



Council of the
European Union

Brussels, 10 February 2016
(OR. en)

5894/16

**Interinstitutional File:
2013/0027 (COD)**

**TELECOM 14
DATAPROTECT 10
CYBER 10
MI 65
CSC 24
CODEC 134**

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
No. Cion doc.:	6342/13 TELECOM 24 DATAPRTOECT 14 CYBER 2 MI 104 CODEC 313
Subject:	Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - Political agreement

With a view to the adoption of a political agreement, delegations will find in Annex the text of the above proposal, which was agreed in substance at the informal trilogue of 7 December 2015. It was subsequently endorsed by the Permanent Representatives Committee¹ and by the Internal Market and Consumer Protection (IMCO) Committee of the European Parliament, on 18 December 2015 on 14 January 2016 respectively.

¹ Doc. 15229/2/15 REV 2.

In order to comply with formal requirements for the Council documents, lawyers-linguists of the Council and of the European Parliament made some initial technical adjustments to the compromise text, without however changing in any way the substance. Those technical modifications consist in arranging the recitals in a standard order, editing the references to the EU legal acts according to the Joint Practical Guide for drafting of EU legislation and minor consistency check of the use of abbreviations throughout the text. The modifications are of course without prejudice to further legal/linguistic revision that will start after the confirmation of the political agreement by the Council.

DIRECTIVE (EU) 2016/... OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**of ...****concerning measures for a high common level of security of network and information systems
across the Union**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee²,Acting in accordance with the ordinary legislative procedure³,

Whereas:

² OJ C [...], [...], p. [...].

³ Position of the European Parliament of ... [(OJ ...)/(not yet published in the Official Journal)] and position of the Council at first reading of ... [(OJ ...)/(not yet published in the Official Journal)]. Position of the European Parliament of ... [(OJ ...)/(not yet published in the Official Journal)].

- (1) Network and information systems and services play a vital role in the society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.
- (2) The magnitude, frequency and impact of security incidents is increasing and represents a major threat to the functioning of networks and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.
- (3) Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Due to that transnational nature, substantial disruption of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential to the smooth functioning of the internal market.
- (4) Building upon the significant progress within the European Forum of Member States ('EFMS') in fostering discussions and exchanges on good policy practices including the development of principles for European cyber crisis cooperation, a cooperation group should be established composed of Member States' representatives, the Commission and the European Union Agency for Network and Information Security ('ENISA') to support and facilitate strategic cooperation between the Member States regarding network and information security ('NIS'). For that group to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of NIS in their territory. In addition, security and incident notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported.

- (5) The existing capabilities are not sufficient to ensure a high level of NIS within the Union. Member States have very different levels of preparedness leading to fragmented approaches across the Union. This leads to an unequal level of protection of consumers and businesses, and undermines the overall level of NIS within the Union. Lack of common requirements on operators of essential services and digital service providers in turn makes it impossible to set up a global and effective mechanism for cooperation at Union level. Universities and research centres have a decisive role in spurring research, development and innovation in those areas.
- (6) Responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information, cooperation and common security requirements for operators of essential services and digital service providers.
- (6a) Operators of essential services and digital service providers are not precluded from implementing stricter security measures than provided for under this Directive.
- (7) To cover all relevant incidents and risks, this Directive should apply to both operators of essential services and digital service providers. The obligations on operators of essential services and digital service providers should however not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002⁴, which are subject to the specific security and integrity requirements laid down in Article 13a of that Directive nor should they apply to trust service providers within the meaning of Regulation (EU) No 910/2014 of the European Parliament and of the Council⁵, which are subject to the requirements laid down in Article 19 of that Regulation.

⁴ Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24.4.2002, p. 33).

⁵ 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).

- (8) The provisions of this Directive should be without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of its essential security interests, to safeguard public policy and public security, and to permit the investigation, detection and prosecution of criminal offences. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security. In this context, Council Decision 2011/292/EU⁶, non-disclosure agreements or informal non-disclosure agreements, such as the Traffic Light Protocol, are of relevance.
- (9) Certain sectors of the economy are already regulated or may be regulated in the future by sector-specific Union legal acts that include rules related to the security of networks and information systems. Whenever those Union legal acts contain provisions imposing requirements concerning the security of networks and information systems or notifications of incidents, these provisions should apply instead of the corresponding provisions of this Directive if they contain requirements which are at least equivalent in effect to the obligations contained in this Directive.
- (10) Member States should then apply the provisions of such sector-specific Union legal act, including those relating to jurisdiction, and should not carry out the identification process for operators of essential services as defined by this Directive. In this context, Member States should provide information to the Commission on the application of the provision on *lex specialis*.
- (11) In determining whether the requirements on the security of networks and information systems and/or the notification of incidents contained in sector specific Union legal acts are equivalent to those contained in Articles 14 and 15a of this Directive, regard should only be had to the provisions of relevant Union legal acts and their application in the Member States.

⁶ Council Decision 2011/292/EU of 31 March 2011 on the security rules for protecting EU classified information (OJ L 141, 27.5.2011, p. 17)

- (12) Entities falling outside the scope of this Directive, may experience incidents having a significant impact on the services they provide. Where those entities consider that it is in the public interest to notify the relevant authorities of Member States of the occurrence of such incidents, they should be able to do so on a voluntary basis. Such notifications should be processed by those bodies where such processing does not constitute a disproportionate or undue burden on the Member States concerned.
- (13) An online marketplace should allow consumers and/or traders to conclude online sales and service contracts with traders, and should be the final destination for the conclusion of those contracts. It should not cover online services that serve only as an intermediary to third-party services where a contract can ultimately be concluded. It should therefore not cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product. Computing services provided by the online marketplace may include processing of transactions, aggregations of data or profiling of users. Application stores, which operate as online stores enabling the digital distribution of applications or software programmes from third parties, ~~is~~ are to be understood as being a type of online marketplace.
- (14) An online search engine should allow the user to perform searches of in principle all websites on the basis of a query on any subject. It may alternatively be focused on websites in a particular language. The definition of an online search engine provided in this Directive should not cover search functions that are limited to the content of a specific website, irrespective of whether the search function is provided by an external search engine. It should also not cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product.

- (15) Cloud computing services span a wide range of activities that can be delivered according to different models. For the purposes of this Directive, "cloud computing services" means services that enable access to a scalable and elastic pool of shareable computing resources. The term "computing resources" covers resources such as networks, servers or other infrastructure, storage, applications and services. "Scalable" means that, in order to handle fluctuations in demand, computing resources are flexibly allocated by the cloud service provider irrespective of the geographical location of the resources. "Elastic pool" means that these computing resources, in order to rapidly increase and decrease resources available in accordance with workload, are provisioned and released according to demand. "Shareable" means that these computing resources 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.
- (16) The function of an Internet Exchange Point (IXP) is to interconnect networks. An IXP does not provide network access or act as a transit provider or carrier. An IXP also does not provide other services unrelated to interconnection (although this does not preclude an IXP operator from also providing unrelated services). An IXP exists to interconnect networks that are technically and organisationally separate. The term autonomous system is used to describe a technically stand-alone network.

- (17) Member States should be responsible for determining which entities meet the criteria of the definition of operator of essential services as part of the transposition- of the Directive into national law. In order to ensure a consistent approach, the definition of operator of essential services should be coherently applied by all Member States. For this purpose the Directive provides for the assessment of the entities active in the subsectors, or in the sector where no subsector is listed in Annex II, the establishment of a list of essential services, the consideration of a common list of cross-sectoral factors to determine whether a potential incident would have a significant disruptive effect, a consultation process involving relevant Member States in case of entities providing services in more than one Member State, and the support of the Cooperation Group in the identification process. In order to ensure that possible changes in the market are accurately reflected, the list of identified operators should be reviewed regularly by Member States and updated when necessary. Finally Member States should submit to the Commission the information necessary to assess the extent to which this common methodology allowed a consistent application of the definition by Member States.
- (18) In the process of identification of operators of essential services, Member States should assess, at least for each subsector referred to in this Directive, which services have to be considered as essential for the maintenance of critical societal and economic activities and assess whether the entities listed in the sectors and subsectors in this Directive and providing those services meet the criteria for the identification of operators. When assessing whether an entity provides a service which is essential for the maintenance of critical societal or economic activities, it is sufficient to examine whether a specific entity provides an essential service that is included in the list of services. Furthermore, it should be demonstrated that provision of the essential service is dependent on network and information systems. Finally, when assessing whether an incident to the network and information systems of the service would have significant disruptive effect on its provision, Member States should take into account a number of cross-sectoral factors. They should also take into account sector-specific factors where appropriate.

- (19) For the purposes of identifying operators of essential services, establishment implies the effective and real 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 this respect.
- (20) Entities in the sectors and subsectors listed in Annex II may provide essential and non-essential services. For example, in the air transport sector, airports may provide services, which might be considered by a Member State as essential, such as the management of the runways, but also a number of services which might be considered as non-essential, such as the provision of shopping areas. Operators of essential services should be subject to the specific security obligations only with respect to those services which are deemed essential. For the purpose of identifying operators, Member States should therefore establish a list of the services which are considered as essential.
- (21) The list of services should serve as a reference point for the competent national authorities allowing for identification of operators of essential services. Its purpose is to identify the types of essential services in any given sector listed in Annex II, thus distinguishing them from non-essential activities that an entity active in any given sector may be responsible for. The list of services should contain all services provided in the territory of the Member State that fulfil the requirements under this Directive. The Member State should be able to include new services to the existing list if such emerge in the future. The list of services established by each Member State would serve as further input in the assessment of the regulatory practice of each Member State with a view to ensuring the overall level of consistency of the identification process amongst Member States.

- (22) For the purposes of the identification process, where a potential operator provides the essential service in two or more Member States, those Member States should engage in bilateral or multilateral discussions with each other. This consultation process is intended to help Member States to assess the criticality of the operator in terms of cross-border impact and allows each Member State involved to present its views regarding the risks associated to the services provided by the operator. In this process Member States concerned should take into account each other's views. The Member States concerned may request the assistance of the Cooperation Group in this regard.
- (23) As a result of the identification process Member States should adopt national measures which will determine which entities are subject to NIS obligations. This result could be achieved by adopting a list enumerating all operators of essential services or by adopting national measures including objective quantifiable criteria (e.g. output of the operator or number of users) which would allow to determine which entities are subject to NIS obligations and which are not. The national measures should include all legal measures, administrative measures and policies allowing for the identification of operators of essential services under this Directive, whether already existing or adopted in the context of this Directive.
- (24) In order to give an indication of the importance of the identified operators in relation to the sector concerned, Member States should take into account the number and the size of identified operators, for example in terms of market share or of the quantity produced or carried, without being obliged to divulge information which would reveal which operators have been identified.
- (25) For the purpose of determining the significance of a disruptive effect of an incident on an essential service, Member States should take into account the number of natural persons and legal entities using that service for private or professional purposes. The use of that service can be direct, indirect or by intermediation.

- (26) In order to determine whether an incident would have a significant disruptive effect on the provision of a service, Member States should take into account a number of different factors. When assessing the impact an incident could have, in terms of its degree and duration, on economic and societal activities or public safety, Member States should also assess the time likely to elapse before the discontinuity would start to have a negative impact.
- (27) In order to determine whether an incident would have a significant disruptive effect on the provision of a service, in addition to the cross-sectorial factors, sector specific factors should also be considered. With regard to energy suppliers such factors could include the volume or proportion of national power generated; for oil suppliers the volume per day; for air transport (including airports and air carriers), rail transport and maritime ports the proportion of national traffic volume and the number of passengers or cargo operations per year; for banking/financial market infrastructures their systemic importance based on total assets or the ratio of those total assets to GDP; for health, the number of patients under the provider's care per year; for water production, processing and supply the volume and number and types of users supplied (including for instance hospitals, public service, organisations or individuals), and the existence of alternative sources of water to cover the same geographical area.
- (28) To achieve and maintain a common high level of security of network and information systems, each Member State should have a national NIS strategy defining the strategic objectives and concrete policy actions to be implemented.

- (29) To allow for the effective implementation of the provisions adopted pursuant to this Directive, a body responsible for coordinating NIS issues and acting as a single point of contact for cross-border cooperation at Union level should be established or identified in each Member State. The competent authorities and the single point of contact should be given the adequate technical, financial and human resources to ensure that they can carry out in an effective and efficient manner the tasks assigned to them and thus achieve the objectives of this Directive. As this Directive aims at improving the functioning of the internal market by creating trust and confidence, Member State bodies need to be able to cooperate effectively with economic actors and to be structured accordingly.
- (30) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, and to avoid duplication, Member States should be able to designate more than one national competent authority responsible for fulfilling the tasks linked to the security of the networks and information systems of operators of essential services and digital service providers under this Directive. However, in order to facilitate cross-border cooperation and communication, it is necessary for each Member State, without prejudice to sectoral regulatory arrangements, to designate a national single point of contact in charge of cross-border cooperation at Union level.
- (31) Competent authorities or the Computer Security Incident Response Teams ('CSIRTs') should receive the notifications of incidents. The single points of contact should not receive directly any notifications of incidents unless they also act as a competent authority or CSIRT. A competent authority or CSIRT might however task the single point of contact to forward incident notifications to the single points of contact of other affected Member States.

- (32) The summary report submitted by the single point of contact to the cooperation group should be anonymised in order to preserve the confidentiality of the notifications and the identity of operators of essential services and digital service providers as information on the identity of the notifying entities is not required for the exchange of best practices in the cooperation group. The summary report should include information on the number of notifications received, as well as an indication on the nature of the notified incidents, such as the types of security breaches, their seriousness or their duration.
- (33) All Member States should be adequately equipped, both in terms of technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information systems' incidents and risks. All Member States should therefore ensure they have well-functioning CSIRTs, also known as Computer Emergency Response Teams ("CERTs"), complying with essential requirements to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level. In order for all types of operators of essential services and digital service providers to benefit from such capabilities and cooperation, Member States should ensure that all types are covered by a designated CSIRT. Given the importance of international cooperation on cybersecurity, CSIRTs should have the possibility to participate in international cooperation networks in addition to the CSIRTs network established by this Directive.
- (34) As most network and information systems are privately operated, cooperation between the public and private sector is essential. Operators of essential services and digital service providers should be encouraged to pursue their own informal cooperation mechanisms to ensure NIS. The cooperation group should be able to invite relevant stakeholders to the discussions where appropriate. To effectively encourage the sharing of information and of best practices, it is essential to ensure that operators of essential services and digital service providers who participate in such exchanges are not disadvantaged as a result of their cooperation.

- (35) ENISA should assist the Member States and the Commission by providing its expertise and advice and by facilitating exchange of best practices. In particular, in the application of this Directive, the Commission should and Member States could consult ENISA. To ensure effective information to the Member States and the Commission, a summary report on notification should be submitted to the cooperation group. To build capacity and knowledge among Member States, the cooperation group should also serve as an instrument for the exchange of best practices, discussion of capabilities and preparedness of the Member States and on a voluntary basis assisting its members in evaluating national NIS strategies, building capacity and NIS exercises.
- (36) Where appropriate, Member States should be able to use or adapt existing organisational structures or strategies when applying the provisions of this Directive.
- (37) The respective tasks of the Cooperation Group and ENISA are interdependent and complementary. In general, ENISA should assist the Cooperation Group established under Article 8a in the execution of its tasks, in line with the objective of ENISA set out in Article 2 of Regulation (EU) No 526/2013 of the European Parliament and the Council⁷ to "[...] assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union [...]". In particular, ENISA should provide assistance in those areas that correspond to its own tasks, as set out in Article 3 of Regulation 526/2013, i.e. analysing NIS strategies, supporting the organisation and running of Union NIS exercises, and exchanging information and best practice on awareness-raising and training. ENISA should also be involved in the development of guidelines for sector-specific criteria for determining the significance of the impact of an incident.

⁷ Regulation (EU) No 526/2013 of the European Parliament and the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (OJ L 165, 18.6.2013, p. 41).

- (38) In order to promote advanced network and information security, the cooperation group should, where appropriate, cooperate with relevant Union institutions, bodies, offices and agencies, to exchange know-how and best practices and to provide advice on NIS aspects that might have an impact on their work, while respecting existing arrangements for the exchange of restricted information. In cooperating with law enforcement bodies regarding network and information security aspects that might have an impact on their work, the cooperation group should respect existing channels of information and established networks.
- (39) Information about NIS incidents is increasingly valuable to the general public and businesses, particularly small and medium-sized businesses. In some cases, such information is already provided via websites at the national level, in the language of a specific country and focusing mainly on incidents and occurrences with a national dimension. Given that businesses increasingly operate cross-border and citizens use online services, information on incidents should be provided in an aggregated form at EU level. The secretariat of the CSIRT network is encouraged to maintain a website or host a dedicated page on an existing website where general information on major NIS incidents occurring across the Union is put at the disposal of the general public, with a specific focus on the interests and needs of businesses. CSIRTs participating in the CSIRTs network are encouraged to provide on a voluntary basis the information to be published in this website. Such a website is not supposed to include confidential or sensitive information.
- (40) Where information is considered confidential in accordance with Union and national rules on business confidentiality, such confidentiality should be ensured when carrying out the activities and fulfilling the objectives set by this Directive.

- (41) Cybersecurity exercises, which simulate real time incident scenarios, are essential for testing Member States' preparedness and cooperation. The CyberEurope cycle of exercises coordinated by ENISA with the participation of the Member States is a useful tool for testing and drawing up recommendations on how incident response at EU level should improve over time. Considering that, at present, the Member States are not under an obligation to either plan or participate in exercises, the creation of the CSIRTs network under this Directive should enable the Member States to participate in exercises on the basis of accurate planning and strategic choices. The Cooperation group set up under this Directive should deal with the strategic decisions regarding exercises, in particular but not exclusively as regards the regularity of the exercises and the design of the scenarios. ENISA should, in accordance with its mandate support the organisation and running of Union-wide exercises by providing its expertise and advice to the Cooperation Group and the CSIRTs network.
- (42) Given the global nature of NIS problems, there is a need for closer international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues.
- (43) Responsibilities in ensuring NIS lie to a great extent on operators of essential services and digital service providers. A culture of risk management-involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed through appropriate regulatory requirements and voluntary industry practices. Establishing a trustworthy level playing field is also essential to the effective functioning of the cooperation group and CSIRTs network to ensure effective cooperation from all Member States.
- (44) This Directive only applies to public administrations of the type listed in Annex II and identified as operators of essential services. It is the responsibility of Member States to ensure the security of network and information systems of public administrations not falling within the scope of this Directive.

- (45) Measures to manage the risk include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact; the security of network and information systems comprises the security of stored, transmitted and processed data.
- (46) Competent authorities should retain the ability to adopt national guidelines concerning the circumstances in which operators of essential services are required to notify incidents.
- (47) Many EU businesses rely on digital service providers as defined in this Directive for the provision of their own services. As some digital services can be an important resource for their users, including operators of essential services, and as such users may not always have alternatives available, this Directive should also apply to providers of such services. The security, continuity and reliability of the type of services referred to in Annex III is of the essence for the smooth functioning of many businesses. A disruption of a digital service as listed in Annex III could prevent the provision of other services which rely on it and could thus have an impact on key economic and societal activities in the Union. Such digital services may therefore be of crucial importance for the smooth functioning of businesses that depend on them and moreover for the participation of such businesses in the internal market and cross-border trade across the Union. The digital service providers included in this Directive are those considered to offer digital services on which many EU businesses increasingly rely.

- (48) Digital service providers should ensure a level of security commensurate to the degree of risk posed to the security of the services they provide, given the importance of their services to the operations of other businesses within the EU. In practice the degree of risk for operators of essential services, which are often essential for the maintenance of critical societal and economic activities, will be higher than for digital service providers. Therefore the security requirements for digital service providers should be lighter. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their networks and information systems. Because of their cross-border nature, digital service providers should be subject to a more harmonised approach at the European level. Implementing acts should facilitate the specification and implementation of such measures.
- (49) While hardware manufacturers and software developers are not operators of essential services or digital service providers comparable to those covered in this Directive, their products facilitate the security of network and information systems. They therefore have an important role in enabling operators of essential services and digital service providers to secure their network and information infrastructures. Such hardware and software products are already subject to existing rules on product liability.
- (50) Technical and organisational measures imposed on operators of essential services and digital service providers should not require that a particular commercial information and communications technology product be designed, developed or manufactured in a particular manner.

- (51) The operators of essential services and digital service providers should ensure security of the networks and systems which they use. These would be primarily private networks and systems managed either by their internal IT staff or the security of which has been outsourced. The security and notification obligations should apply to the relevant operators of essential services and digital service providers regardless of whether they perform the maintenance of their network and information systems internally or outsource it.
- (52) To avoid imposing a disproportionate financial and administrative burden on operators of essential services and digital service providers, the requirements should be proportionate to the risk presented by the network or information system concerned, taking into account the state of the art of such measures. In the case of digital service providers, these requirements should not apply to micro enterprises and small enterprises.
- (53) Where public administrations in Member States use services offered by digital service providers, in particular cloud computing services, they may wish to require additional security measures from the providers of such services beyond what digital service providers would normally offer in compliance with the requirements of this Directive. They may do so by means of contractual obligations.
- (54) The definitions of online marketplaces, online search engines and cloud computing services in this Directive are for the specific purpose of this Directive, and without prejudice to any other instruments.
- (55) This Directive should not prevent Member States from adopting national measures obliging public sector bodies to ensure specific security requirements when they contract cloud computing services. Any such national measures should apply to the public sector body (the client) and not to the cloud computing service provider.

- (56) Given the fundamental differences between operators of essential services, in particular their direct link with physical infrastructure, and digital service providers, in particular their cross-border nature, this Directive should take a differentiated approach with respect to the level of harmonisation in relation to those two groups of entities. For operators of essential services, Member States should be able to identify the relevant operators and impose stricter requirements than those laid down in this Directive. Member States should not identify digital service providers, as this Directive should apply to all digital service providers within its scope. In addition, this Directive and the implementing acts adopted under it should ensure a high level of harmonisation for digital service providers with respect to security and notification requirements. These elements should allow for a uniform treatment of digital service providers across the Union, in a manner proportionate to their nature and degree of risk they may face.
- (57) This Directive should not prohibit Member States from imposing security and notification requirements on entities that are not digital service providers within the scope of this Directive, without prejudice to Member States' obligations under Union law.
- (58) When adopting implementing acts on the security requirements for digital service providers, the Commission is encouraged to take into account the following examples: Relating to security of systems and facilities: physical and environmental security, security of supplies, access control to network and information systems and integrity of network and information systems; relating to incident management: incident management procedures, incident detection capability, incident reporting and communication; relating to business continuity management: service continuity strategy and contingency plans, disaster recovery capabilities; and relating to monitoring, auditing and testing: monitoring and logging policies, exercise contingency plans, network and information systems testing, security assessments and compliance monitoring.

- (59) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing. Publicity of incidents reported to the competent authorities should duly balance the interest of the public in being informed about threats with possible reputational and commercial damages for the operators of essential services and digital service providers reporting incidents. In the implementation of the notification obligations, competent authorities and CSIRTs should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes.
- (60) Digital service providers should be subject to light-touch and reactive ex post supervisory activities justified by the nature of their services and operations. The competent authority should therefore only take action when provided with evidence (for example by the digital service provider itself, by another competent authority, including a competent authority of another Member State, or by a user of the service) that a digital service provider does not comply with the requirements of this Directive, in particular following an incident that has occurred. The competent authority should therefore have no general obligation to supervise digital service providers.
- (61) Competent authorities should have the necessary means to perform their duties, including powers to obtain sufficient information in order to assess the level of security of network and information systems.

- (62) Incidents may be the result of criminal activities, the prevention, investigation and prosecution of which is supported by coordination and cooperation between operators of essential services, digital service providers, competent authorities and law enforcement authorities. Where an incident is suspected to be related to serious criminal activities under national or Union law, Member States should encourage operators of essential services and digital service providers to themselves report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. Where appropriate, it is desirable that coordination between competent authorities and law enforcement authorities of different Member States be facilitated by the Europol Cybercrime Centre (EC3) and ENISA.
- (63) Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle the personal data breaches resulting from incidents.
- (64) Jurisdiction for digital service providers should be attributed to only one Member State, where the operator has its main establishment in the Union, which in principle corresponds to the place where the provider has its head office in the Union. Establishment implies the effective and real 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 this respect. This criterion should not depend on whether the network and information systems are physically located in that place; the presence and use of such systems do not, in themselves, constitute such main establishment and are therefore not criteria for determining the main establishment.

- (65) Where a digital service provider not established in the Union offers services within the Union, it should designate a representative. In order to determine whether such a digital service provider is offering services within the Union, it should be ascertained whether it is apparent that the digital service provider is envisaging the offering of services to persons in one or more Member States in the Union. Whereas the mere accessibility of the digital service provider's or an intermediary's website in the Union or of an email address and of other contact details or the use of a language generally used in the third country where the digital service provider is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that other language, and/or the mentioning of customers or users who are in the Union, may make it apparent that the digital service provider envisages offering services within the Union. The representative should act on behalf of the digital service provider and competent authorities or CSIRTs may contact the representative. The representative should be explicitly designated by a written mandate of the digital service provider to act on his behalf with regard to the latter's obligations, including incident reporting, under this Directive.
- (66) Standardisation of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards to ensure a high level of security at Union level. ENISA should assist Member States through advice and guidelines. To this end it might be helpful to draft harmonised standards, which should be done in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council⁸.

⁸ 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).

- (67) When identifying operators in the maritime sector, Member States should take into account existing and future international codes and guidelines developed in particular by the International Maritime Organisation, with a view to providing individual maritime operators with a coherent approach.
- (68) In the water transport sector, security requirements for companies, ships, port facilities, ports and vessel traffic systems, under Union legal acts cover all operations including the radio and telecommunication systems, computer systems and networks. Part of the mandatory procedures to be followed includes the reporting of all security incidents and should therefore be considered as *lex specialis*, insofar as those requirements are at least equivalent to the corresponding provisions of this Directive.
- (69) Regulation and supervision in the sectors of banking and financial market infrastructures is highly harmonised at EU level, through the use of primary and secondary EU legislation and standards developed together with the European Supervisory Authorities. Within the Banking Union, the application and supervision of these requirements is assured by the Single Supervisory Mechanism (SSM). For Member States that do not form part of the Banking Union this is assured by the relevant banking regulators for Member States. In other areas of financial sector regulation, the European System of Financial Supervision also assures a high degree of commonality and convergence in supervisory practices. The European Securities Markets Authority (ESMA) also has a direct supervision role for certain entities (i.e. credit rating agencies and trade repositories).

- (70) Operational risk is a crucial part of prudential regulation and supervision in the sectors of banking and financial market infrastructures. It covers all operations including the security, integrity and resilience of network and information systems. The requirements for these systems, which often exceed the requirements provided for under this Directive, are set out in a number of Union legal acts, including but not limited to rules on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (CRD IV) and rules on prudential requirements for credit institutions and investment firms (CRR), which include requirements on operational risk; rules on markets in financial instruments (MiFID II), which include requirements on risk assessment for investment firms and for regulated markets; rules on OTC derivatives, central counterparties and trade repositories, which include requirements on operational risk for central counterparties and trade repositories; and rules on improving securities settlement in the European Union and on central securities depositories, which include requirements on operational risk. Furthermore, requirements for notification of incidents are part of normal supervisory practice in the financial sector and are often included in supervisory manuals. Member States should consider the foregoing in their application of *lex specialis*.
- (71) As noted by the European Central Bank in its opinion of 25 July 2014⁹ on the NIS proposal, this Directive does not affect the regime under Union law for the Eurosystem's oversight of payment and settlement systems. It would be appropriate for the authorities responsible for such oversight to exchange experiences on matters concerning NIS with the competent authorities for this Directive. The same consideration applies to non-Eurosystem members of the European System of Central Banks exercising such oversight of payment and settlement systems on the basis of national laws and regulations.

⁹ OJ C 352, 7.10.2014, p. 4.

- (72) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission to specify the procedural arrangements necessary for the functioning of the cooperation group and the security and notification requirements applicable to digital service providers. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council¹⁰. When adopting implementing acts related to the security and notification requirements for digital service providers, the Commission should take utmost account of the opinion of ENISA and should consult interested stakeholders. When adopting implementing acts related to the procedural arrangements necessary for the functioning of the cooperation group, the Commission should take utmost account of the opinion of ENISA.
- (73) In the application of this Directive, the Commission should liaise as appropriate with relevant sectoral committees and relevant bodies set up at Union level in the fields covered by this.
- (74) The Commission should periodically review this Directive, in consultation with all interested stakeholders, in particular with a view to determining the need for modification in the light of changing societal, political, technological or market conditions.

¹⁰ 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 Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

- (75) The sharing of information on risks and incidents within the cooperation group and CSIRTs network and compliance with the requirements to notify incidents to the national competent authorities or CSIRTs may require the processing of personal data. Such a processing of personal data should comply with Directive 95/46/EC of the European Parliament and the Council¹¹ and Regulation (EC) No 45/2001 of the European Parliament and of the Council¹². In the application of this Directive, Regulation (EC) No 1049/2001 of the European Parliament and of the Council¹³ of 30 May 2001 regarding public access to European Parliament, Council and Commission documents should apply as appropriate.
- (76) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 14 June 2013¹⁴.

¹¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p.31).

¹² Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p.1).

¹³ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

¹⁴ OJ C 32, 4.2.2014, p. 19.

- (77) Since the objectives of this Directive, aiming to achieve a high level of NIS in the Union, cannot be sufficiently achieved by the Member States alone and can therefore, 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 those objectives.
- (78) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union notably, the right to respect for private life and communications, the protection for personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive must be implemented according to these rights and principles,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Directive lays down measures with a view to achieving a high common level of security of networks and information systems (hereinafter referred to as "NIS") within the Union so as to improve the functioning of the internal market.
2. To that end, this Directive:
 - (a) lays down obligations for all Member States to adopt a national NIS strategy;
 - (b) creates a cooperation group in order to support and facilitate strategic cooperation and the exchange of information among Member States and develop trust and confidence amongst them;
 - (ba) creates a Computer Security Incident Response Team (CSIRTs) network in order to contribute to developing confidence and trust between Member States and to promote swift and effective operational cooperation;

- (c) establishes security and notification requirements for operators of essential services.
 - (ca) establishes security and notification requirements for digital service providers;
 - (d) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of networks and information systems.
3. The security and notification requirements provided for in this Directive shall apply neither to undertakings which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC, nor to trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014.
4. This Directive shall be without prejudice to Directive 2013/40/EU of the European Parliament and of the Council¹⁵, Directive 2011/93/EU of the European Parliament and of the Council¹⁶ and Council Directive 2008/114/EC¹⁷.
5. This Directive shall be without prejudice to Directive 95/46/CE.

¹⁵ 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).

¹⁶ 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).

¹⁷ Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

- 6a. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other competent authorities only where such exchange is necessary for the application of this Directive. The exchanged information shall be limited to that which is relevant and proportionate to the purpose of such exchange. Such exchange of information shall preserve the confidentiality of that information as well as the security and commercial interests of operators of essential services and digital service providers.
- 6b. This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security (including actions protecting information, the disclosure of which Member States consider contrary to the essential interests of their security), and to maintain law and order, in particular to permit the investigation, detection and prosecution of criminal offences.
7. Where a sector specific Union legal act requires operators of essential services or digital service providers to ensure either the security of their networks and information systems or the notification of incidents, provided that such requirements are at least equivalent in effect to the obligations contained in this Directive, those provisions of that sector specific Union legal act shall apply instead the corresponding provisions of this Directive.

Article 1a

Protection and processing of personal data

1. Processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC.
2. Processing of personal data by Union institutions and bodies pursuant to this Directive shall be carried out in accordance with Regulation (EC) No 45/2001.

Article 1b

Voluntary notification

1. Without prejudice to Article 2, entities which have not been identified as operators of essential services and are not digital service providers may notify incidents having a significant impact on the continuity of the services they provide on a voluntary basis.
2. When processing notifications, Member States shall act in accordance with the procedure set out in Article 14. Member States may process mandatory notifications in priority to voluntary notifications. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on Member States concerned.

Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification.

Article 2

Minimum harmonisation

Without prejudice to Article 15a(1b) and to their obligations under Union law, Member States shall not be prevented from adopting or maintaining provisions with a view to achieving a higher level of security of networks and information systems.

Article 3

Definitions

For the purpose of this Directive, the following definitions shall apply:

- (1) "network and information system" means:
 - (a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC, and
 - (b) any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data, as well as
 - (c) digital data stored, processed, retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance;

- (2) "security of networks and information systems" means the ability of networks and information systems to resist, at a given level of confidence, any action that compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by or accessible via that network and information systems;
- (3) "risk" means any reasonably identifiable circumstance or event having a potential adverse effect on the security of networks and information systems;
- (4) "incident" means any event having an actual adverse effect on the security of networks and information systems;
- (6a) "National strategy on the security of networks and informations systems ("NIS strategy")" means a framework providing strategic objectives and priorities on NIS at national level;
- (7) "incident handling" means all procedures supporting the detection, analysis, containment and response to an incident;
- (8) "operator of essential services" means a public or private entity the type of which is referred to in Annex II, which meets the criteria laid down in Article 3a(1a);

- (9) "standard" means a standard within the meaning of point (1) of Article 2 of Regulation (EU) No 1025/2012;
- (10) "specification" means a technical specification within the meaning of point (4) of Article 2 of Regulation (EU) No 1025/2012;
- (11d) 'digital service ' means a service within the meaning of point 2 (b) of Article 1 of Directive (EU) 2015/1535 of the European Parliament and of the Council¹⁸ which is of a type listed in Annex III;
- (11 da) 'digital service provider' means any legal person that provides a digital service;
- (11e) 'Online marketplace' is a digital service that allows consumers and/or traders as defined respectively in point (a) of Article 4(1) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council¹⁹ to conclude online sales and service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;
- (11g) 'Online search engine' is a digital service that allows users to perform searches of in principle all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input; and returns links in which information related to the requested content can be found;

¹⁸ 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).

¹⁹ Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR)

- (11j) 'Cloud computing service' is a digital service that enables access to a scalable and elastic pool of shareable computing resources;
- (11k) "representative" means any natural or legal person established in the Union explicitly designated to act on behalf of a digital services provider not established in the Union, which may be addressed by the competent authority or CSIRT instead of the digital service provider, with regard to the obligations of the digital service provider under this Directive;
- (11l) "Internet Exchange Point (IXP)" means a network facility that enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic. An IXP provides interconnection only for autonomous systems. An IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;
- (11m) "Domain Name System service provider" means an entity which provides DNS services on the internet (DNS is a hierarchical distributed naming system in a network which refers queries for domain names);
- (11n) "Top-level domain name registry" means an entity which administers and operates the registration of internet domain names under a specific Top-level domain (TLD).

Identification of operators of essential services

1. By ... [6 months after the date referred to in Article 21(1)], for each subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory.
 - 1a. The criteria referred to in Article 3(8) shall be as follows:
 - (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
 - (b) the provision of that service depends on network and information systems; and
 - (c) an incident to the network and information systems of that service would have significant disruptive effects on its provision.

2. For the purposes of paragraph 1, each Member State shall establish a list of the services referred to in point (a) of paragraph 1a.
3. For the purposes of paragraph 1, where an entity provides a service referred to in point (a) of paragraph 1a in two or more Member States, those Member States shall engage in consultation with each other. That consultation shall take place before a decision on identification is taken.
4. Member States shall on a regular basis, and at least every two years after the date referred to in Article 21(1), review and, where appropriate, update the list of identified operators of essential services.
5. The role of the Cooperation Group shall be, in accordance with the tasks referred to in Article 8a, to support Member States to take a consistent approach in the process of identification of operators of essential services.

6. For the purpose of the review referred to in Article 20 and by six months after the date of transposition, and every two years thereafter, Member States shall submit to the Commission the information necessary for the Commission to assess the implementation of this Directive, in particular the consistency of Member States' approaches to the identification of operators of essential services. That information shall include at least:
- (a) national measures allowing for the identification of operators of essential services;
 - (b) the list of services referred to in paragraph 2;
 - (c) the number of operators of essential services identified for each sector referred to in Annex II and an indication of their importance in relation to that sector;
 - (d) thresholds, where they exist, to determine the relevant supply level in accordance with the number of users relying on that service in accordance with point (a) of Article 3b or the importance of that particular operator of essential services in accordance with point (f) of Article 3b.

In order to contribute to the provision of comparable information, the Commission, taking the utmost account of the opinion of the European Network and Information Security Agency (ENISA), may adopt appropriate technical guidelines on parameters for the information referred to in this paragraph.

Significant disruptive effect

1. When determining the significance of a disruptive effect referred to in point (c) of Article 3a(1a), Member States shall take into account at least the following cross-sectoral factors:
 - (a) the number of users relying on the services provided by the entity;
 - (b) the dependency of other sectors referred to in Annex II on the service provided by the entity;
 - (c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
 - (d) the market share of the entity;
 - (e) the geographic spread with regard to the area that could be affected by an incident;
 - (f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternatives for the provision of that service.

2. In order to determine whether an incident would have a significant disruptive effect, Member States shall also take into account sector-specific factors where appropriate.

Article 5

National NIS strategy

1. Each Member State shall adopt a national NIS strategy defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of networks and information systems and covering at least the sectors referred to in Annex II and the services referred to in Annex III. The national NIS strategy shall address in particular the following issues:
 - (a) The objectives and priorities of the national NIS strategy;
 - (b) A governance framework to achieve the objectives and priorities of the national NIS strategy, including roles and responsibilities of the government bodies and the other relevant actors;
 - (c) The identification of measures on preparedness, response and recovery, including cooperation between the public and private sectors;
 - (d) An indication of the education, awareness raising and training programmes relating to the NIS strategy;

- (e) An indication of the research and development plans relating to the NIS strategy;
 - (f) A risk assessment plan to identify possible risks;
 - (g) A list of the various actors involved in the implementation of the NIS strategy;
- 2a. Member States may request the assistance of ENISA in developing national NIS strategies.
3. The national NIS strategy shall be communicated to the Commission within three months from its adoption. In so doing, Member States may exclude elements of the strategy related to national security.

Article 6

National competent authorities and single point of contact

1. Each Member State shall designate one or more national competent authorities on the security of network and information systems (the "competent authority") covering at least the sectors referred to in Annex II and the digital services referred to in Annex III. Member States may designate this role to an existing authority or authorities.
2. The competent authorities shall monitor the application of this Directive at national level.
 - 2a. Each Member State shall designate a national single point of contact on the security of networks and information systems ("single point of contact"). Member States may designate this role to an existing authority. Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.
 - 2c. The single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the cooperation group and the CSIRTs network.
3. Member States shall ensure that the designated competent authorities and the single points of contact have adequate resources to carry out in an effective and efficient manner the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the cooperation group referred to in Article 8a.

4. Member States shall ensure that the competent authorities or CSIRTs receive incident notifications submitted pursuant to this Directive.
 - 4a. In order to enable the single points of contact to submit a summary report on notifications to the Cooperation Group, Member States shall ensure that the competent authorities or CSIRTs inform the single points of contact about incident notifications submitted pursuant to this Directive.
 - 4b. Once a year, the single point of contact shall submit a summary report to the cooperation group on the notifications received, including the number of notifications and the nature of notified incidents, and the action taken in accordance with article 14(2), 14(2ac) and 15a(2).
5. The competent authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate, with the relevant national law enforcement authorities and national data protection authorities.
6. Each Member State shall notify to the Commission without delay the designation of the competent authority and single point of contact, their tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority and single point of contact. The Commission shall publish the list of designated single points of contacts.

Computer Security Incident Response Teams

1. Each Member State shall designate one or more Computer Security Incident Response Teams ("CSIRTs ") covering at least the sectors referred to in Annex II and types of digital services referred to in Annex III, responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CSIRT may be established within a competent authority.
 - 1a. Where they are separate, the competent authority, the single point of contact and the CSIRTs of the same Member State shall cooperate with regard to the obligations laid down in this Directive. Where a Member State decides that CSIRTs shall not receive notifications, the CSIRTs shall, to the extent necessary to fulfil their tasks, be granted access to data on incidents notified by operators of essential services pursuant to Article 14(2) and (2ac) or by digital service providers pursuant to Article 15a(2).
2. Member States shall ensure that the designated CSIRTs have adequate resources to effectively carry out their tasks set out in point (2) of Annex I.

Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRT network referred to in Article 8b.
3. Member States shall ensure that the designated CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level.
4. Member States shall inform the Commission about the remit as well as the main elements of the incident handling process of the CSIRTs.
- 5c. Member States may request the assistance of ENISA in developing national CSIRTs.

CHAPTER III

COOPERATION BETWEEN COMPETENT AUTHORITIES

Article 8a

Cooperation group

1. In order to support and facilitate strategic cooperation among Member States, to develop trust and confidence and with a view to achieving a high common level of security of networks and information systems in the Union, a cooperation group is hereby established.

The cooperation group shall carry out its tasks on the basis of biennial work programmes as referred to in Article 8a(3)(a).

2. The cooperation group shall be composed of representatives from the Member States, the Commission and ENISA.

The Commission shall provide the secretariat.

Where appropriate, the cooperation group may invite representatives from the relevant stakeholders to participate in its work.

3. The cooperation group shall have the following tasks:
- a. By ... [18 months after entry into force of this Directive] and every two years thereafter, establish a work programme on actions to be undertaken to implement the objectives and tasks, which shall be consistent with the objectives of this Directive.
 - b. Provide strategic guidance for the activities of the CSIRTs network established under Article 8b.
 - c. Exchange best practice on the exchange of information related to incident notification referred to in Article 14(2ac) and 15a(2).
 - d. Exchange best practices between Member States and, in collaboration with ENISA, assist Member States in building capacity in NIS;
 - e. Discuss capabilities and preparedness of the Member States, and, on a voluntary basis, evaluate national NIS strategies and the effectiveness of CSIRTs, and identify best practices.
 - f. Exchange information and best practice on awareness raising and training.
 - g. Exchange information and best practice on research and development on network and information security.

- h. Where relevant, exchange experiences on matters concerning NIS with relevant Union institutions bodies, offices and agencies.
- i. Discuss, with representatives from the relevant European Standardisation Organisations, the standards referred to in Article 16.
- j. Collect best practice information on risks and incidents affecting network and information systems;
- k. Examine on an annual basis the summary reports referred to in Article 6(4b).
- l. Discuss the work undertaken with regard to NIS exercises, education programmes and training, including the work by ENISA.
- m. With ENISA's assistance, exchange best practices with regard to the identification of operators of essential services by the Member States, including in relation to cross-border dependencies regarding NIS risks and incidents.
- n. Discuss modalities for reporting notifications of incidents referred to in Article 14 and 15a.

4. As input to the Commission's periodic review of the functioning of this Directive, the cooperation group shall every one and a half years produce a report assessing the experience gained with the strategic cooperation pursued under this Article.

5. The Commission shall establish by means of implementing acts, 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 19(3). For the purposes of the first subparagraph, the Commission shall submit the first draft implementing act to the Committee by ... [6 months after entry into force of this Directive].

CSIRTs network

1. In order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is hereby established.
2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and actively support the cooperation among the CSIRTs.
3. The CSIRTs network shall have the following tasks:
 - a. Exchange information on CSIRTs services, operations and cooperation capabilities.
 - b. At the request of the representative of a Member State potentially affected by an incident, exchange and discuss non-commercially sensitive information related to that incident and associated risks. Any Member State may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident.
 - c. Exchange and make available on a voluntary basis non-confidential information on individual incidents.
 - d. At the request of the representative of a Member State's CSIRT, discuss and, where possible, identify a coordinated response to an incident that has been identified within the jurisdiction of that same Member State.

- e. Support Member States in addressing cross-border incidents on the basis of their voluntary mutual assistance.
- f. Discuss, explore and identify further forms of operational cooperation, including in relation to:
 - (i) categories of risks and incidents
 - (ii) early warnings
 - (iii) mutual assistance
 - (iv) principles and modalities for coordination, when Member States respond to cross border NIS risks and incidents.
- g. Inform the Cooperation Group on its activities and on the further forms of operational cooperation discussed pursuant to paragraph 3(f), and request guidance related thereto.
- h. Discuss lessons learnt from NIS exercises, including from those organised by ENISA.
- i. At the request of an individual CSIRT, discuss the capabilities and preparedness of that same CSIRT.
- j. Issue 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. As input to the Commission's periodic review of the functioning of this Directive, the CSIRTs network shall every one and a half years produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations, pursued under this article. That report shall also be submitted to the cooperation group.
5. The CSIRTs network shall define its own rules of procedure.

Article 13

International cooperation

The Union may conclude international agreements in accordance with Article 218 TFEU with third countries or international organisations allowing and organizing their participation in some activities of the cooperation group. Such agreement shall take into account the need to ensure adequate protection of sensitive data.

CHAPTER IV

SECURITY OF THE NETWORKS AND INFORMATION SYSTEMS OF OPERATORS OF ESSENTIAL SERVICES

Article 14

Security requirements and incident notification

1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of networks and information systems appropriate to the risk presented.
 - 1a. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the networks and information systems used for the provision of such essential services with a view to ensuring the continuity of those services.
2. Member States shall ensure that operators of essential services notify without undue delay to the competent authority or to the CSIRT incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information to enable the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not expose the notifying party to increased liability.

2a. To determine the significance of the impact of an incident, the following parameters in particular shall be taken into account:

- (a) the number of users affected by the disruption of the essential service;
- (b) the duration of the incident;
- (c) the geographical spread with regard to the area affected by the incident.

2ac. Based on the information provided by the operator of essential services, the notified competent authority or CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In doing so, the competent authority or CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the operator's security and commercial interests as well as the confidentiality of the information provided by the operator.

Where the circumstances allow for it, the competent authority or CSIRT shall provide the notifying operator of essential services with relevant information with regards to the follow-up of the notification of an incident, such as information that could support the effective handling of the incident.

At the request of the competent authority or CSIRTs, the single point of contact shall forward notifications referred to in the first subparagraph to single points of contact in other affected Member States.

4. After consulting the operator of essential services concerned, the notified competent authority or CSIRT may inform the public, about individual incidents, where public awareness is necessary to prevent an incident or deal with an ongoing incident.

6. Competent authorities acting together within the cooperation group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 2a.

Implementation and enforcement

1. Member States shall ensure that the competent authorities have the necessary powers and means to assess the compliance of operators of essential services with their obligations under Article 14 and the effects thereof on the security of networks and information systems.
2. Member States shall ensure that the competent authority has the powers and means to require operators of essential services to:
 - (a) provide information needed to assess the security of their networks and information systems, including documented security policies;
 - (b) provide evidence of effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, make the results thereof, including the underlying evidence, available to the competent authority.

When sending that request, the competent authorities shall state the purpose of the request and specify what information is required.

3. Following the assessment of information or results of security audits referred to in paragraph 2, the competent authority may issue binding instructions to the operators of essential services to remedy their operations.
5. The competent authority shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.

*SECURITY OF THE NETWORKS AND INFORMATION SYSTEMS OF DIGITAL SERVICE
PROVIDERS*

Article 15a

Security requirements and incident notification

1. Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented and shall take into account the following elements:
 - security of systems and facilities,
 - incident management,
 - business continuity management,
 - monitoring, auditing and testing,
 - compliance with international standards.

- 1a. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting the security of the digital service provider's networks and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services.
- 1b. Member States shall not impose any further security or notification requirements on digital service providers without prejudice to Article 1(6b).
2. Member States shall ensure that digital service providers notify any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union to the competent authority or to the CSIRT without undue delay. Notifications shall include information to enable the competent authority or CSIRT to determine the significance of any cross-border impact. Notification shall not expose the notifying party to increased liability.

2a. To determine the impact of an incident, the following parameters shall be taken into account, in particular:

(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;

(b) the duration of the incident;

(c) the geographical spread with regard to the area affected by the incident;

(d) the extent of the disruption of the functioning of the service;

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

The obligation to notify an incident shall only apply where the digital service provider has access to the information required to appreciate if the criteria are fulfilled.

2b. Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by the operator of essential services.

3. Where appropriate, in particular if the incident referred to in paragraph 2 concerns two or more Member States, the notified competent authority or the CSIRT shall inform other affected Member States. In doing so, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided.

After consulting the digital service provider concerned, the notified competent authority or CSIRT, and, where appropriate, the authorities or CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where public awareness is necessary to prevent an incident or deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

4. The Commission shall be empowered to adopt implementing acts in accordance with Article 19(3) further specifying the elements referred to in paragraph 1. Those implementing acts shall be adopted by ... [1 year after entry into force of this Directive].
 - 4a. The Commission shall be empowered to adopt implementing acts in accordance with Article 19(3) specifying the parameters listed in paragraph 2. Those implementing acts shall be adopted by ... [1 year after entry into force of this Directive].
 - 4b. The Commission may by means of implementing acts adopt the formats and procedures applicable to notification requirements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).
5. This Chapter shall not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC²⁰.

²⁰ 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).

Implementation and enforcement

1. Member States shall ensure that the competent authorities take action, if necessary, through ex post supervisory activities, when provided with evidence that a digital service provider does not meet the requirements laid down in Article 15a. Such evidence may be submitted by a competent authority of another Member State where the service is provided.
2. For the purpose of paragraph 1, the competent authorities shall have the necessary powers and means to:
 - (a) require digital service providers to provide information needed to assess the security of their networks and information systems including documented security policies
 - (b) require that digital service providers remedy any failure to fulfil the requirements laid down in article 15a.
3. If a digital service provider has its main establishment or a representative in one Member State, but its networks and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or of the representative and the competent authorities of these other Member States shall cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between competent authorities concerned and requests to carry out the supervisory measures referred to in paragraph 2.

Jurisdiction and territoriality

1. For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State where it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in the Union in that Member State.

2. A digital service provider that is not established in the Union, but offers services as referred to in Annex III within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established.

4. The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself.

CHAPTER IVb

STANDARDISATION

Article 16

Standardisation

1. To promote convergent implementation of Article 14(1), 14(1a), 15a(1) and 15a(1a) Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and/or specifications relevant to security of networks and information systems.
- 1a. ENISA, in collaboration with Member States, shall elaborate advice and guidelines regarding the technical areas which should be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for covering these areas.

CHAPTER V

FINAL PROVISIONS

Article 17

Penalties

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

Article 19

Committee procedure

1. The Commission shall be assisted by a committee (the Network and Information Security Committee). That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
3. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 20

Review

1. The Commission shall submit a report to the European Parliament and to Council one year after the date of transposition, assessing the consistency of the approach taken by Member States in the identification of the operators of essential services.
2. The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and CSIRT network on the experience gained at a strategic and operational level. In its review the Commission shall also assess the list contained in Annex II and III, and the consistency in the identification of operators of essential services and services in the sectors referred to in Annex II. The first report shall be submitted no later than three years after the date referred to in Article 21(1).

Article 20a

Transitional measures

1. Without prejudice to Article 21 and with a view of providing Member States with additional possibilities for appropriate cooperation during the period of transposition, the Cooperation Group and the CSIRTs Network shall begin to perform their tasks set out respectively in Articles 8a(3) and 8b(3) by 6 months after the date of entry into force of this Directive.
 - 1a. In the period between the dates set out in paragraph 1 and in article 3a(1) , and for the purposes of supporting Member States to take a consistent approach in the process of identification of operators of essential services, the Cooperation Group shall discuss the process, substance and type of national measures allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 3a and 3b. The Cooperation Group shall also discuss, at the request of a Member State, specific draft national measures of that Member State, allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 3a and 3b.
2. By 6 months after the date of entry into force of this Directive and for the purposes of this Article, Member States shall ensure appropriate representation in the Cooperation Group and the CSIRTs Network.

Article 21

Transposition

1. Member States shall adopt and publish, by ... [21 months after the date of entry into force of this Directive] at the latest, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith communicate to the Commission the text of such provisions.
2. They shall apply those measures from one day after the date referred to in paragraph 1.
3. When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.
4. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 22

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 23

Addressees

This Directive is addressed to the Member States.

Done at ...,

For the European Parliament
The President

For the Council
The President

Requirements and tasks of the Computer Security Incident Response Team (CSIRT)

The requirements and tasks of the CSIRT shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following elements:

(1) Requirements for the CSIRT

(a) The CSIRTs shall ensure high availability of its communications services by avoiding single points of failure and have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.

(c) The offices of the CSIRT and the supporting information systems shall be located in secure sites.

(e) Business continuity:

- The CSIRT shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers,
- The CSIRT shall be adequately staffed to ensure availability at all times,
- The CSIRT shall rely on an infrastructure whose continuity is ensured. To this end, redundant systems and backup working space shall be available.

(f) CSIRTs shall have the possibility to participate, where appropriate, in international cooperation networks

(2) Tasks of the CSIRT

(a) Tasks of the CSIRT shall include at least the following:

- Monitoring incidents at a national level,
- Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents,
- Responding to incidents,
- Providing dynamic risk and incident analysis and situational awareness,
- Participating in the CSIRT network

(b) The CSIRT shall establish cooperative relationships with private sector.

(c) To facilitate cooperation, the CSIRT shall promote the adoption and use of common or standardised practises for:

- incident and risk handling procedures,
- incident, risk and information classification schemes.

Sector	Subsector	Type of entity for the purposes of Article 3(8)
1. Energy	<i>a) Electricity</i>	- Electricity undertaking as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council ²¹ , which carries out the function of "supply" as defined in point (19) of Article 2 of Directive 2009/72/EC
		- Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC
		- Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC
	<i>b) Oil</i>	- Operator of oil transmission pipelines
		- Operators of oil production, refining and treatment facilities, storage and transmission

²¹ Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (OJ L 211, 14.8.2009, p. 55).

	<i>c) Gas</i>	- Supply undertakings as defined in point (8) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council ²²
		- Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC
		- Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC
		- Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC
		- LNG system operator as defined in point (12) of Article 2 of Directive 2009/73/EC
		- Natural gas undertaking as defined in point (1) of Article 2 of Directive 2009/73/EC
		- Operator of natural gas refining and treatment facilities

²² 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).

2. Transport	<i>(a) Air transport</i>	- Air carriers as defined in point (4) of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council ²³
		- Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council ²⁴ , managing airports as defined in point (1) of Article 2 of Directive 2009/12/EC, including the core airports listed in section 2 of Annex II of Regulation (EU) No 1315/2013 of the European Parliament and of the Council ²⁵ ; and entities operating ancillary installations contained within airports.
		- Traffic management control operators providing air traffic control (ATC) service as defined in point (1) of Article 2 of Regulation (EC) No 549/2004 of the European Parliament and of the Council ²⁶
	<i>(b) Rail transport</i>	- Infrastructure managers as defined in point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council ²⁷

²³ 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).

²⁴ 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).

²⁵ 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).

²⁶ 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).

²⁷ 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).

		- Railway undertakings as defined in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities as defined in point (12) of Article 3 of Directive 2012/34/EU
	<i>(c) Water transport</i>	(i) inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I of Regulation (EC) No 725/2004 of the European Parliament and of the Council ²⁸ , not including the individual vessels operated by those companies
		(ii) Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council ²⁹ , including their port facilities as defined in point (11) of Article 2 of Regulation (EC) 725/2004; and entities operating works and equipment contained within ports

²⁸ 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).

²⁹ 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).

		(iii) Operators of vessel traffic services, as defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council ³⁰
	<i>(d) Road Transport</i>	(i) Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 ³¹ responsible for traffic management control
		(ii) Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council ³²

³⁰ 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).

³¹ 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).

³² 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).

3. Banking		- credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council ³³
4. Financial market infrastructures		- Operators of trading venues as defined in Article 4 of Directive 2014/65/EU of the European Parliament and of the Council ³⁴
		- Central counterparty as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council ³⁵
5. Health sector	Health care settings (including hospitals and private clinics)	- healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council ³⁶

³³ Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p.1).

³⁴ 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).

³⁵ 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).

³⁶ 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).

6. Drinking water supply and distribution		Supplier and distributor of "water intended for human consumption" as defined in point (1)(a) of Article 2 of Council Directive 98/83/EC ³⁷ but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distribution of commodities and goods.
7. Digital Infrastructure		Internet exchange points
		Domain name system service providers
		Top Level Domain name registries

³⁷ Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).

Types of digital services for purposes of Article 3(11d)

1. Online marketplace
 2. Online search engine
 3. Cloud computing service
-