DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

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 Central Bank ([1]),

Having regard to the opinion of the European Economic and Social Committee ([2]),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) Directive (EU) 2016/1148 of the European Parliament and the Council ([4]) aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing 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 cyber 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 on the security of network and information systems by establishing national strategies on security of network and information systems and establishing national capabilities and by implementing regulatory measures covering essential infrastructures and entities identified by each Member State. Directive (EU) 2016/1148 has also contributed to cooperation at Union level through the establishment of the Cooperation Group and the network of national computer security incident response teams. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively current and emerging cybersecurity challenges.

(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 cyber 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 incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss,

([1]) OJ C 233, 16.6.2022, p. 22.
([2]) OJ C 286, 16.7.2021, p. 170.
([3]) Position of the European Parliament of 10 November 2022 (not yet published in the Official Journal) and decision of the Council of 28 November 2022.
([4]) 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, 19.7.2016, p. 1).

undermine user confidence and cause major damage to the Union's 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.

(4) The legal basis of Directive (EU) 2016/1148 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 carrying out activities which are economically significant 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 entities that offer goods or services across borders. Requirements imposed by one Member State that are different from, or even in conflict with, those imposed by another Member State, may substantially affect such cross-border activities. Furthermore, the possibility of the inadequate design or implementation of cybersecurity requirements in one Member State is likely to have repercussions at the level of cybersecurity of other Member States, in particular given the intensity of 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 the implementation of the security and incident reporting obligations laid down therein. Those obligations were therefore implemented in significantly different ways at national level. There are similar divergences in the implementation of the provisions of Directive (EU) 2016/1148 on supervision and enforcement.

(5) All those divergences entail a fragmentation of the internal market and can have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and the level of cyber resilience due to the application of a variety of measures. Ultimately, those divergences could lead to the higher vulnerability of some Member States to cyber 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 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 enforcement measures which are key to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.

(6) With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy to provide a comprehensive coverage of sectors and services of vital importance to key societal and economic activities in the internal market. In particular, this Directive aims to overcome the shortcomings of the differentiation between operators of essential services and digital service providers, which has been proven to be obsolete, since it does not reflect the importance of the sectors or services for the societal and economic activities in the internal market.

(7) Under Directive (EU) 2016/1148, Member States were responsible for identifying the entities which met the criteria to qualify as operators of essential services. In order to eliminate the wide divergences among Member States in that regard and ensure legal certainty as regards the cybersecurity risk-management measures and reporting obligations for all relevant entities, a uniform criterion should be established that determines the entities falling within the scope of this Directive. That criterion should consist of the application of a size-cap rule, whereby all entities which qualify as medium-sized enterprises under Article 2 of the Annex to Commission Recommendation 2003/361/EC ([5]), or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which operate within the sectors and provide the types of service or carry out the activities covered by this

([5]) 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).

Directive fall within its scope. Member States should also provide for certain small enterprises and microenterprises, as defined in Article 2(2) and (3) of that Annex, which fulfil specific criteria that indicate a key role for society, the economy or for particular sectors or types of service to fall within the scope of this Directive.

(8) The exclusion of public administration entities from the scope of this Directive should apply to entities whose activities are predominantly carried out in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences. However, public administration entities whose activities are only marginally related to those areas should not be excluded from the scope of this Directive. For the purposes of this Directive, entities with regulatory competences are not considered to be carrying out activities in the area of law enforcement and are therefore not excluded on that ground from the scope of this Directive. Public administration entities that are jointly established with a third country in accordance with an international agreement are excluded from the scope of this Directive. This Directive does not apply to Member States' diplomatic and consular missions in third countries or 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.

(9) Member States should be able to take the necessary measures to ensure the protection of the essential interests of national security, to safeguard public policy and public security, and to allow for the prevention, investigation, detection and prosecution of criminal offences. To that end, Member States should be able to exempt specific entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, from certain obligations laid down in this Directive with regard to those activities. Where an entity provides services exclusively to a public administration entity that is excluded from the scope of this Directive, Member States should be able to exempt that entity from certain obligations laid down in this Directive with regard to those services. Furthermore, no Member State should be required to supply information the disclosure of which would be contrary to the essential interests of its national security, public security or defence. Union or national rules for the protection of classified information, non-disclosure agreements, and informal non-disclosure agreements such as the traffic light protocol should be taken into account in that context. The traffic light protocol is to be understood as a means to provide information about any limitations with regard to the further spreading of information. It is used in almost all computer security incident response teams (CSIRTs) and in some information analysis and sharing centres.

(10) Although this Directive applies to entities carrying out activities in the production of electricity from nuclear power plants, some of those activities may be linked to national security. Where that is the case, a Member State should be able to exercise its responsibility for safeguarding national security with respect to those activities, including activities within the nuclear value chain, in accordance with the Treaties.

(11) Some entities carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, while also providing trust services. Trust service providers which fall within the scope of Regulation (EU) No 910/2014 of the European Parliament and of the Council ([6]) should fall within the scope of this Directive in order to secure the same level of security requirements and supervision as that which was previously laid down in that Regulation in respect of trust service providers. In line with the exclusion of certain specific services from Regulation (EU) No 910/2014, 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.

([6]) 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).

(12) Postal service providers as defined in Directive 97/67/EC of the European Parliament and of the Council ([7]), including providers of courier services, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain, in particular clearance, sorting, transport or distribution of postal items, including pick-up services, while taking account of the degree of their dependence on network and information systems. Transport services that are not undertaken in conjunction with one of those steps should be excluded from the scope of postal services.

(13) 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 those entities.

(14) Union data protection law and Union privacy law applies to any processing of personal data under this Directive. In particular, this Directive is without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council ([8]) and Directive 2002/58/EC of the European Parliament and of the Council ([9]). This Directive should therefore not affect, inter alia, the tasks and powers of the authorities competent to monitor compliance with the applicable Union data protection law and Union privacy law.

(15) Entities falling within the scope of this Directive for the purpose of compliance with cybersecurity risk-management measures and reporting obligations should be classified into two categories, essential entities and important entities, reflecting the extent to which they are critical as regards their sector or the type of service they provide, as well as their size. In that regard, due account should be taken of any relevant sectoral risk assessments or guidance by the competent authorities, where applicable. The supervisory and enforcement regimes for those two categories of entities should be differentiated to ensure a fair balance between risk-based requirements and obligations on the one hand, and the administrative burden stemming from the supervision of compliance on the other.

(16) In order to avoid entities that have partner enterprises or that are linked enterprises being considered to be essential or important entities where this would be disproportionate, Member States are able to take into account the degree of independence an entity enjoys in relation to its partner or linked enterprises when applying Article 6(2) of the Annex to Recommendation 2003/361/EC. In particular, Member States are able to take into account the fact that an entity is independent from its partner or linked enterprises in terms of the network and information systems that that entity uses in the provision of its services and in terms of the services that the entity provides. On that basis, where appropriate, Member States are able to consider that such an entity does not qualify as a medium-sized enterprise under Article 2 of the Annex to Recommendation 2003/361/EC, or does not exceed the ceilings for a medium-sized enterprise provided for in paragraph 1 of that Article, if, after taking into account the degree of independence of that entity, that entity would not have been considered to qualify as a medium-sized enterprise or to exceed those ceilings in the event that only its own data had been taken into account. This leaves unaffected the obligations laid down in this Directive of partner and linked enterprises which fall within the scope of this Directive.

(17) Member States should be able to decide 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 to be essential entities.

([7]) 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).

([8]) 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).

([9]) 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).

(18) In order to ensure a clear overview of the entities falling within the scope of this Directive, Member States should establish a list of essential and important entities as well as entities providing domain name registration services. For that purpose, Member States should require entities to submit at least the following information to the competent authorities, namely, the name, address and up-to-date contact details, including the email addresses, IP ranges and telephone numbers of the entity, and, where applicable, the relevant sector and subsector referred to in the annexes, as well as, where applicable, a list of the Member States where they provide services falling within the scope of this Directive. To that end, the Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA), should, without undue delay, provide guidelines and templates regarding the obligation to submit information. To facilitate the establishing and updating of the list of essential and important entities as well as entities providing domain name registration services, Member States should be able to establish national mechanisms for entities to register themselves. Where registers exist at national level, Member States can decide on the appropriate mechanisms that allow for the identification of entities falling within the scope of this Directive.

(19) Member States should be responsible for submitting to the Commission at least the number of essential and important entities for each sector and subsector referred to in the annexes, as well as relevant information about the number of identified entities and the provision, from among those laid down in this Directive, on the basis of which they were identified, and the type of service that they provide. Member States are encouraged to exchange with the Commission information about essential and important entities and, in the case of a large-scale cybersecurity incident, relevant information such as the name of the entity concerned.

(20) The Commission should, in cooperation with the Cooperation Group and after consulting the relevant stakeholders, provide guidelines on the implementation of the criteria applicable to microenterprises and small enterprises for the assessment of whether they fall within the scope of this Directive. The Commission should also ensure that appropriate guidance is given to microenterprises and small enterprises falling within the scope of this Directive. The Commission should, with the assistance of the Member States, make information available to microenterprises and small enterprises in that regard.

(21) The Commission could provide guidance to assist Member States in implementing the provisions of this Directive on 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 carry out activities, some of which fall within and some of which are excluded from the scope of this Directive.

(22) This Directive sets out the baseline for cybersecurity risk-management measures and reporting obligations across the sectors that fall within its scope. In order to avoid the fragmentation of cybersecurity provisions of Union legal acts, where further sector-specific Union legal acts pertaining to cybersecurity risk-management measures and reporting obligations are considered to be necessary to ensure a high level of cybersecurity across the Union, the Commission should assess whether such further provisions could be stipulated in an implementing act under this Directive. Should such an implementing act not be suitable for that purpose, sector-specific Union legal acts could contribute to ensuring a high level of cybersecurity across the Union, while taking full account of the specificities and complexities of the sectors concerned. To that end, this Directive does not preclude the adoption of further sector-specific Union legal acts addressing cybersecurity risk-management measures and reporting obligations that take due account of the need for a comprehensive and consistent cybersecurity framework. This Directive is without prejudice to the existing implementing powers that have been conferred on the Commission in a number of sectors, including transport and energy.

(23) Where a sector-specific Union legal act contains provisions requiring 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, those provisions, including on supervision

and enforcement, should apply to such entities. If a sector-specific Union legal act does 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 that act.

(24) Where provisions of a sector-specific Union legal act require essential or important entities to comply with reporting obligations that are at least equivalent in effect to the reporting obligations laid down in this Directive, the consistency and effectiveness of the handling of incident notifications should be ensured. To that end, the provisions relating to incident notifications of the sector-specific Union legal act should provide the CSIRTs, the competent authorities or the single points of contact on cybersecurity (single points of contact) under this Directive with an immediate access to the incident notifications submitted in accordance with the sector-specific Union legal act. In particular, such immediate access can be ensured if incident notifications are being forwarded without undue delay to the CSIRT, the competent authority or the single point of contact under this Directive. Where appropriate, Member States should put in place an automatic and direct reporting mechanism that ensures systematic and immediate sharing of information with the CSIRTs, the competent authorities or the single points of contact concerning the handling of such incident notifications. For the purpose of simplifying reporting and of implementing the automatic and direct reporting mechanism, Member States could, in accordance with the sector-specific Union legal act, use a single entry point.

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

(26) Where sector-specific Union legal acts require or provide incentives to entities to notify significant cyber threats, Member States should also encourage the sharing of significant cyber threats with the CSIRTs, the competent authorities or the single points of contact under this Directive, in order to ensure an enhanced level of those bodies' awareness of the cyber threat landscape and to enable them to respond effectively and in a timely manner should the significant cyber threats materialise.

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

(28) Regulation (EU) 2022/2554 of the European Parliament and of the Council ([10]) should be considered to be a sector-specific Union legal act in relation to this Directive with regard to financial entities. The provisions of Regulation (EU) 2022/2554 relating to information and communication technology (ICT) risk management, management of ICT-related incidents and, in particular, major ICT-related incident reporting, as well as on digital operational resilience testing, information-sharing arrangements and ICT third-party risk should apply instead of those provided for 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 (EU) 2022/2554. 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 (EU) 2022/2554 allows the European Supervisory Authorities (ESAs) and the competent authorities under that Regulation to participate in the activities of the Cooperation Group and to exchange information and cooperate with the single points of contact, as well as with the CSIRTs and the competent authorities under this Directive. The competent authorities under Regulation (EU) 2022/2554 should also transmit details of major ICT-related incidents and, where relevant, significant cyber threats to the CSIRTs, the competent authorities or the single points of contact under this Directive. This is achievable by providing immediate access to incident notifications and forwarding them either

([10]) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (see page 1 of this Official Journal).

directly or through a single entry point. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies and CSIRTs can cover the financial sector in their activities.

(29) In order to avoid gaps between or duplications of cybersecurity obligations imposed on entities in the aviation sector, national authorities under Regulations (EC) No 300/2008 ([11]) and (EU) 2018/1139 ([12]) of the European Parliament and of the Council and the competent authorities under this Directive should cooperate in relation to the implementation of cybersecurity risk-management measures and the supervision of compliance with those measures at national level. The compliance of an entity with the security requirements laid down in Regulations (EC) No 300/2008 and (EU) 2018/1139 and in the relevant delegated and implementing acts adopted pursuant to those Regulations could be considered by the competent authorities under this Directive to constitute compliance with the corresponding requirements laid down in this Directive.

(30) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) 2022/2557 of the European Parliament and of the Council ([13]) and this Directive. To achieve this, entities identified as critical entities under Directive (EU) 2022/2557 should be considered to be essential entities under this Directive. Moreover, each Member State should ensure that its national cybersecurity strategy provides for a policy framework for enhanced coordination within that Member State between its competent authorities under this Directive and those under Directive (EU) 2022/2557 in the context of information sharing about risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents, and the exercise of supervisory tasks. The competent authorities under this Directive and those under Directive (EU) 2022/2557 should cooperate and exchange information without undue delay, in particular in relation to the identification of critical entities, risks, cyber threats, and incidents as well as in relation to non-cyber risks, threats and incidents affecting critical entities, including the cybersecurity and physical measures taken by critical entities as well as the results of supervisory activities carried out with regard to such entities.

Furthermore, in order to streamline supervisory activities between the competent authorities under this Directive and those under Directive (EU) 2022/2557 and in order to minimise the administrative burden for the entities concerned, those competent authorities should endeavour to harmonise incident notification templates and supervisory processes. Where appropriate, the competent authorities under Directive (EU) 2022/2557, should be able to request the competent authorities under this Directive to exercise their supervisory and enforcement powers in relation to an entity that is identified as a critical entity under Directive (EU) 2022/2557. The competent authorities under this Directive and those under Directive (EU) 2022/2557 should, where possible in real time, cooperate and exchange information for that purpose.

(31) Entities belonging to the digital infrastructure sector are in essence based on network and information systems and therefore the obligations imposed on those entities pursuant to this Directive should address in a comprehensive manner the physical security of such systems as part of their cybersecurity risk-management measures and reporting obligations. Since those matters are covered by this Directive, the obligations laid down in Chapters III, IV and VI of Directive (EU) 2022/2557 do not apply to such entities.

([11]) 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).

([12]) 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).

([13]) Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (see page 164 of this Official Journal).

(32) Upholding and preserving a reliable, resilient and secure domain name system (DNS) are key factors in maintaining the integrity of the internet and are 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 registries, and DNS service providers that are to be understood as entities providing publicly available recursive domain name resolution services for internet end-users or authoritative domain name resolution services for third-party usage. This Directive should not apply to root name servers.

(33) Cloud computing services should cover digital services that enable on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations. 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, inter alia, 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 cloud computing 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 and 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 computing resources that are provided and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe 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 computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing.

(34) Given the emergence of innovative technologies and new business models, new cloud computing service and deployment models are expected to appear in the internal 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).

(35) Services offered by data centre service providers may not always be provided in the form of a 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 therefore cover providers of data centre services that are not cloud computing services. For the purposes 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 (IT) 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' should not apply to in-house corporate data centres owned and operated by the entity concerned, for its own purposes.

(36) Research activities play a key role in the development of new products and processes. Many of those activities are carried out by entities that share, disseminate or exploit the results of their research for commercial purposes. Those 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 include entities which focus the essential part of their activities on the conduct of applied

research or experimental development, within the meaning of the Organisation for Economic Cooperation and Development's Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development, with a view to exploiting their results for commercial purposes, such as the manufacturing or development of a product or process, the provision of a service, or the marketing thereof.

(37) The growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in sectors such as energy, transport, digital infrastructure, drinking water and waste water, health, certain aspects of public administration, as well as space in so 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 programme. 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 cyberattacks during the COVID-19 pandemic have shown the vulnerability of increasingly interdependent societies in the face of low-probability risks.

(38) 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 or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks under this Directive.

(39) 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 single point of contact responsible for coordinating issues related to the security of network and information systems and cross-border cooperation at Union level.

(40) The single points of contact should ensure effective cross-border cooperation with relevant authorities of other Member States and, where appropriate, with the Commission and ENISA. The single points of contact should therefore be tasked with forwarding notifications of significant incidents with cross-border impact to the single points of contact of other affected Member States upon the request of the CSIRT or the competent authority. At national level, the single points of contact should enable smooth cross-sectoral cooperation with other competent authorities. The single points of contact could also be the addressees of relevant information about incidents concerning financial entities from the competent authorities under Regulation (EU) 2022/2554 which they should be able to forward, as appropriate, to the CSIRTs or the competent authorities under this Directive.

(41) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate incidents and risks. Member States should therefore establish or designate one or more CSIRTs under this Directive and ensure that they have adequate resources and technical capabilities. The CSIRTs should comply with the requirements laid down in this Directive in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. Member States should be able to designate existing computer emergency response teams (CERTs) as CSIRTs. In order to enhance the trust relationship between the entities and the CSIRTs, where a CSIRT is part of a competent authority, Member States should be able to consider functional separation between the operational tasks provided by the CSIRTs, in particular in relation to information sharing and assistance provided to the entities, and the supervisory activities of the competent authorities.

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

(43) As regards personal data, the CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679, upon the request of an essential or important entity, a proactive scanning of the network and information systems used for the provision of the entity's services. Where applicable, Member States should aim to ensure an equal level of technical capabilities for all sectoral CSIRTs. Member States should be able to request the assistance of ENISA in developing their CSIRTs.

(44) The CSIRTs should have the ability, upon an essential or important entity's request, to monitor the entity's internet-facing assets, both on and off premises, in order to identify, understand and manage the entity's overall organisational risks as regards newly identified 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.

(45) Given the importance of international cooperation on cybersecurity, the 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, the CSIRTs and the competent authorities should be able to exchange information, including personal data, with the national computer security incident response teams or competent authorities of third countries provided that the conditions under Union data protection law for transfers of personal data to third countries, inter alia those of Article 49 of Regulation (EU) 2016/679, are met.

(46) Ensuring adequate resources to meet the objectives of this Directive and to enable the competent authorities and the CSIRTs to carry out the tasks laid down herein is essential. The Member States can introduce at the national level a 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 and non-discriminatory and should take into account different approaches to providing secure services.

(47) 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.

(48) For the purpose of achieving and maintaining a high level of cybersecurity, the national cybersecurity strategies required under this Directive should consist of coherent frameworks providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them. Those strategies can be composed of one or more legislative or non-legislative instruments.

(49) 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 upon which entities rely. Cyber hygiene policies comprising a common baseline set of practices, including software and hardware updates, password changes, the management of new installs, the limitation of administrator-level access accounts, and the backing-up of data, enable a proactive framework of preparedness and overall safety and security in the event of incidents or cyber threats. ENISA should monitor and analyse Member States' cyber hygiene policies.

(50) Cybersecurity awareness and cyber hygiene are essential to enhance the level of cybersecurity within the Union, in particular in light of the growing number of connected devices that are increasingly used in cyberattacks. Efforts should be made to enhance the overall awareness of risks related to such devices, while assessments at Union level could help ensure a common understanding of such risks within the internal market.

(51) Member States should encourage the use of any innovative technology, including artificial intelligence, the use of which could improve the detection and prevention of cyberattacks, enabling resources to be diverted towards cyberattacks more effectively. Member States should therefore encourage in their national cybersecurity strategy activities in research and development to facilitate the use of such technologies, in particular those relating to automated or semi-automated tools in cybersecurity, and, where relevant, the sharing of data needed for training users of such technology and for improving it. The use of any innovative technology, including artificial intelligence, should comply with Union data protection law, including the data protection principles of data accuracy, data minimisation, fairness and transparency, and 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.

(52) 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 use 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 introduction and sustainable use of open-source cybersecurity tools are of particular importance for small and medium-sized enterprises facing significant costs for implementation, which could be minimised by reducing the need for specific applications or tools.

(53) Utilities are increasingly connected to digital networks in cities, for the purpose of improving urban transport networks, upgrading water supply and waste disposal facilities and increasing the efficiency of lighting and the heating of buildings. Those digitalised utilities are vulnerable to cyberattacks and run the risk, in the event of a successful cyberattack, of harming citizens at a large scale due to their interconnectedness. Member States should develop a policy that addresses the development of such connected or smart cities, and their potential effects on society, as part of their national cybersecurity strategy.

(54) In recent years, the Union has faced an exponential increase in ransomware attacks, in which malware encrypts data and systems and demands a ransom payment for release. The increasing frequency and severity of ransomware attacks can be driven by several factors, such as different attack patterns, criminal business models 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 cybersecurity strategy.

(55) Public-private partnerships (PPPs) in the field of cybersecurity can provide an appropriate framework for knowledge exchange, the sharing of best practices and the establishment of a common level of understanding among 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 with regard to PPPs. PPPs can leverage the expertise of private-sector entities to assist the competent authorities in developing state-of-the-art services and processes including information exchange, early warnings, cyber threat and incident exercises, crisis management and resilience planning.

(56) Member States should, in their national cybersecurity strategies, address the specific cybersecurity needs of small and medium-sized enterprises. Small and medium-sized enterprises represent, across the Union, a large percentage of the industrial and business market and often struggle to adapt to new business practices in a more connected world and to the digital environment, with employees working from home and business increasingly being conducted online. Some small and medium-sized enterprises 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 assistance. Small and medium-sized enterprises are increasingly becoming the target of supply chain attacks due to their less rigorous cybersecurity risk-management measures and attack management, and the fact that they have limited security resources. Such supply chain attacks not only have an impact on small and medium-sized enterprises and their operations in isolation but can also have a cascading effect on larger attacks on entities to which they provided supplies. Member States should, through their national

cybersecurity strategies, help small and medium-sized enterprises to address the challenges faced in their supply chains. Member States should have a point of contact for small and medium-sized enterprises at national or regional level, which either provides guidance and assistance to small and medium-sized enterprises or directs them to the appropriate bodies for guidance and assistance with regard to cybersecurity related issues. Member States are also encouraged to offer services such as website configuration and logging enabling to microenterprises and small enterprises that lack those capabilities.

(57) 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 certain 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 preventing, detecting, addressing and blocking attacks against network and information systems. Active cyber protection is based on a defensive strategy that excludes offensive measures.

(58) Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying such vulnerabilities is an important factor in reducing risk. Entities that develop or administer network and information systems should therefore establish appropriate procedures to handle vulnerabilities when they are discovered. Since vulnerabilities are often discovered and disclosed by third parties, the manufacturer or provider of ICT products or ICT services should also put in place the necessary procedures to receive vulnerability information from third parties. In that regard, international standards ISO/IEC 30111 and ISO/IEC 29147 provide guidance on vulnerability handling and vulnerability disclosure. Strengthening the coordination between reporting natural and legal persons and manufacturers or providers of ICT products or ICT services is particularly important for the purpose of facilitating the voluntary framework of vulnerability disclosure. Coordinated vulnerability disclosure specifies a structured process through which vulnerabilities are reported to the manufacturer or provider of the potentially vulnerable ICT products or ICT services in a manner allowing it to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure should also include coordination between the reporting natural or legal person and the manufacturer or provider of the potentially vulnerable ICT products or ICT services as regards the timing of remediation and publication of vulnerabilities.

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

(60) Member States, in cooperation with ENISA, should 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 national law. Given that natural and legal persons researching vulnerabilities could in some Member States be exposed to criminal and civil liability, Member States are encouraged to adopt guidelines as regards the non-prosecution of information security researchers and an exemption from civil liability for their activities.

(61) Member States should designate one of its CSIRTs as a coordinator, acting as a trusted intermediary between the reporting natural or legal persons and the manufacturers or providers of ICT products or ICT services, which are likely to be affected by the vulnerability, where necessary. The tasks of the CSIRT designated as coordinator should include identifying and contacting the entities concerned, assisting the natural or legal persons reporting a vulnerability, negotiating disclosure timelines and managing vulnerabilities that affect multiple entities (multi-party

coordinated vulnerability disclosure). Where the reported vulnerability could have significant impact on entities in more than one Member State, the CSIRTs designated as coordinators should cooperate within the CSIRTs network, where appropriate.

(62) Access to correct and timely information about vulnerabilities affecting ICT products and ICT services contributes to an enhanced cybersecurity risk management. Sources of publicly available information about vulnerabilities are an important tool for the entities and for the users of their services, but also for the competent authorities and the CSIRTs. For that reason, ENISA should establish a European vulnerability database where entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, as well as the competent authorities and the CSIRTs, can disclose and register, on a voluntary basis, publicly known vulnerabilities for the purpose of allowing users to take appropriate mitigating measures. The aim of that database is to address the unique challenges posed by risks to Union entities. Furthermore, ENISA should establish an appropriate 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 risk-management measures as well as machine-readable datasets and corresponding interfaces. To encourage a culture of disclosure of vulnerabilities, disclosure should have no detrimental effects on the reporting natural or legal person.

(63) Although similar vulnerability registries or databases exist, they 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 publicly disclosed, and resilience in the event of a disruption or an interruption of the provision of similar services. In order, to the extent possible, to avoid a duplication of efforts and to seek complementarity, ENISA should explore the possibility of entering into structured cooperation agreements with similar registries or databases that fall under third-country jurisdiction. In particular, ENISA should explore the possibility of close cooperation with the operators of the Common Vulnerabilities and Exposures (CVE) system.

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

(65) 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 an alignment of the transposition of this Directive among Member States, to be addressed through a 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 to sectors that have an international or cross-border nature.

(66) 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 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, offices and agencies involved in cybersecurity policy, such as the European Parliament, Europol, the European Data

Protection Board, the European Union Aviation Safety Agency, established by Regulation (EU) 2018/1139, and the European Union Agency for Space Programme, established by Regulation (EU) 2021/696 of the European Parliament and the Council ([14]), to participate in its work.

(67) The competent authorities and the CSIRTs should be able to participate in exchange schemes for officials from other Member States, within a specific framework and, where applicable, subject to 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 the host CSIRT.

(68) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework as set out in Commission Recommendation (EU) 2017/1584 ([15]) through the existing cooperation networks, in particular the European cyber crisis liaison organisation network (EU-CyCLONe), the CSIRTs network and the Cooperation Group. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements that specify the details of that cooperation and avoid any duplication of tasks. EU-CyCLONe's rules of procedure should further specify the arrangements through which that network should function, including the network's roles, means of cooperation, 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 EU Integrated Political Crisis Response arrangements under Council Implementing Decision (EU) 2018/1993 ([16]) (IPCR arrangements). The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for that purpose. If the crisis entails an important external or Common Security and Defence Policy dimension, the European External Action Service Crisis Response Mechanism should be activated.

(69) In accordance with the Annex to Recommendation (EU) 2017/1584, a large-scale cybersecurity incident should mean an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States. Depending on their cause and impact, large-scale cybersecurity 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 the relevant Union institutions, bodies, offices and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.

(70) 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 Member States. The availability of cyber-resilient network 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 citizens, businesses and institutions against incidents and cyber threats, as well as for enhancing the trust of individuals and organisations in the Union'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.

([14]) Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU (OJ L 170, 12.5.2021, p. 69).

([15]) 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).

([16]) Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements (OJ L 320, 17.12.2018, p. 28).

(71) 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, having regard to the Commission's competence in the area of crisis management, EU-CyCLONe should build on the CSIRTs network findings and use its own capabilities to create impact analysis of large-scale cybersecurity incidents and crises.

(72) Cyberattacks are of a cross-border nature, and a significant incident can disrupt and damage critical information infrastructures on which the smooth functioning of the internal market depends. Recommendation (EU) 2017/1584 addresses the role of all relevant actors. Furthermore, the Commission is responsible, within the framework of the Union Civil Protection Mechanism, established by Decision No 1313/2013/EU of the European Parliament and of the Council ([17]), for general preparedness actions including managing the Emergency Response Coordination Centre and the 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 IPCR arrangements under Implementing Decision (EU) 2018/1993, 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 emergencies, and energy.

(73) 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 particular activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements should ensure the Union's interests and the adequate protection of data. This should not preclude the right of Member States to cooperate with third countries on management of vulnerabilities and cybersecurity risk management, facilitating reporting and general information sharing in accordance with Union law.

(74) In order to facilitate the effective implementation of this Directive with regard, inter alia, to the management of vulnerabilities, cybersecurity risk-management measures, reporting obligations and cybersecurity information-sharing arrangements, Member States can cooperate with third countries and undertake activities that are considered to be appropriate for that purpose, including information exchange on cyber threats, incidents, vulnerabilities, tools and methods, tactics, techniques and procedures, cybersecurity crisis management preparedness and exercises, training, trust building and structured information-sharing arrangements.

(75) Peer reviews should be introduced to help learn from shared experiences, 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, peer reviews should take account of the results of similar mechanisms, such as the peer-review system of the CSIRTs network, and should add value and avoid duplication. The implementation of peer reviews should be without prejudice to Union or national law on the protection of confidential or classified information.

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

([17]) Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ L 347, 20.12.2013, p. 924).

(77) Responsibility for ensuring the security of network and information system lies, to a great extent, with essential and important entities. A culture of risk management, involving risk assessments and the implementation of cybersecurity risk-management measures appropriate to the risks faced, should be promoted and developed.

(78) Cybersecurity risk-management measures should take into account the degree of dependence of the essential or important 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 include the security of stored, transmitted and processed data. Cybersecurity risk-management measures should provide for systemic analysis, taking into account the human factor, in order to have a complete picture of the security of the network and information system.

(79) As threats to the security of network and information systems can have different origins, cybersecurity risk-management measures should be based on an all-hazards approach, which aims to protect network and information systems and the physical environment of those systems from events such as theft, fire, flood, telecommunication or power failures, or unauthorised physical access and damage to, and interference with, an essential or important entity's information and information processing facilities, which 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 cybersecurity risk-management measures should therefore also address the physical and environmental security of network and information systems by including measures to protect such systems from system failures, human error, malicious acts or natural phenomena, in line with European and international standards, such as those included in the ISO/IEC 27000 series. In that regard, essential and important entities should, as part of their cybersecurity risk-management measures, also address human resources security and have in place appropriate access control policies. Those measures should be consistent with Directive (EU) 2022/2557.

(80) For the purpose 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 of the European Parliament and of the Council ([18]), Member States should, in consultation with the Cooperation Group and the European Cybersecurity Certification Group, promote the use of relevant European and international standards by essential and important entities or may require entities to use certified ICT products, ICT services and ICT processes.

(81) In order to avoid imposing a disproportionate financial and administrative burden on essential and important entities, the cybersecurity risk-management measures should be proportionate to the risks posed to the network and information system concerned, taking into account the state-of-the-art of such measures, and, where applicable, relevant European and international standards, as well as the cost for their implementation.

(82) Cybersecurity risk-management measures should be proportionate to the degree of the essential or important entity's exposure to risks and to the societal and economic impact that an incident would have. When establishing 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, the risks, including societal risks, to which it is exposed, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

([18]) 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).

(83) Essential and important entities should ensure the security of the network and information systems which they use in their activities. Those systems are primarily private network and information systems managed by the essential and important entities' internal IT staff or the security of which has been outsourced. The cybersecurity risk-management measures and reporting obligations laid down in this Directive should apply to the relevant essential and important entities regardless of whether those entities maintain their network and information systems internally or outsource the maintenance thereof.

(84) Taking account of their cross-border nature, DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online marketplaces, of online search engines and of social networking services platforms, and trust service providers should be subject to a high degree of harmonisation at Union level. The implementation of cybersecurity risk-management measures with regard to those entities should therefore be facilitated by an implementing act.

(85) Addressing 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 service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers.

(86) Among service providers, managed security service providers 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. Managed security service providers have however also themselves been the target of cyberattacks and, because of their close integration in the operations of entities pose a particular risk. Essential and important entities should therefore exercise increased diligence in selecting a managed security service provider.

(87) The competent authorities, in the context of their supervisory tasks, may also benefit from cybersecurity services such as security audits, penetration testing or incident responses.

(88) Essential and important entities should also address risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem, including with regard to countering industrial espionage and protecting trade secrets. In particular, those 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 essential and important entities, when relying on data transformation and data analytics services from third parties, those entities should take all appropriate cybersecurity risk-management measures.

(89) Essential and important 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, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those 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 security of network and information systems.

(90) To further address key supply chain risks and assist essential and important entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related risks, the Cooperation Group, in cooperation with the Commission and ENISA, and where appropriate after consulting relevant stakeholders including from the industry, should carry out coordinated security risk assessments of critical supply chains, as carried out for 5G networks following Commission Recommendation (EU) 2019/534 ([19]), with the aim of identifying, per sector, the critical ICT services, ICT systems or ICT products, relevant threats and vulnerabilities. Such coordinated security risk assessments should identify measures, mitigation plans and best practices to counter 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 essential and important 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 the case of technological lock-in or provider dependency.

(91) The coordinated security risk assessments of critical supply chains, 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 coordinated risk assessment of the cybersecurity of 5G networks 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 security 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, ICT systems or ICT products; (ii) the relevance of specific critical ICT services, ICT systems or ICT products for performing critical or sensitive functions, including the processing of personal data; (iii) the availability of alternative ICT services, ICT systems or ICT products; (iv) the resilience of the overall supply chain of ICT services, ICT systems or ICT products throughout their lifecycle against disruptive events; and (v) for emerging ICT services, ICT systems or ICT products, their potential future significance for the entities' activities. Furthermore, particular emphasis should be placed on ICT services, ICT systems or ICT products that are subject to specific requirements stemming from third countries.

(92) In order to streamline the obligations imposed on providers of public electronic communications networks or of 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 the competent authorities under Directive (EU) 2018/1972 of the European Parliament and of the Council ([20]) and Regulation (EU) No 910/2014 respectively to benefit from the legal framework established by this Directive, including the designation of a CSIRT responsible for incident handling, the participation of the competent authorities concerned in the activities of the Cooperation Group and the CSIRTs network, those entities should fall within the scope of this Directive. The corresponding provisions laid down in Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 related to the imposition of security and notification requirements on those types of entity should therefore be deleted. The rules on reporting obligations laid down in this Directive should be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC.

(93) The cybersecurity obligations laid down in this Directive should be considered to be complementary to the requirements imposed on trust service providers under Regulation (EU) No 910/2014. Trust service providers should be required 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 incidents under this Directive. Such cybersecurity and reporting obligations should also concern the physical protection of the services provided. The requirements for qualified trust service providers laid down in Article 24 of Regulation (EU) No 910/2014 continue to apply.

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

([20]) 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).

(94) Member States can assign the role of the competent authorities for trust services to the supervisory bodies under Regulation (EU) No 910/2014 in order to ensure the continuation of current practices and to build on the knowledge and experience gained in the application of that Regulation. In such a case, the competent authorities under this Directive should cooperate closely and in a timely manner with those supervisory bodies by exchanging relevant information in order to ensure effective supervision and compliance of trust service providers with the requirements laid down in this Directive and in Regulation (EU) No 910/2014. Where applicable, the CSIRT or the competent authority under this Directive should immediately inform the supervisory body under Regulation (EU) No 910/2014 about any notified significant cyber threat or incident affecting trust services as well as about any infringements by a trust service provider of this Directive. For the purpose of reporting, Member States can, where applicable, use the single entry point established to achieve a common and automatic incident reporting to both the supervisory body under Regulation (EU) No 910/2014 and the CSIRT or the competent authority under this Directive.

(95) Where appropriate and in order 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 the transposition of this Directive, thereby building on the knowledge and skills already acquired under Directive (EU) 2018/1972 concerning security measures and incident notifications. ENISA can also develop guidance on security requirements and on reporting obligations for providers of public electronic communications networks or of publicly available electronic communications services to facilitate harmonisation and transition and to minimise disruption. Member States can assign the role of the competent authorities for electronic communications to the national regulatory authorities under Directive (EU) 2018/1972 in order to ensure the continuation of current practices and to build on the knowledge and experience gained as a result of the implementation of that Directive.

(96) Given the growing importance of number-independent interpersonal communications services as defined in Directive (EU) 2018/1972, it is necessary to ensure that such services are also subject to appropriate security requirements in view of their specific nature and economic importance. As the attack surface continues to expand, number-independent interpersonal communications services, such as messaging services, are becoming widespread attack vectors. Malicious perpetrators 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 network and information systems. Providers of number-independent interpersonal communications services should ensure a level of security of network and information systems appropriate to the risks 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 risks posed to such services can be considered in some respects to be lower than for traditional electronic communications services. The same applies to interpersonal communications services as defined in Directive (EU) 2018/1972 which make use of numbers and which do not exercise actual control over signal transmission.

(97) 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 communications networks have appropriate cybersecurity risk-management measures in place and report significant incidents in relation thereto. Member States should ensure that the security of the public electronic communications networks is maintained and that their vital security interests are protected from sabotage and espionage. Since international connectivity enhances and accelerates the competitive digitalisation of the Union and its economy, incidents affecting undersea communications cables should be reported to the CSIRT or, where applicable, the competent authority. The national cybersecurity strategy should, where relevant, take into account the cybersecurity of undersea communications cables and include a mapping of potential cybersecurity risks and mitigation measures to secure the highest level of their protection.

(98) In order to safeguard the security of public electronic communications networks and publicly available electronic communications 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, in particular end-to-end encryption should be mandatory for providers of public electronic communications networks or of publicly available electronic communications services in accordance with the principles of security and privacy by default and by design for the purposes of this Directive. The use of end-to-end encryption should be reconciled with the Member States' powers to ensure the protection of their essential security interests and public security, and to allow for the prevention, investigation, detection and prosecution of criminal offences in accordance with Union law. However, this should not weaken end-to-end encryption, which is a critical technology for the effective protection of data and privacy and the security of communications.

(99) In order to safeguard the security, and to prevent abuse and manipulation, of public electronic communications networks and of publicly available electronic communications 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.

(100) In order to safeguard the functionality and integrity of the internet and to promote the security and resilience of the DNS, relevant stakeholders including Union private-sector entities, providers of publicly available electronic communications 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.

(101) This Directive lays down a multiple-stage approach to the reporting of significant incidents in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of significant incidents and allows essential and important entities to seek assistance, and, on the other, in-depth reporting that draws valuable lessons from individual incidents and improves over time the cyber resilience of individual entities and entire sectors. In that regard, this Directive should include the reporting of incidents that, based on an initial assessment carried out by the entity concerned, could cause severe operational disruption of the services or financial loss for that entity or affect other natural or legal persons by causing considerable material or non-material damage. Such initial assessment should take into account, inter alia, the affected network and information systems, 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 identifying whether the operational disruption of the service is severe.

(102) Where essential or important entities become aware of a significant incident, they should be required to submit an early warning without undue delay and in any event within 24 hours. That early warning should be followed by an incident notification. The entities concerned should submit an incident notification without undue delay and in any event within 72 hours of becoming aware of the significant incident, with the aim, in particular, of updating information submitted through the early warning and indicating an initial assessment of the significant incident, including its severity and impact, as well as indicators of compromise, where available. A final report should be submitted not later than one month after the incident notification. The early warning should only include the information necessary to make the CSIRT, or where applicable the competent authority, aware of the significant incident and allow the entity concerned to seek assistance, if required. Such early warning, where applicable, should indicate whether the significant incident is suspected of being caused by unlawful or malicious acts, and whether it is likely to have a cross-border impact. Member States should ensure that the obligation to submit that early warning, or the subsequent incident notification, does not divert the notifying entity's resources from activities related to incident handling that should be prioritised, in order to prevent incident reporting obligations from either diverting resources from significant incident response handling or otherwise compromising the entity's efforts in that respect.

In the event of an ongoing incident at the time of the submission of the final report, Member States should ensure that entities concerned provide a progress report at that time, and a final report within one month of their handling of the significant incident.

(103) Where applicable, essential and important entities should communicate, without undue delay, to their service recipients any measures or remedies that they can take to mitigate the resulting risks from a significant cyber threat. Those entities should, where appropriate and in particular where the significant cyber threat is likely to materialise, also inform their service recipients of the threat itself. The requirement to inform those recipients of significant cyber threats should be met on a best efforts basis but should not discharge those entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any such threats and restore the normal security level of the service. The provision of such information about significant cyber threats to the service recipients should be free of charge and drafted in easily comprehensible language.

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

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

(106) In order to simplify the reporting of 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, regardless of whether they fall within the scope of this Directive, for the submission of the relevant information to be reported. Union funding supporting the implementation of this Directive, in particular within the Digital Europe programme, established by Regulation (EU) 2021/694 of the European Parliament and of the Council ([21]), could include support for single entry points. Furthermore, 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 administrative burden and could also lead to uncertainties with regard to the format and procedures of such notifications. Where a single entry point is established, Member States are encouraged also to use that single entry point 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 the independence of the authorities referred to therein. ENISA, in cooperation with the Cooperation Group, should develop common notification templates by means of guidelines to simplify and streamline the information to be reported under Union law and decrease the administrative burden on notifying entities.

(107) 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 accordance 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 the competent authorities and the law enforcement authorities of different Member States be facilitated by the European Cybercrime Centre (EC3) and ENISA.

([21]) Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).

(108) Personal data are in many cases compromised as a result of incidents. In that context, the competent authorities should cooperate and exchange information about all relevant matters with the authorities referred to in Regulation (EU) 2016/679 and Directive 2002/58/EC.

(109) Maintaining accurate and complete databases of domain name registration data (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 across the Union. For that specific purpose, TLD name registries and 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 the meaning of Article 6(1), point (c), of Regulation (EU) 2016/679. That obligation is without prejudice to the possibility to collect domain name registration data for other purposes, for example on the basis of contractual arrangements or legal requirements established in other Union or national law. That obligation aims to achieve a complete and accurate set of registration data and should not result in collecting the same data multiple times. The TLD name registries and the entities providing domain name registration services should cooperate with each other in order to avoid the duplication of that task.

(110) The availability and timely accessibility of domain name registration data to legitimate access seekers is essential for the prevention and combating of DNS abuse, and for the prevention and detection of and response to incidents. Legitimate access seekers are to be understood as any natural or legal person making a request pursuant to Union or national law. They can include authorities that are competent under this Directive and those that are competent under Union or national law for the prevention, investigation, detection or prosecution of criminal offences, and CERTs or CSIRTs. TLD name registries and entities providing domain name registration services should be required to enable lawful access to specific domain name registration data, which are necessary for the purposes of the access request, to legitimate access seekers in accordance with Union and national law. The request of legitimate access seekers should be accompanied by a statement of reasons permitting the assessment of the necessity of access to the data.

(111) In order to ensure the availability of accurate and complete domain name registration data, TLD name registries and entities providing domain name registration services should collect and guarantee the integrity and availability of domain name registration data. In particular, TLD name registries and entities providing domain name registration services should establish policies and procedures to collect and maintain accurate and complete domain name registration data, as well as to prevent and correct inaccurate registration data, in accordance with Union data protection law. Those 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 name registries and the entities providing domain name registration services should adopt and implement proportionate procedures to verify domain name registration data. Those procedures should reflect the best practices used within the industry and, to the extent possible, the progress made in the field of electronic identification. Examples of verification procedures may include *ex ante* controls carried out at the time of the registration and *ex post* controls carried out after the registration. The TLD name registries and the entities providing domain name registration services should, in particular, verify at least one means of contact of the registrant.

(112) TLD name registries and 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 law, such as data that concern legal persons, in line with the preamble of Regulation (EU) 2016/679. 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, such as in the case of email aliases or functional accounts. TLD name registries and 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 require TLD name registries and entities providing domain name registration services to respond without undue delay to requests for the disclosure of domain name registration data from legitimate access seekers. TLD name registries and entities providing domain name registration services should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. Those 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 could include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission can, without prejudice to the competences of the European Data Protection Board, provide guidelines with regard to such procedures, which take into account, to the extent possible, the standards developed by the multi-stakeholder governance structures at international level. Member States should ensure that all types of access to personal and non-personal domain name registration data are free of charge.

(113) Entities falling within the scope of this Directive should be considered to fall under the jurisdiction of the Member State in which they are established. However, providers of public electronic communications networks or providers of publicly available electronic communications services should be considered to fall under the jurisdiction of the Member State in which they provide their services. DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms should be considered to fall 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. 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 those Member States. The competent authorities of those 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 not impose enforcement measures or penalties more than once for the same conduct, in line with the principle of *ne bis in idem*.

(114) 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, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, only one Member State should have jurisdiction over those entities. Jurisdiction should be attributed to the Member State in which the entity concerned 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 that 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 considered to be in the Member State 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 entities' central administration in the Union. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment should be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment should be considered to be in the Member State where the entity has the 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.

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

(116) Where a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider or a provider of an online marketplace, of an online search engine or of a social networking services platform, which is not established in the Union, offers services within the Union, it should designate a representative in the Union. In order to determine whether such an entity is offering services within the Union, it should be ascertained whether 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 or other contact details, or the use of a language generally used in the third country where the entity is established, should be considered to be 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 language, or the mentioning of customers or users who are in the Union, could 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 the competent authorities or the CSIRTs to address 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 laid down in this Directive, including incident reporting.

(117) In order to ensure a clear overview of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, which provide services across the Union that fall within the scope of this Directive, ENISA should create and maintain a registry of such entities, based on the information received by Member States, where applicable through national mechanisms established for entities to register themselves. The single points of contact should forward to ENISA the information and any changes thereto. With a view to ensuring the accuracy and completeness of the information that is to be included in that registry, Member States can submit to ENISA the information available in any national registries on those 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.

(118) Where information which is classified in accordance with Union or national law is exchanged, reported or otherwise shared under this Directive, the corresponding 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 accordance with the applicable security rules for protecting EU classified information.

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

(120) Entities should be encouraged and assisted by Member States to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhancing their capabilities to adequately prevent, detect, respond to or recover from incidents or to mitigate their impact. It is thus necessary to enable the emergence at Union level of voluntary cybersecurity information-sharing arrangements. To that end, Member States should actively assist and encourage entities, such as those providing cybersecurity services and research, as well as relevant entities not falling within the scope of this Directive, to participate in such cybersecurity information-sharing arrangements. Those arrangements should be established in accordance with the Union competition rules and Union data protection law.

(121) The processing of personal data, to the extent necessary and proportionate for the purpose of ensuring security of network and information systems by essential and important entities, could be considered to be lawful on the basis that such processing complies with a legal obligation to which the controller is subject, in accordance with the requirements of Article 6(1), point (c), and Article 6(3) of Regulation (EU) 2016/679. Processing of personal data could 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 those entities, pursuant to Article 6(1), point (f), of Regulation (EU) 2016/679, including where such processing is necessary for cybersecurity information-sharing arrangements or the voluntary notification of relevant information in accordance with 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 vulnerability disclosure, the voluntary exchange of information about those incidents, and cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools could require the processing of certain categories of personal data, such as IP addresses, uniform resources locators (URLs), domain names, email addresses and, where they reveal personal data, time stamps. Processing of personal data by the competent authorities, the single points of contact and the CSIRTs, could constitute a legal obligation or be considered to be necessary for carrying out a task in the public interest or in the exercise of official authority vested in the controller 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), point (f), of that Regulation. Furthermore, national law could lay down rules allowing the competent authorities, the single points of contact and the CSIRTs, to the extent that is 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.

(122) In order to strengthen the supervisory powers and measures that help ensure effective compliance, this Directive should provide for a minimum list of supervisory measures and means through which the 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 on those entities and on the competent authorities. Therefore, essential entities should be subject to a comprehensive *ex ante* and *ex post* supervisory regime, while important entities should be subject to a light, *ex post* only, supervisory regime. Important entities should therefore not be required to systematically document compliance with cybersecurity risk-management measures, while the competent authorities should implement a reactive *ex post* approach to supervision and, hence, not have a general obligation to supervise those entities. The *ex post* supervision of important entities may be triggered by evidence, indication or information brought to the attention of the competent authorities considered by those authorities to suggest potential infringements of this Directive. For example, such evidence, indication or information could be of the type provided to the competent authorities by other authorities, entities, citizens, media or other sources or publicly available information, or could emerge from other activities conducted by the competent authorities in the fulfilment of their tasks.

(123) The execution of supervisory tasks by the competent authorities should not unnecessarily hamper the business activities of the entity concerned. Where the competent authorities execute their supervisory tasks in relation to essential entities, including the conduct of on-site inspections and off-site supervision, the investigation of infringements of this Directive and the conduct of security audits or security scans, they should minimise the impact on the business activities of the entity concerned.

(124) In the exercise of *ex ante* supervision, the competent authorities should be able to decide on the prioritisation of the use of supervisory measures and means at their disposal in a proportionate manner. This entails that the 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 measures and means recommended per risk category, such as the use, frequency or types of on-site inspections, targeted security audits or security scans, the type of information to be requested and the level of detail of that information. Such supervisory methodologies

could also be accompanied by work programmes and be assessed and reviewed on a regular basis, 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 legislative and institutional frameworks.

(125) The competent authorities should ensure that their supervisory tasks in relation to essential and important entities are carried out by trained professionals, who should have the necessary skills to carry out those tasks, in particular with regard to conducting on-site inspections and off-site supervision, including the identification of weaknesses in databases, hardware, firewalls, encryption and networks. Those inspections and that supervision should be conducted in an objective manner.

(126) In duly substantiated cases where it is aware of a significant cyber threat or an imminent risk, the competent authority should be able to take immediate enforcement decisions with the aim of preventing or responding to an incident.

(127) In order to make enforcement effective, a minimum list of enforcement powers that can be exercised for breach of the cybersecurity risk-management measures and reporting obligations provided for in this Directive should be laid down, setting up a clear and consistent framework for such enforcement across the Union. Due regard should be given to the nature, gravity and duration of the infringement of this Directive, the material or non-material damage caused, whether the infringement was intentional or negligent, actions taken to prevent or mitigate the material or non-material damage, 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 enforcement measures, 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 the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

(128) This Directive does not require Member States to provide for criminal or civil liability with regard to natural persons with responsibility for ensuring that an entity complies with this Directive for damage suffered by third parties as a result of an infringement of this Directive.

(129) 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.

(130) Where an administrative fine is imposed on an essential or important entity that is an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where an administrative fine is imposed on a person that is not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when 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 of the competent authorities or of other penalties laid down in the national rules transposing this Directive.

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

(132) Where this Directive does not harmonise administrative penalties or where necessary in other cases, for example in the event of a serious infringement of this Directive, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties and whether they are criminal or administrative should be determined by national law.

(133) In order to further strengthen the effectiveness and dissuasiveness of the enforcement measures applicable to infringements of this Directive, the competent authorities should be empowered to suspend temporarily or to request the temporary suspension of a certification or authorisation concerning part or all of the relevant services provided or activities carried out by an essential entity and request the imposition of a temporary prohibition of the exercise of managerial functions by any natural person discharging managerial responsibilities at chief executive officer or legal representative level. Given their severity and impact on the entities' activities and ultimately on users, such temporary suspensions or prohibitions should only be applied proportionally to the severity of the infringement and taking account of the circumstances of each individual case, including whether the infringement was intentional or negligent, and any actions taken to prevent or mitigate the material or non-material damage. Such temporary suspensions or prohibitions should only be applied as a last resort, namely only after the other relevant enforcement measures laid down in this Directive have been exhausted, and 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 temporary suspensions or prohibitions were applied. The imposition of such temporary suspensions or prohibitions should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence.

(134) For the purpose of ensuring entities' compliance with their obligations laid down in this Directive, Member States should cooperate with and assist each other with regard to supervisory and enforcement measures, in particular where an entity provides services in more than one Member State or where its network and information systems are located in a Member State other than that where it provides services. When providing assistance, the requested competent authority should take supervisory or enforcement measures in accordance with national law. In order to ensure the smooth functioning of mutual assistance under this Directive, the competent authorities should use the Cooperation Group as a forum to discuss cases and particular requests for assistance.

(135) In order to ensure effective supervision and enforcement, in particular in a situation with a cross-border dimension, a Member State that has received a request for mutual assistance should, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity that is the subject of that request, and that provides services or has a network and information system on the territory of that Member State.

(136) This Directive should establish cooperation rules between the competent authorities and the supervisory authorities under Regulation (EU) 2016/679 to deal with infringements of this Directive related to personal data.

(137) This Directive should aim to ensure a high level of responsibility for the cybersecurity risk-management measures and reporting obligations at the level of the essential and important entities. Therefore, the management bodies of the essential and important entities should approve the cybersecurity risk-management measures and oversee their implementation.

(138) In order to ensure a high common level of cybersecurity across 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 and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme. 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 Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([22]). 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.

([22]) OJ L 123, 12.5.2016, p. 1.

(139) 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 sectoral requirements concerning the cybersecurity risk-management measures, and 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 ([23]).

(140) The Commission should periodically review this Directive, after consulting stakeholders, in particular with a view to determining whether it is appropriate to propose amendments in light of changes to societal, political, technological or market conditions. As part of those reviews, the Commission should assess the relevance of the size of the entities concerned, and the sectors, subsectors and types of entity referred to in the annexes to this Directive for the functioning of the economy and society in relation to cybersecurity. The Commission should assess, inter alia, whether providers, falling within the scope of this Directive, that are designated as very large online platforms within the meaning of Article 33 of Regulation (EU) 2022/2065 of the European Parliament and of the Council ([24]) could be identified as essential entities under this Directive.

(141) 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 tasks, as well as to meet any higher level of execution of those 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 able to allocate resources internally for the purpose of effectively carrying out its tasks and meeting expectations.

(142) Since the objective of this Directive, namely to achieve a high common level of cybersecurity across 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.

(143) 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 and to a fair trial, the presumption of innocence and the rights of the defence. The right to an effective remedy extends to the recipients of services provided by essential and important entities. This Directive should be implemented in accordance with those rights and principles.

(144) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([25]) and delivered an opinion on 11 March 2021 ([26]),

---

([23]) 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).

([24]) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).

([25]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

([26]) OJ C 183, 11.5.2021, p. 3.

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

1. This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.

2. To that end, this Directive lays down:

(a) obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);

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

(c) rules and obligations on cybersecurity information sharing;

(d) supervisory and enforcement obligations on Member States.

Article 2

Scope

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

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

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

(a) services are provided by:

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

  (ii) trust service providers;

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

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

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

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

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

(f) the entity is a public administration entity:

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

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

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

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

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

(a) public administration entities at local level;

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

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

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

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

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

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

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

12. This Directive applies without prejudice to Regulation (EU) 2016/679, Directive 2002/58/EC, Directives 2011/93/EU ([27]) and 2013/40/EU ([28]) of the European Parliament and of the Council and Directive (EU) 2022/2557.

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

([27]) 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).

([28]) 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).

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

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

Article 3

Essential and important entities

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

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

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

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

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

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

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

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

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

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

4. For the purpose of establishing the list referred to in paragraph 3, Member States shall require the entities referred to in that paragraph to submit at least the following information to the competent authorities:

(a) the name of the entity;

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

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

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

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

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

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

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

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

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

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

Article 4

Sector-specific Union legal acts

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

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

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

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

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

Article 5

Minimum harmonisation

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

Article 6

Definitions

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

(1) 'network and information system' means:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(16) 'standard' means a standard as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council ([29]);

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

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

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

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

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

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

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

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

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

(23) 'digital service' means a service as defined in Article 1(1), point (b), of Directive (EU) 2015/1535 of the European Parliament and of the Council ([30]);

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

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

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

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

(28) 'online marketplace' means an online marketplace as defined in Article 2, point (n), of Directive 2005/29/EC of the European Parliament and of the Council ([31]);

(29) 'online search engine' means an online search engine as defined in Article 2, point (5), of Regulation (EU) 2019/1150 of the European Parliament and of the Council ([32]);

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

([30]) 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).

([31]) 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).

([32]) 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).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CHAPTER II

COORDINATED CYBERSECURITY FRAMEWORKS

Article 7

National cybersecurity strategy

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(j) promoting active cyber protection.

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

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

Article 8

Competent authorities and single points of contact

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

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

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

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

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

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

Article 9

National cyber crisis management frameworks

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

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

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

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

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

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

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

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

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

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

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

Article 10

Computer security incident response teams (CSIRTs)

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

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

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

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

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

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

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

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

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

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

Article 11

Requirements, technical capabilities and tasks of CSIRTs

1. The CSIRTs shall comply with the following requirements:

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

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

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

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

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

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

The CSIRTs may participate in international cooperation networks.

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

3. The CSIRTs shall have the following tasks:

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

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

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

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

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

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

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

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

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

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

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

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

(a) incident-handling procedures;

(b) crisis management; and

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

Article 12

Coordinated vulnerability disclosure and a European vulnerability database

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

(a) identifying and contacting the entities concerned;

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

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

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

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

(a) information describing the vulnerability;

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

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

Article 13

Cooperation at national level

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

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

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

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

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

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

CHAPTER III

COOPERATION AT UNION AND INTERNATIONAL LEVEL

Article 14

Cooperation Group

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

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

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

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

The Commission shall provide the secretariat.

4. The Cooperation Group shall have the following tasks:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 15

CSIRTs network

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

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

3. The CSIRTs network shall have the following tasks:

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

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

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

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

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

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

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

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

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

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

  (i) categories of cyber threats and incidents;

  (ii) early warnings;

  (iii) mutual assistance;

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

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

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

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

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

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

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

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

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

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

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

Article 16

European cyber crisis liaison organisation network (EU-CyCLONe)

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

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

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

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

3. EU-CyCLONe shall have the following tasks:

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

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

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

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

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

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

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

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

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

Article 17

International cooperation

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

Article 18

Report on the state of cybersecurity in the Union

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

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

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

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

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

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

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

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

Article 19

Peer reviews

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

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

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

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

(c) the operational capabilities of the CSIRTs;

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

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

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

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

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

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

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

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

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

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

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

CHAPTER IV

CYBERSECURITY RISK-MANAGEMENT MEASURES AND REPORTING OBLIGATIONS

Article 20

Governance

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

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

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

Article 21

Cybersecurity risk-management measures

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

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

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

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

(b) incident handling;

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

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

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

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

(g) basic cyber hygiene practices and cybersecurity training;

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

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

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

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

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

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

The Commission may adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph.

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

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

Article 22

Union level coordinated security risk assessments of critical supply chains

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

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

Article 23

Reporting obligations

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(iii) applied and ongoing mitigation measures;

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

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

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

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

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

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

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

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

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

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

By 17 October 2024, the Commission shall, with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, adopt implementing acts further specifying the cases in which an incident shall be considered to be significant as referred to in paragraph 3. The Commission may adopt such implementing acts with regard to other essential and important entities.

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

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

Article 24

Use of European cybersecurity certification schemes

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

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

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

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

Article 25

Standardisation

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

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

CHAPTER V

JURISDICTION AND REGISTRATION

Article 26

Jurisdiction and territoriality

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

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

(b) DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms, which shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2;

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

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

3. If an entity as referred to in paragraph 1, point (b), is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established. In the absence of a representative in the Union designated under this paragraph, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Directive.

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

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

Article 27

Registry of entities

1. ENISA shall create and maintain a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to that registry, while ensuring that the confidentiality of information is protected where applicable.

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

(a) the name of the entity;

(b) the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable;

(c) the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 26(3);

(d) up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative designated pursuant to Article 26(3);

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

(f) the entity's IP ranges.

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

4. Upon receipt of the information referred to in paragraphs 2 and 3, except for that referred to in paragraph 2, point (f), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.

5. Where applicable, the information referred to in paragraphs 2 and 3 of this Article shall be submitted through the national mechanism referred to in Article 3(4), fourth subparagraph.

Article 28

Database of domain name registration data

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

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

(a) the domain name;

(b) the date of registration;

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

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

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

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

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

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

CHAPTER VI

INFORMATION SHARING

Article 29

Cybersecurity information-sharing arrangements

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

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

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

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

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

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

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

Article 30

Voluntary notification of relevant information

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

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

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

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

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

CHAPTER VII

SUPERVISION AND ENFORCEMENT

Article 31

General aspects concerning supervision and enforcement

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

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

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

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

Article 32

Supervisory and enforcement measures in relation to essential entities

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  (i) repeated violations;

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

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

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

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

(b) the duration of the infringement;

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

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

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

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

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

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

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

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

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

Article 33

Supervisory and enforcement measures in relation to important entities

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 34

General conditions for imposing administrative fines on essential and important entities

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

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

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

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

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

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

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

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

Article 35

Infringements entailing a personal data breach

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

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

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

Article 36

Penalties

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

Article 37

Mutual assistance

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

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

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

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

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

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

CHAPTER VIII

DELEGATED AND IMPLEMENTING ACTS

Article 38

Exercise of the delegation

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

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

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

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

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

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

Article 39

Committee procedure

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

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

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

CHAPTER IX

FINAL PROVISIONS

Article 40

Review

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

Article 41

Transposition

1. By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof.

They shall apply those measures from 18 October 2024.

2. When Member States adopt the measures referred to in paragraph 1, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

Article 42

Amendment of Regulation (EU) No 910/2014

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

Article 43

Amendment of Directive (EU) 2018/1972

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

Article 44

Repeal

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

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

Article 45

Entry into force

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

Article 46

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 14 December 2022.

For the European Parliament	*For the Council*
The President	*The President*
R. METSOLA	M. BEK

ANNEX I

SECTORS OF HIGH CRITICALITY

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

Sector	Subsector	Type of entity
2. Transport	(a) Air	— Air carriers as defined in Article 3, point (4), of Regulation (EC) No 300/2008 used for commercial purposes
		— Airport managing bodies as defined in Article 2, point (2), of Directive 2009/12/EC of the European Parliament and of the Council ([6]), airports as defined in Article 2, point (1), of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council ([7]), and entities operating ancillary installations contained within airports
		— Traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of Regulation (EC) No 549/2004 of the European Parliament and of the Council ([8])
	(b) Rail	— Infrastructure managers as defined in Article 3, point (2), of Directive 2012/34/EU of the European Parliament and of the Council ([9])
		— Railway undertakings as defined in Article 3, point (1), of Directive 2012/34/EU, including operators of service facilities as defined in Article 3, point (12), of that Directive
	(c) Water	— Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council ([10]), not including the individual vessels operated by those companies
		— Managing bodies of ports as defined in Article 3, point (1), of Directive 2005/65/EC of the European Parliament and of the Council ([11]), including their port facilities as defined in Article 2, point (11), of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		— Operators of vessel traffic services (VTS) as defined in Article 3, point (o), of Directive 2002/59/EC of the European Parliament and of the Council ([12])
	(d) Road	— Road authorities as defined in Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962 ([13]) responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity
		— Operators of Intelligent Transport Systems as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council ([14])
3. Banking		Credit institutions as defined in Article 4, point (1), of Regulation (EU) No 575/2013 of the European Parliament and of the Council ([15])
4. Financial market infrastructures		— Operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU of the European Parliament and of the Council ([16])
		— Central counterparties (CCPs) as defined in Article 2, point (1), of Regulation (EU) No 648/2012 of the European Parliament and of the Council ([17])

Sector	Subsector	Type of entity
5. Health		— Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council ([18])
		— EU reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council ([19])
		— Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council ([20]) — Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 — Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list) within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council ([21])
6. Drinking water		Suppliers and distributors of water intended for human consumption as defined in Article 2, point (1)(a), of Directive (EU) 2020/2184 of the European Parliament and of the Council ([22]), excluding distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods
7. Waste water		Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2, points (1), (2) and (3), of Council Directive 91/271/EEC ([23]), excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity
8. Digital infrastructure		— Internet Exchange Point providers
		— DNS service providers, excluding operators of root name servers
		— TLD name registries
		— Cloud computing service providers
		— Data centre service providers
		— Content delivery network providers
		— Trust service providers
		— Providers of public electronic communications networks
		— Providers of publicly available electronic communications services
9. ICT service management (business-to-business)		— Managed service providers — Managed security service providers

Sector	Subsector	Type of entity
10. Public administration		— Public administration entities of central governments as defined by a Member State in accordance with national law
		— Public administration entities at regional level as defined by a Member State in accordance with national law
11. Space		Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

(1) Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125).
(2) Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (OJ L 158, 14.6.2019, p. 54).
(3) Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources (OJ L 328, 21.12.2018, p. 82).
(4) Council Directive 2009/119/EC of 14 September 2009 imposing an obligation on Member States to maintain minimum stocks of crude oil and/or petroleum products (OJ L 265, 9.10.2009, p. 9).
(5) Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).
(6) Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).
(7) Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).
(8) Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p. 1).
(9) Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p. 32).
(10) Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).
(11) Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).
(12) Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).
(13) Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21).
(14) Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).
(15) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).
(16) Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).
(17) Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).
(18) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(19) Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU (OJ L 314, 6.12.2022, p. 26).
(20) Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 67).
(21) Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.1.2022, p. 1).
(22) Directive (EU) 2020/2184 of the European Parliament and of the Council of 16 December 2020 on the quality of water intended for human consumption (OJ L 435, 23.12.2020, p. 1).
(23) Council Directive 91/271/EEC of 21 May 1991 concerning urban waste water treatment (OJ L 135, 30.5.1991, p. 40).

ANNEX II

OTHER CRITICAL SECTORS

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

Sector	Subsector	Type of entity
6. Digital providers		— Providers of online marketplaces
		— Providers of online search engines
		— Providers of social networking services platforms
7. Research		Research organisations

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

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

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

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

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

ANNEX III

CORRELATION TABLE

Directive (EU) 2016/1148	This Directive
Article 1(1)	Article 1(1)
Article 1(2)	Article 1(2)
Article 1(3)	-
Article 1(4)	Article 2(12)
Article 1(5)	Article 2(13)
Article 1(6)	Article 2(6) and (11)
Article 1(7)	Article 4
Article 2	Article 2(14)
Article 3	Article 5
Article 4	Article 6
Article 5	–
Article 6	–
Article 7(1)	Article 7(1) and (2)
Article 7(2)	Article 7(4)
Article 7(3)	Article 7(3)
Article 8(1) to (5)	Article 8(1) to (5)
Article 8(6)	Article 13(4)
Article 8(7)	Article 8(6)
Article 9(1), (2) and (3)	Article 10(1), (2) and (3)
Article 9(4)	Article 10(9)
Article 9(5)	Article 10(10)
Article 10(1), (2) and (3), first subparagraph	Article 13(1), (2) and (3)
Article 10(3), second subparagraph	Article 23(9)
Article 11(1)	Article 14(1) and (2)
Article 11(2)	Article 14(3)
Article 11(3)	Article 14(4), first subparagraph, points (a) to (q) and (s), and paragraph (7)
Article 11(4)	Article 14(4), first subparagraph, point (r), and second subparagraph
Article 11(5)	Article 14(8)
Article 12(1) to (5)	Article 15(1) to (5)
Article 13	Article 17
Article 14(1) and (2)	Article 21(1) to (4)
Article 14(3)	Article 23(1)
Article 14(4)	Article 23(3)
Article 14(5)	Article 23(5), (6) and (8)

Directive (EU) 2016/1148	This Directive
Article 14(6)	Article 23(7)
Article 14(7)	Article 23(11)
Article 15(1)	Article 31(1)
Article 15(2), first subparagraph, point (a)	Article 32(2), point (e)
Article 15(2), first subparagraph, point (b)	Article 32(2), point (g)
Article 15(2), second subparagraph	Article 32(3)
Article 15(3)	Article 32(4), point (b)
Article 15(4)	Article 31(3)
Article 16(1) and (2)	Article 21(1) to (4)
Article 16(3)	Article 23(1)
Article 16(4)	Article 23(3)
Article 16(5)	–
Article 16(6)	Article 23(6)
Article 16(7)	Article 23(7)
Article 16(8) and (9)	Article 21(5) and Article 23(11)
Article 16(10)	–
Article 16(11)	Article 2(1), (2) and (3)
Article 17(1)	Article 33(1)
Article 17(2), point (a)	Article 32(2), point (e)
Article 17(2), point (b)	Article 32(4), point (b)
Article 17(3)	Article 37(1), points (a) and (b)
Article 18(1)	Article 26(1), point (b), and paragraph (2)
Article 18(2)	Article 26(3)
Article 18(3)	Article 26(4)
Article 19	Article 25
Article 20	Article 30
Article 21	Article 36
Article 22	Article 39
Article 23	Article 40
Article 24	–
Article 25	Article 41
Article 26	Article 45
Article 27	Article 46
Annex I, point (1)	Article 11(1)
Annex I, points (2)(a)(i) to (iv)	Article 11(2), points (a) to (d)

Directive (EU) 2016/1148	This Directive
Annex I, point (2)(a)(v)	Article 11(2), point (f)
Annex I, point (2)(b)	Article 11(4)
Annex I, points (2)(c)(i) and (ii)	Article 11(5), point (a)
Annex II	Annex I
Annex III, points (1) and (2)	Annex II, point (6)
Annex III, point (3)	Annex I, point (8)