators of vessel traffic services referred to in point (o) of Article 3 of Directive 2002/59/EC([54])
	(d) Road	— Road authorities referred to in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962([55]) responsible for traffic management control***, excluding public entities for whom traffic-management or operators of intelligent transport systems is only a non-essential part of their general activity***
		— Operators of Intelligent Transport Systems referred to in point (1) of Article 4 of Directive 2010/40/EU([56])

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

[55] 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).

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

Sector	Subsector	Type of entity
3. Banking		— Credit institutions referred to in point (1) of Article 4 of Regulation (EU) No 575/2013([57])
4. Financial market infrastructures		— Operators of trading venues referred to in point (24) of Article 4 of Directive 2014/65/EU([58])
		— Central counterparties (CCPs) referred to in point (1) of Article 2 of Regulation (EU) No 648/2012([59])
5. Health		— Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU([60])
		— EU reference laboratories referred to in Article 15 of Regulation XXXX/XXXX on serious cross-border threats to health[61]

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

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

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

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

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

Sector	Subsector	Type of entity
		— Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC([62]) — Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 — Entities manufacturing medical devices considered as critical during a public health emergency ('the public health emergency critical devices list') referred to in Article 20 of Regulation XXXX[63]
6. Drinking water		Suppliers and distributors of water intended for human consumption referred to in point (1)(a) of Article 2 of Council Directive 98/83/EC([64]) but excluding distributors for whom distribution of water for human consumption is only ***non-essential***

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

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

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

Sector	Subsector	Type of entity
		part of their general activity of distributing other commodities and goods ▌
7. Waste water		Undertakings collecting, disposing or treating urban, domestic and industrial waste water referred to in points (1) to (3) of Article 2 of Council Directive 91/271/EEC([65]) ***but excluding undertakings for whom collecting, disposing or treating of urban, domestic and industrial waste water is only a non-essential part of their general activity***
8. Digital infrastructure		— Internet Exchange Point providers
		— DNS service providers***, excluding operators of root name servers***
		— TLD name registries
		— Cloud computing service providers
		— Data centre service providers
		— Content delivery network providers

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

Sector	Subsector	Type of entity
		— Trust service providers referred to in point (19) of Article 3 of Regulation (EU) No 910/2014([66])
		— Providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972([67]) or providers of electronic communications services referred to in point (4) of Article 2 of Directive (EU) 2018/1972 where their services are publicly available
8a. ICT-service management (B2B)		***— Managed service providers (MSP)*** ***— Managed Security service providers (MSSP)***
9. Public administration ***entities excluding the judiciary, parliaments and central banks***		— Public administration entities of central governments ***as defined by a Member State in accordance with national law***
		— Public administration entities ***at regional*** level ***as defined by a Member State in accordance***

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

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

Sector	Subsector	Type of entity
		with national law
		▌
10. Space		Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks referred to in point (8) of Article 2 of Directive (EU) 2018/1972

ANNEX II

OTHER CRITICAL SECTORS

Sector	Subsector	Type of entity
1. Postal and courier services		Postal service providers referred to in point (1) of Article 2 of Directive 97/67/EC([68])***, including*** providers of courier services
2. Waste management		Undertakings carrying out waste management referred to in point (9) of Article 3 of Directive 2008/98/EC([69]) but excluding undertakings for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		Undertakings carrying out the manufacture ▌ and distribution of substances and ***mixtures*** referred to in points ▌ (9) and (14) of Article 3 of Regulation (EC) No 1907/2006([70]) ***and undertakings carrying out the production of articles referred to in point (3) of Article 3 of that Regulation from substances or***

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

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

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

Sector	Subsector	Type of entity
		mixtures
4. Food production, processing and distribution		Food businesses referred to in point (2) of Article 3 of Regulation (EC) No 178/2002([71]) ***which are engaged in wholesale distribution and industrial production and processing***
5. Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices referred to in Article 2 point 1 of Regulation (EU) 2017/745([72]), and entities manufacturing in vitro diagnostic medical devices referred to in Article 2 point 2 of Regulation (EU) 2017/746([73]) with exception of entities manufacturing medical devices mentioned in Annex 1, point 5.
	(b) Manufacture of computer, electronic and optical products	Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	(c) Manufacture of electrical equipment	Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2

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

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

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

Sector	Subsector	Type of entity
	(d) Manufacture of machinery and equipment n.e.c.	Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
	(e) Manufacture of motor vehicles, trailers and semi-trailers	Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2
	(f) Manufacture of other transport equipment	Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2
6. Digital providers		— Providers of online marketplaces
		— Providers of online search engines
		— Providers of social networking services platform
6a. Research		***— Research organisations as defined in Article 4: [for the purpose of this directive]***

ANNEX III

CORRELATION TABLE

Directive (EU) 2016/1148	This Directive
Article 1 (1)	Article 1 (1)
Article 1 (2)	Article 1 (2)
Article 1 (3)	-
Article 1 (4)	Article 2 (4)
Article 1 (5)	Article 2 (5)
Article 1 (6)	Article 2 (3)
Article 1 (7)	Article 2 (6)
Article 2	-
Article 3	Article 3
Article 4	Article 4
Article 5	-
Article 6	-
Article 7 (1)	Article 5 (1)
Article 7 (2)	Article 5 (4)
Article 7 (3)	Article 5 (3)
Article 8 (1)–(5)	Article 8 (1)–(5)

Directive (EU) 2016/1148	This Directive
Article 8 (6)	Article 11 (4)
Article 8 (7)	Article 8 (6)
Article 9 (1)-(3)	Article 9 (1)-(3)
Article 9 (4)	Article 9 (7)
Article 9 (5)	Article 9 (8)
Article 10 (1)-(3)	Article 11 (1)-(3)
Article 11 (1)	Article 12 (1) –(2)
Article 11 (2)	Article 12 (3)
Article 11 (3)	Article 12(4) and (6)
Article 11 (4)	-
Article 11 (5)	Article 12 (7)
Article 12 (1)-((5)	Article 13 (1)-(5)
Article 13	-
Article 14 (1)	Article 18 (1)
Article 14 (2)	Article 18 (2)-(4)
Article 14 (3)	Article 20 (1)
Article 14 (4)	Article 20 (3)
Article 14 (5)	Article 20 (5), (6), (8)
Article 14 (6)	Article 20 (7)
Article 14 (7)	-

Directive (EU) 2016/1148	This Directive
Article 15 (1)	Article 29 (2)
Article 15 (2)(a)	Article 29 (2) (e)
Article 15 (2)(b)	Article 29 (2) (g)
Article 15 (2) second indent	Article 29 (3)
Article 15 (3)	Article 29 (4) (b)
Article 15 (4)	Article 28 (2)
Article 16 (1)	Article 18 (1), (2)
Article 16 (2)	Article 18 (2)-(4)
Article 16 (3)	Article 20 (1)
Article 16 (4)	Article 20 (3)
Article 16 (5)	-
Article 16 (6)	Article 20 (6)
Article 16 (7)	Article 20 (7)
Article 16 (8), (9)	Article 20 (11)
Article 16 (10)	-
Article 16 (11)	Article 2 (1)
Article 17 (1)	-
Article 17 (2)(a)	Article 29 (2) (e)
Article 17 (2)(b)	Article 29 (4) (b)
Article 17 (3)	Article 34 (1) (a), (b)

Directive (EU) 2016/1148	This Directive
Article 18 (1)	Article 24 (1)-(2)
Article 18 (2)	Article 24 (3)
Article 18 (3)	Article 24 (4)
Article 19	Article 22
Article 20	Article 27
Article 21	Article 33
Article 22 (1)-(2)	Article 37 (1)-(2)
Article 23	Article 35
Article 24	-
Article 25	Article 38
Article 26	Article 42
Article 27	Article 43
Annex I(1)	Article 10 (1)
Annex I (2) (a) (i)-(iv)	Article 10 (2) (a)-(d)
Annex I (2) (a) (v)	Article 10 (2) (f)
Annex I (2) (b)	Article 10 (3)
Annex I (2) (c) (i)-(ii)	Article 10 (4) (a)

Directive (EU) 2016/1148	This Directive
Annex II	Annex I
Annex III 1, 2	Annex II, 6.
Annex III, 3	Annex I, 8.