Council of the European Union

Brussels, 16 September 2014

13143/14

LIMITE

TELECOM 162
DATAPROTECT 119
CYBER 44
MI 650
CSC 206
CODEC 1800

Interinstitutional File: 2013/0027 (COD)

NOTE

from:	Presidency
to:	Delegations
No. prev. doc.:	12062/14 TELECOM 146 DATAPROTECT 106 CYBER 41 MI 562 CSC 174 CODEC 1649
No. Cion prop.:	6342/13 TELECOM 24 DATAPROTECT 14 CYBER 2 MI 104 CODEC 313 ADD 1 + ADD 2
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 *- draft Coreper mandate*

1. On the basis of document 10153/14, the WP TELE discussed on 25 June and 17 July, and on the basis of doc. 12062/14 on 4 and 11 September, in particular three issues in relation to the above mentioned proposal: scope -- i.e. operators in specific sectors providing essential services; cooperation, -- i.e. strategic and operational cooperation in the short and longer-term; and incident notification at national and EU levels. On the basis of the discussions and on the written comments received from delegations, the following amendments were introduced in the annexed text:

2. Article 1 (Subject matter and scope):

— 1(1): the words "so as to improve the functioning of the internal market" have been added" so as to reinforce 114 TFEU.

— 1(2)b: "of Member States" has been deleted as membership of the cooperation group is broader than Member States.

— 1(2)d: "single points of contact amd CERTs" were added.

— 1(3) has been editorially modified.

— 1(6a): it is suggested to link this paragraph to a new recital, which recall the respective article in the Treaty and which would underline that it is up to the Member States to assess whether or not to supply NIS-related information: “It is appropriate to recall that according to Article 346 TFEU, no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security."

3. Article 3 (Definitions):

— 3(1)a: the reference in this paragraph has been specified.

— 3(2): "accident or malicious" has been replaced with "any" and the word "and" in "integrity and confidentiality" has been replaced with "or".

— 3(2a): the words " contributing to the functioning of the internal market" have been added.

— 3(3) and 3(4): the words "network and information" have been put before "security" and in 3(3), "and" has been replaced by "or".

— 3(5) has been deleted.

— 3(8): the definition of "operator" has been substantially modified. An additional field "digital infrastructure underpinning the Internet" has been added, which should be understood to cover the definitions of 'telecommunications infrastructure' and 'digital service infrastructure' of the CEF Telecoms Guidelines (Regulation 283/2014). Furthermore, it has been clarified that it is the responsibility of the Member States to identify operators which meet the criteria of Article 3(8) and which are thus covered by the security and incident notification requirements of this Directive. In view of these changes, further consideration is needed whether or not to maintain ANNEX II.

4. Article 5 (National NIS strategy):

— 5(1): the words "in the fields referred to in Article 3(8)" have been inserted.

— 5(1)a & b have been linguistically modified.

— 5(2)a and 5(2)b have been replaced and added to 5(1) and, as a consequence, the chapeau in 5(2) has been deleted.

5. Article 6 (National competent authorities and single point of contact):

— 6(1): the words "or authorities" has been added.

— 6(2)a has been simplified and requires Member States to designate a single point of contact.

— 6(3): the words "technical, financial and human" and "notably" have been deleted.

— 6(4) has been deleted as the substance is covered by Article 14(2).

— 6(5): the words "consult and cooperate" have been re-instated and "in accordance with national legislation" has been added. However, this paragraph may need further adjustment pending the final wording on Article 8a.

6. Article 7 (Computer Emergency Response Team):

— Article 7: in this article as well as throughout the text, "Computer Emergency Response Team" will be replaced by "Computer Security Incident Response Team" in the next version of the proposal.

— 7(1): the words "at a national level" have been deleted.

— 7(1a): the last sentence of this paragraph has been modified.

— 7(2): as in Article 6(3), the words "technical, financial and human" have been deleted.

— 7(5) has been deleted.

7. Article 8a (Cooperation Group):

— 8a(1): the words "in the fields referred to in Article 3(8)" have been inserted.

— 8a(3)ab: a new paragraph on information on incident notification has been added.

— 8a(3)g: the words "and discuss links to Horizon 2020" have been deleted.

— 8a(3)i has been substantially modified.

8. Article 8b (CERTs network):

— 8b(1): the words "in the fields referred to in Article 3(8)" have been inserted.

— 8b(3)b has been modified.

— 8b(3)c has been linguistically modified.

9. Article 14 (security requirements and incident notification):

— 14(1) & (2): the word "provide" has been replaced with "require".

— 14(1): "the words "the security of network and information" has been replaced with "network and information security".

— 14(1a): it should be considered to re-instate the word "continuity" in the last sentence or to clarify the term “security” used therein. Similar considerations are needed in relation to the use of the term “security” in the last sentence of Article 14(2).

— 14(2): the last sentence has been deleted.

— 14(2)2a has been linguisticaly modified.

— 14(2b) new: a new paragraph on incident notification has been added. In order to clarify the role of the Single Point of Contact, the proposal needs to specify the tasks of the SPC. In this respect, futher consideration is also needed in relation to Articles 14(4) and 15(2).

— 14(6): the words "when requested" have been re-instated.

10. Articles 16 (Standardisation), 20 (Review) & 21 (Transposition):

— Article 16(1): the words "internationally accepted" have been deleted.

— Article 20 has been substantially amended in view of addressing the possibility of further enhanced cooperation at a specific point in time.

— Article 21(3): the word "shall" has been replaced with "may".

11. ANNEXES I & II:

— ANNEX I: further detailed discussions on this ANNEX are needed, taking the suggestions from Member States into account.

— ANNEX II: further detailed discussions on this ANNEX are needed, taking the current wording of Article 3(8) into account. In case delegations wish to maintain ANNEX II, it could possibly be simplified in accordance with ANNEX I from Directive 2008/114/EC for as far as energy and transport is concerned and to complement it with the other fields referred to in Article 3(8) of the current proposal. For example and in as far as "digital infrastructure underpinning the Internet" (see art.3(8)) is concerned, further discussion is needed as to which subsectors to include (Internet-enablers? OTT?).

12. A first exploratory trilogue with the Parliament is planned to take place on 14 October. The Presidency intends to request Coreper for a mandate for this event on 10 October on the basis of the attached text, which will first be discussed in the WP TELE on 18 September and on 1 October.

13. At the WP TELE on 18 September, delegations will be invited to comment on the annexed revised text and on the outstanding above mentioned issues. Delegations are also urged to signal their position on the EP amendments, either at the WP TELE meeting or in writing before 1 October.

ANNEX

2013/0027 (COD)

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

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

After consulting the European Data Protection Supervisor,

Acting in accordance with the ordinary legislative procedure,

Whereas:

HAVE ADOPTED THIS DIRECTIVE:

[1] OJ C […], […], p. […].

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Directive lays down measures to facilitate a high common level of network and information security (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 concerning the prevention, the handling of and the response to serious risks and incidents affecting networks and information systems;

   (b) creates a cooperation group ~~mechanism~~ **~~of between Member States~~** in order to ~~ensure a uniform application of this Directive within the Union~~**support and facilitate strategic cooperation and the exchange of information among Member States** ~~and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems~~;[2]

   (ba) creates a CERTs network in order to contribute to developing confidence and trust between Member States and to promote swift, effective operational cooperation

   (c) establishes security and notification requirements for ~~**market**~~ operators ~~**and public administrations**~~.[3]

---

[2] **AM 40:** (b) creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated**,** efficient ***and effective*** handling of and response to risks and incidents affecting network and information systems ***with the participation of relevant stakeholders***;

[3] **AM 41:** (c) establishes security requirements for market operators.

(d) lays down obligations for Member States to designate national competent authorities**, single points of contact and CERTs concerned with ~~on~~** the security of network and information systems, and provides for the competenceof those authorities to enforce the compliance of ~~**market**~~ operatorswith security and notification requirements.

3. The security **and notification** requirements provided for in Article 14 shall apply neither to undertakings ~~**providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC, which shall comply with the specific security and integrity requirements laid down in**~~**which are subject to the requirements of** Articles 13a and 13b of Directive **2002/21/EC**, nor to trust service providers ~~**within the meaning of the eIDAS Regulation (reference article 3(19) of**~~ **which are subject to the requirements of Article 19 of Regulation 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**.

4. This Directive shall be without prejudice to EU laws on cybercrime and 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[4]

[4] OJ L 345, 23.12.2008, p. 75.

5. This Directive shall also be without prejudice to Directive 95/46/CE 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[5], and to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [and to the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data][6]. [7]

6. ~~The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require t~~The processing of personal data~~. Such processing, which is~~ necessary to meet the objectives of public interest pursued by this Directive, shall comply with the requirements laid down in ~~be authorised by the Member State pursuant to~~ [Article 7 of] Directive 95/46/EC and Directive 2002/58/EC, as implemented in national law.

---

5 OJ L 281 , 23/11/1995 p. 31.

6 SEC(2012) 72 final.

7 **AM 42:** 5. This Directive shall also be without prejudice to Directive 95/46/CE 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 and to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector and to the 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. ***Any use of the personal data shall be limited to what is strictly necessary for the purposes of this Directive, and those data shall be as anonymous as possible, if not completely anonymous.***

[8]

[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.]

[*Article 2*

Minimum harmonisation

Member States shall not be prevented from adopting or maintaining provisions facilitating ~~ensuring~~ a higher level of **network and information** security, without prejudice to their obligations under Union law.]

[8] **AM 43:** ***Article 1a (new) Protection and processing of personal data***
1. Any processing of personal data in the Member States pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC and Directive 2002/58/EC.
2. Any processing of personal data by the Commission and ENISA pursuant to this Regulation shall be carried out in accordance with Regulation (EC) No 45/2001.
3. Any processing of personal data by the European Cybercrime Centre within Europol for the purposes of this Directive shall be carried out pursuant to Decision 2009/371/JHA.
4. The processing of personal data shall be fair and lawful and strictly limited to the minimum data needed for the purposes for which they are processed. They shall be kept in a form which permits the identification of data subjects for no longer than necessary for the purpose for which the personal data are processed.
5. Incident notifications referred to in Article 14 shall be without prejudice to the provisions and obligations regarding personal data breach notifications set out in Article 4 of Directive 2002/58/EC and in Regulation (EU) No 611/2013.

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 computer data, as well as [9]

(c) computer data stored, processed, retrieved or transmitted by elements covered under point (a) and (b) for the purposes of their operation, use, protection and maintenance.[10]

(2) "network and information security" means the ability of a network and information system to resist, at a given level of confidence, **any ~~accident or malicious~~** action that compromise the availability, authenticity, integrity **or ~~and~~** confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system;[11]

---

[9] **AM 44:** (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

[10] **AM 45:** (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.

[11] **AM 46:** (2) 'security' means the ability of a network and information system to resist, at a given level of confidence, accident or malicious action that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data or the related services offered by or accessible via that network and information system; ***'security' includes appropriate technical devices, solutions and operating procedures ensuring the security requirements set out in this Directive.***

(2a) "essential services" means ~~**vital**~~ economic and societal **services ~~activities~~ essential for ~~contributing to~~ the functioning of the internal market**.

(3) "risk" means any circumstance or event having a potential serious **or ~~and~~** actual adverse effect on **network and information** security;[12]

(4) "incident" means any circumstance or event having an actual adverse effect on **network and information** security that can lead to a substantial loss or disruption to essential services;[13]

~~**[(5) "information society service" mean service within the meaning of point (2) of Article 1 of Directive 98/34/EC;]**~~[14]

~~(6) "NIS cooperation plan" means a plan establishing the framework for organisational roles, responsibilities and procedures to maintain or restore the operation of networks and information systems, in the event of a risk or an incident affecting them;~~

(6a) "National NIS strategy" means a framework providing high-level vision, objectives and priorities on NIS at national level;

(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;[15]

---

12 **AM 47:** (3) 'risk' means any ***reasonably identifiable*** circumstance or event having a potential adverse effect on security;

13 **AM 48:** (4) 'incident' means any event having an actual adverse effect on security;

14 **AM 49:** ***deleted***

15 **AM 50:** (7) 'incident handling' means all procedures supporting the ***detection, prevention,*** analysis, containment and response to an incident;

(8) "~~market~~ operator" means **a public or private entity** [16] **referred to in Annex II, which provides an essential service ~~or a critical infrastructure~~ in the fields of digital infrastructure underpinning the Internet, energy, transport, banking, financial market infrastructures, health and water supply and which fulfills at leat one of the following criteria:**

- **the service ~~or infrastructure~~ depends heavily on network and information technologies;**

- ~~**the service or infrastructure is provided to a high critical mass of customers or users;**~~

- **a failure or attack to the ~~underlying~~ network and information technologies of the service ~~or infrastructure will~~ havinge serious disruptive effects for social and economic activities, and/or having public safety implications.** [17]

Each Member State shall identify on its territory operators which provide essential services in the above mentioned fields and which fulfil the above mentioned criteria.

~~**The subsectors to be used for the purposes of implementing this Directive are identified in ANNEX II.**~~ [18] ~~**[**~~

~~**(a) provider of information society services which enable the provision of other information society services, a non exhaustive list of which is set out in Annex II;**~~

---

16 **a recital will clarify that "operator" covers also public administrations**

17 **AM 51:** ***deleted***

18 **AM 52:** (b) operator of infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, ***financial market infrastructures, internet exchange points, food supply chain*** and health***, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions***, a non exhaustive list of which is set out in Annex II***, insofar as the network and information systems concerned are related to its core services;***

~~**(b)]** **an operator of critical infrastructure that is necessary are essential for the maintenance of essential services vital economic and societal activities in the fields of energy, transport, banking and financial market infrastructure stock exchanges and health [, a non-exhaustive list of which is set out in Annex II].**~~

19

(9) "standard" means a standard referred to in **point (1) of Article 2** of Regulation (EU) No 1025/2012;

(10) "specification" means a **technical** specification referred to in **point (4) of Article 2 of** Regulation (EU) No 1025/2012;

(11) "Trust service provider" means a natural or legal person within the meaning of **point (19) of Article 3 of** Regulation **910/2014** ~~who provides any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals~~.

19 **AM 53:** ***(8a) 'incident having a significant impact' means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions;***

[20]

[21]

[22]

CHAPTER II

NATIONAL FRAMEWORKS ON NETWORK AND INFORMATION SECURITY

~~*Article 4*~~

~~**Principle**~~

~~Member States shall ensure a high level of security of the network and information systems in their territories in accordance with this Directive.~~

---

[20] **AM 54:** ***(11a) 'regulated market' means regulated market as defined in point 14 of Article 4 of Directive 2004/39/EC of the European Parliament and of the Council[1a]***

[1a] ***Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments (OJ L 45, 16.2.2005, p. 18).***

[21] **AM 55:** ***(11b) 'multilateral trading facility (MTF)' means multilateral trading facility as defined in point 15 of Article 4 of Directive 2004/39/EC;***

[22] **AM 56:** ***(11c) 'organised trading facility' means a multilateral system or facility, which is not a regulated market, a multilateral trading facility or a central counterparty, operated by an investment firm or a market operator, in which multiple third-party buying and selling interests in bonds, structured finance products, emission allowances or derivatives are able to interact in the system in such a way as to result in a contract in accordance with Title II of Directive 2004/39/EC;***

Article 5

National NIS strategy ~~and national NIS cooperation plan~~

1. Each Member State shall adopt a national NIS strategy defining the strategic objectives and concrete policy and regulatory measures to ~~help~~ facilitate ~~achieve and maintain~~ a high level of network and information security **at least in the fields referred to in Article 3(8)**. The national NIS strategy shall address in particular the following issues:

(a) ~~The definition of the~~ **The** ~~its~~ objectives and priorities **of the national NIS strategy** ~~based on an up-to-date risk and incident analysis~~;

[(b) **the** ~~A~~ governance framework **put in place** to achieve **the** ~~the strategy~~ objectives and priorities **of the national NIS strategy**~~, including a clear definition of the roles and responsibilities of the government bodies and the other relevant actors~~;]

(c) The identification of the general measures on preparedness, response and recovery [, including cooperation mechanisms between the public and private sectors];

(d) An indication of the education, awareness raising and training programmes relating to the NIS strategy;

~~(e) Research and development plans and a description of how these plans reflect the identified priorities.~~

(f) A risk assessment plan to identify potential risks ~~and assess the impacts of potential incidents;~~[23]

(g) ~~The definition of the roles and responsibilities~~ A list of the various actors involved in the implementation of the NIS strategy ~~plan;~~[24]

[25]

~~**2. The national NIS strategy shall include details on a national NIS cooperation, such as plan complying at least with the following requirements:**~~

~~**(a) A risk assessment plan to identify potential risks and assess the impacts of potential incidents;**[26]~~

~~**(b) The definition of the roles and responsibilities A list of the various actors involved in the implementation of the NIS strategy plan;**[27]~~

~~(c) The definition of cooperation and communication processes ensuring prevention, detection, response, repair and recovery, and modulated according to the alert level;~~

~~(d) A roadmap for NIS exercises and training to reinforce, validate, and test the plan. Lessons learned to be documented and incorporated into updates to the plan.~~

---

[23] **AM 58:** (a) A risk ***management framework to establish a methodology for the identification, prioritisation, evaluation and treatment of risks, the assessment of*** the impacts of potential incidents***, prevention and control options, and to define criteria for the choice of possible countermeasures***;

[24] **AM 59:** (b) The definition of the roles and responsibilities of the various ***authorities and other*** actors involved in the implementation of the ***framework***;

[25] **AM 57:** ***(ea) Member States may request the assistance of ENISA in developing their national NIS strategies and national NIS cooperation plans, based on a common minimum NIS strategy.***

[26] **AM 58:** (a) A risk ***management framework to establish a methodology for the identification, prioritisation, evaluation and treatment of risks, the assessment of*** the impacts of potential incidents***, prevention and control options, and to define criteria for the choice of possible countermeasures***;

[27] **AM 59:** (b) The definition of the roles and responsibilities of the various ***authorities and other*** actors involved in the implementation of the ***framework***;

~~[2a Member States shall ensure an appropriate governance framework for this work is in place.]~~

3. The Member States shall make available to the Commission **at least** a summary of the national NIS strategy ~~and the national NIS cooperation plan shall be communicated to the Commission within one month from their adoption~~.[28]

Article 6

National competent authorities~~y~~ and single point of contact ~~on the security of network and information systems~~[29]

1. Each Member State shall designate one or more ~~a~~ national competent authorities~~y~~ on the security of network and information systems (the "competent authority").[30] Member States may designate this role to an existing ~~organisation or~~ authority **or authorities**.

~~2. The competent authorities shall monitor the application of this Directive at national level and contribute to its consistent application throughout the Union.~~

[28] **AM 60:** 3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within ***three months*** from their adoption.

[29] **AM 61:** National competent ***authorities and single points of contact*** on the security of network and information systems

[30] **AM 62:** 1. Each Member State shall designate ***one or more civilian*** national competent ***authorities*** on the security of network and information systems (***hereinafter referred to as*** 'competent authority***/ies***').

2a. **~~Where a~~** Member State**s shall** designate **~~more than one competent authority, it shall designate~~** a national single point of contact on **~~the security of~~** network and information **security ~~systems~~** (~~hereinafter referred to a~~ "single point of contact"). **~~Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.~~**

[2b. The competent authorities and the single point of contact of the same Member State shall cooperate closely with regard to the obligations laid down in this Directive.]

31

32

33

---

31 **AM 63:** ***2a.(new) Where a Member State designates more than one competent authority, it shall designate a civilian national authority, for instance a competent authority, as national single point of contact on the security of network and information systems (hereinafter referred to as 'single point of contact'). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.***

32 **AM 64:** ***2b. (new) The competent authorities and the single point of contact of the same Member State shall cooperate closely with regard to the obligations laid down in this Directive.***

33 **AM 65:** ***2c. The single point of contact shall ensure cross-border cooperation with other single points of contact.***

[3. Member States shall ensure that the competent authorities have adequate ~~**technical, financial and human**~~ 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 the effective, efficient and secure cooperation of the competent authorities ~~**notably**~~ via the ~~network~~ **group** referred to in Article 8**a**.] [34]

~~**[4. With the aim to increase the NIS level, Member States shall ensure that the competent authorities receive the notifications of incidents from market operators and public administrations as specified under Article 14(2)and are granted the implementation and enforcement powers referred to under Article 15.]**~~ [35]

[36]

[34] **AM 66:** 3. Member States shall ensure that the competent authorities ***and the single points of contact*** have adequate technical, financial and human 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 the effective, efficient and secure cooperation of the ***single points of contact*** via the network referred to in Article 8.

[35] **AM 67:** 4. Member States shall ensure that the competent authorities ***and single points of contact, where applicable in accordance with paragraph 2a of this Article,*** receive the notifications of incidents from market operators as specified under Article 14(2) and are granted the implementation and enforcement powers referred to under Article 15.

[36] **AM 68:** ***4a. Where Union law provides for a sector-specific Union supervisory or regulatory body, inter alia on the security of network and information systems, that body shall receive the notifications of incidents in accordance with Article 14(2) from the market operators concerned in that sector and be granted the implementation and enforcement powers referred to under Article 15. That Union body shall cooperate closely with the competent authorities and the single point of contact of the host Member State with regard to those obligations. The single point of contact of the host Member State shall represent the Union body with regard to the obligations laid down in Chapter III.***

[5. The competent authorities shall **consult and cooperate**, whenever appropriate **and in accordance with national legislation**, **with** the relevant [law enforcement national authorities and] data protection authorities.][37]

6. Each Member State shall notify to the Commission without delay the designation of the competent authorities~~y~~ and single point of contact, **their** ~~its~~ tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authorities~~y~~ and single point of contact.[38]

Article 7

Computer Emergency Response Team

1. Each Member State shall designate one or more ~~set up a~~ Computer Emergency Response Teams (hereinafter: "CERTs") responsible for handling ~~**at a national level**~~ incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within the competent authority.[39]

---

37 **AM 69:** 5. The competent authorities ***and single points of contact*** shall consult and cooperate, whenever appropriate, with the relevant law enforcement national authorities and data protection authorities.

38 **AM 70:** 6. Each Member State shall notify to the Commission without delay the designation of the competent ***authorities and the single point of contact***, its tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent ***authorities***.

39 **AM 71:** 1. Each Member State shall set up ***at least one*** Computer Emergency Response Team (hereinafter: 'CERT') ***for each of the sectors established in Annex II,*** 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 CERT may be established within the competent authority.

1a. Where they are separate, the competent authorities, the single point of contact and the CERTs of the same Member State shall cooperate closely with regard to the obligations laid down in this Directive. **National CERTs shall have access via the competent authority to the incident notification data provided by operators.**

[2. Member States shall ensure that CERTs have adequate ~~**technical, financial and human**~~ resources to effectively carry out their tasks set out in point (2) of Annex I.]

3. Member States shall ensure that CERTs have access to an appropriate ~~rely on a secure and resilient~~ communication and information infrastructure at national level~~, which shall be compatible and interoperable with the secure information-sharing system referred to in Article 9~~.

4. Member States shall inform the Commission about the remit ~~resources and mandate as well as the incident handling process~~ of the CERTs.

~~**5. Where competent authority and CERTs are separate, the CERTs shall act under the supervision of the competent authority. , whichThe competent authority shall regularly review the adequacy of its the resources of the CERTs, its remit mandate and the effectiveness of its incident-handling process.**~~[40]

[41]

[42]

[43]

---

[40] **AM 72:** 5. The ***CERTs*** shall act under the supervision of the competent authority ***or the single point of contact***, which shall regularly review the adequacy of ***their*** resources, ***mandates*** and the effectiveness of ***their*** incident-handling process.

[41] **AM 73:** ***5a. (new) Member States shall ensure that CERTs have adequate human and financial resources to actively participate in international, and in particular Union, cooperation networks***

[42] **AM 74:** ***5b (new) The CERTs shall be enabled and encouraged to initiate and to participate in joint exercises with other CERTs, with all Member States-CERTs, and with appropriate institutions of non-Member States as well as with CERTs of multi- and international institutions such as NATO and the UN.***

[43] **AM 75:** ***5c. (new) Member States may ask for the assistance of ENISA or of other Member States in developing their national CERTs.***

CHAPTER III

COOPERATION BETWEEN MEMBER STATES ~~COMPETENT AUTHORITIES~~ AND CERTS

Article 8a

Cooperation group ~~network~~

~~1. The … systems.~~[44]

~~2. The … and advice.~~[45]

[44] **AM 76:** 1. The ***single points of contact*** and the Commission ***and ENISA*** shall form a network (***hereinafter referred to as*** 'cooperation network') to cooperate against risks and incidents affecting network and information systems.

[45] **AM 77:** 2. The cooperation network shall bring into permanent communication the Commission and the ***single points of contact***. When requested, ENISA shall assist the cooperation network by providing its expertise and advice. ***Where appropriate, market operators and suppliers of cyber security solutions may also be invited to participate in the activities of the cooperation network referred to in points (g) and (i) of paragraph 3. Where relevant, the cooperation network shall cooperate with the data protection authorities.***
The Commission shall regularly inform the cooperation network of security research and other relevant programmes of Horizon2020.

~~3. Within … shall:~~[46]

~~(a) circulate … Article 10;~~

~~[(b) ensure … Article 11;]~~

~~(c) publish … website;~~

~~(d) jointly … this Directive.~~

~~(e) jointly … Union level;~~

~~(f) cooperate … and health;~~

[46] **AM 78:** 3. Within the cooperation network the ***single points of contact*** shall:
(a) circulate early warnings on risks and incidents in accordance with Article 10;
(b) ensure a coordinated response in accordance with Article 11;
(c) publish on a regular basis non-confidential information on on-going early warnings and coordinated response on a common website;
(d) jointly discuss and assess one or more national NIS strategies and national NIS cooperation plans referred to in Article 5, within the scope of this Directive***;***
(e) jointly discuss and assess the effectiveness of the CERTs, in particular when NIS exercises are performed at Union level;
(f) cooperate and exchange ***expertise on*** relevant matters ***on network and information security,*** in particular in the fields of data protection, energy, transport, banking, ***financial markets*** and health ***with the European Cybercrime Centre within Europol, and with other relevant European bodies***;
(fa) where appropriate, inform the EU Counter-terrorism Coordinator, by means of reporting, and may ask for assistance for analysis, preparatory works and actions of the cooperation network;
(g) exchange information and best practices between themselves and the Commission, and assist each other in building capacity on NIS;
(i) organise NIS exercises at Union level and participate, as appropriate, in international NIS exercises.
(ia) involve, consult and exchange, where appropriate, information with market operators with respect to the risks and incidents affecting their network and information systems;
(ib) develop, in cooperation with ENISA, guidelines for sector-specific criteria for the notification of significant incidents, in addition to the parameters laid down in Article 14(2), for a common interpretation, consistent application and harmonious implementation within the Union.

~~(g) exchange … on NIS;~~

~~(h) organise … preparedness;~~

~~(i) organise … exercises.~~

1. In order to support and facilitate strategic cooperation and the exchange of information among Member States **in the fields referred to in Article 3(8)**, a cooperation group is hereby established.

2. The cooperation group shall be composed of representatives from the Member States, the Commission and the European Network and Information Security Agency ("ENISA"). The Commission shall provide the secretariat. Where appropriate, representatives from the competent authorities and ~~market~~ operators shall be invited to participate in the discussions of the cooperation group.

3. The tasks of the cooperation group shall be to:[47]

a. ~~Steer~~ **Provide guidance for** the activities of the CERTs network established under Article.

ab. Exchange best practice on the exchange of information related to incident notification referred to in Article 14(2b).

b. Exchange best practices between ~~themselves~~ **Member States** and, in collaboration with ENISA, assist **Member States** ~~each other~~ in building capacity in NIS;

c. At the request of a Member State organise regular peer reviews on capabilities and preparedness of that same Member State;

[47] **AM 79:** ***3a. (new) The cooperation network shall publish a report once a year, based on the activities of the network and on the summary report submitted in accordance with Article 14(4) of this Directive, for the preceding 12 months.***

d. At the request of a Member State discuss the national NIS strategy of that same Member State;

e. At the request of a Member State discuss the effectiveness of the CERT of that same Member State

f. Exchange information and best practice on awareness raising and training.

g. Exchange information and best practice on research and development ~~**within**~~ **on network and information** ~~**cyber**~~ security ~~**and discuss links to Horizon 2020**~~.

h. With representatives from the relevant European Standards Organisations, discuss the~~list of~~ standards ~~drawn up under~~ **referred to** in Article 16.

i. **Collect best practice information on risks and ina~~e~~cidents affecting network and information systems** ~~Consult~~ and, where appropriate, exchange relevant **unrestricted** ~~**non-confidential**~~ information with ~~market~~ operators with respect to the risks and incidents affecting their network and information systems;

j. In collaboration with ENISA, agree a roadmap for NIS exercises, education programmes and training.

4. As input to the Commission's periodic review of the functioning of this Directive, the cooperation group shall produce a report on the experience gained with the strategic cooperation pursued under this Directive.

~~4. The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between competent authorities and the Commission referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the consultation procedure referred to in Article 19(2).~~[48]

5. The Commission shall adopt, 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(2).

Article 8b

CERTs network

1. In order to contribute to developing confidence and trust between the Member States and to **promote** swift, effective operational cooperation **in the fields referred to in Article 3(8)**, a network of the national CERTs is hereby established.

2. The CERTs network shall be composed of representatives from the national CERTs, the European Network and Information Security Agency ("ENISA") and CERT-EU. The Commission shall have an observer role **and provide secretariat functions.**

3. The CERTs network shall have the following tasks:

   a. Exchange high-level information on CERTs services, operations and cooperation capabilities.

[48] **AM 80:** 4. The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between ***single points of contact,*** the Commission ***and ENISA*** referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the ***examination*** procedure referred to in Article 19(***3***).

b. At the **request** of **any ~~the~~** Member State **~~where the incident was first reported~~**, exchange and discuss non-**commercially sensitive ~~confidential~~** information **related to ~~about~~** on-going incidents ~~at the discretion of the Member State where the incident was first reported.~~

c. Exchange and publish anonymised information on **~~historic~~** incidents**, which occurred in the past**.

d. At the request of a Member State discuss and, where possible, identify a coordinated response to an incident that has been identified within the jurisdiction of that same Member State.

e. Assist each other in cross-border incidents on the basis of voluntary mutual assistance.

4. As input to the Commission's periodic review of the functioning of this Directive, the CERTs network shall produce a report on the experience gained with the operational cooperation pursued under this Directive.

5. The Commission shall adopt, by means of implementing acts, procedural arrangements necessary for the functioning of the network of the national CERTs. Those implementing acts shall be adopted in accordance with the **examination** procedure referred to in Article 19(2).

~~[*Article 9*~~

~~Secure information-sharing system~~

~~1. The … infrastructure.~~

~~[49]~~

~~2. The Commission …, regarding:~~

~~(a) the availability …, and~~

~~(b) the existence … Article 7(3).~~

~~[50]~~

~~3. The Commission … Article 19(3).]~~[51]

[49] **AM 81:** ***1a. (new) Participants to the secure infrastructure shall comply with, inter alia, appropriate confidentiality and security measures in accordance with Directive 95/46/EC and Regulation (EC) No 45/2001 at all steps of the processing.***

[50] **AM 82: 9(2)** ***deleted***

[51] **AM 83:** 3. The Commission shall adopt, by means of ***delegated*** acts, ***a common set of interconnection and security standards that single points of contact are to meet before exchanging sensitive and confidential information across the cooperation network***.

~~[*Article 10*~~

~~Early warnings~~

~~1. The competent … conditions:~~[52]

~~(a) they grow rapidly or may grow rapidly in scale;~~

~~(b) they exceed or may exceed national response capacity;~~[53]

~~(c) they affect or may affect more than one Member State.~~[54]

~~2. In the early … incident.~~[55]

~~3. At the request … incident.~~[56]

4. ~~Where the risk … within Europol.~~[57]

[52] **AM 84:** 1. The ***single points of contact*** or the Commission shall provide early warnings within the cooperation network on those risks and incidents that fulfil at least one of the following conditions:

[53] **AM 84:** (b) ***the single point of contact assesses that the risk or incident potentially exceeds*** national response capacity;

[54] **AM 84:** (c) ***the single points of contact or the Commission assess that the risk or incident affects*** more than one Member State.

[55] **AM 85:** 2. In the early warnings, the ***single points of contact*** and the Commission shall communicate ***without undue delay*** any relevant information in their possession that may be useful for assessing the risk or incident.

[56] **AM 86:** ***deleted***

[57] **AM 87:** 4. Where the risk or incident subject to an early warning is of a suspected criminal nature ***and where the concerned market operator has reported incidents of a suspected serious criminal nature as referred to in Article 15(4), the Member States*** shall ***ensure that*** the European Cybercrime Centre within Europol ***is informed, where appropriate***.

[58]

[59]

5. ~~The Commission … paragraph 1.~~]

~~[*Article 11*~~

~~Coordinated response~~

~~1. Following … in Article 12.~~[60]

~~2. The various … network.~~]

[58] **AM 88:** ***4a. (new) Members of the cooperation network shall not make public any information received on risks and incidents referred to in paragraph 1 without having received the prior approval of the notifying single point of contact. Furthermore, prior to sharing information in the cooperation network, the notifying single point of contact shall inform the market operator to which the information relates of its intention, and where it considers this appropriate, it shall make the information concerned anonymous.***

[59] **AM 89:** ***4b. (new) Where the risk or incident subject to an early warning is of a suspected severe cross-border technical nature, the single points of contact or the Commission shall inform ENISA.***

[60] **AM 90:** 1. Following an early warning referred to in Article 10 the ***single points of contact*** shall, after assessing the relevant information, agree ***without undue delay*** on a coordinated response in accordance with the Union NIS cooperation plan referred to in Article 12.

~~[*Article 12*~~

~~Union NIS cooperation plan~~

~~1. The Commission … in Article 19(3).~~

~~2. The Union NIS cooperation plan shall provide for:~~

~~(a) for the purposes of Article 10:~~

~~– a definition …authorities,~~[61]

~~– a definition … cooperation network.~~

~~(b) the processes … procedures;~~

~~(c) a roadmap … plan;~~

~~(d) a programme … peer learning;~~

~~(e) a programme … the Member States.~~

~~3. The Union NIS … regularly.]~~[62]

[63]

[61] **AM 91:** – a definition of the format and procedures for the collection and sharing of compatible and comparable information on risks and incidents by the ***single points of contact***,

[62] **AM 92:** 3. The Union NIS cooperation plan shall be adopted no later than one year following the entry into force of this Directive and shall be revised regularly. ***The results of each revision shall be reported to the European Parliament.***

[63] **AM 93:** ***3a. Coherence between the Union NIS cooperation plan and national NIS strategies and cooperation plans, as provided for in Article 5 of this Directive, shall be ensured.***

Article 13

International cooperation

Without prejudice to the possibility for the cooperation network to have informal international cooperation, the Union may conclude international agreements with third countries or international organisations allowing and organizing their participation in some activities of the cooperation group ~~network~~. Such agreement shall take into account the need to ensure adequate protection of the personal data circulating within ~~on~~ the cooperation group ~~network~~.[64]

[65]

[64] **AM 94:** Without prejudice to the possibility for the cooperation network to have informal international cooperation, the Union may conclude international agreements with third countries or international organisations allowing and organizing their participation in some activities of the cooperation network. Such agreement shall take into account the need to ensure adequate protection of the personal data circulating on the cooperation network ***and shall set out the monitoring procedure that must be followed to guarantee the protection of such personal data***. ***The European Parliament shall be informed about the negotiation of the agreements***. ***Any transfer of personal data to recipients located in countries outside the Union shall be conducted in accordance with Articles 25 and 26 of Directive 95/46/EC and Article 9 of Regulation (EC) No 45/2001.***

[65] **AM 95:** ***Article 13a***
Level of criticality of market operators
Member States may determine the level of criticality of market operators, taking into account the specificities of sectors, parameters including the importance of the particular market operator for maintaining a sufficient level of the sectoral service, the number of parties supplied by the market operator, and the time period until the discontinuity of the core services of the market operator has a negative impact on the maintenance of vital economic and societal activities.

CHAPTER IV

SECURITY OF THE NETWORKS AND INFORMATION SYSTEMS OF ~~PUBLIC ADMINISTRATIONS AND MARKET~~ OPERATORS

Article 14

Security requirements and incident notification

1. Member States shall **require** ~~**provide** ensure~~ that ~~**market**~~ operators ~~**and public administrations**~~ take appropriate, sector-specific technical and organisational measures to manage the risks posed to ~~**the security of the**~~ network~~**s**~~ and information **security of** systems which they control and use in their operations. Having regard to the state of the art, these measures shall maintain ~~guarantee~~ a level of **network and information** security appropriate to the risk presented.

1a Member States shall **require** ~~**provide** ensure~~ that ~~market~~ operators take appropriate ~~In particular,~~ measures ~~shall be taken~~ to prevent and minimise the impact of incidents affecting their network and information system on the essential ~~core~~ services they provide and thus ensure the security ~~continuity~~ of the services underpinned by those networks and information systems.[66] .

[66] **AM 96:** 1. Member States shall ensure that market operators take appropriate ***and proportionate*** technical and organisational measures to ***detect and effectively*** manage the risks posed to the security of the networks and information systems which they control and use in their operations. Having regard to the state of the art, ***those*** measures shall ***ensure*** a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting ***the security of*** their network and information ***systems*** on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.

2. Member States shall provide for a reporting scheme pursuant to which ~~ensure that~~ **~~market~~** operators **~~and public administrations~~ shall** notify without undue delay to the competent authority incidents **~~within their territory~~** having a significant impact on the security of the essential ~~core~~ services they provide. **~~In cases where the competent authority assesses that the notified incident grows rapidly in scale, exceeds or may exceed national response capacity and affect or may affect more than one Member State, that competent authority shall provide an early warning within the cooperation group.~~**[67]

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 essential ~~whose core~~** service ~~is affected~~;

(b) the duration of the incident;

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

2b Where essential services in more than one Member State are affected, the single point of contact which has received the notification shall, based on the information provided by the operator, alert the single points of contact of the Member States concerned. The operator shall be informedwithout undue delay, which other single points of contact have been informed of the incident, as well as of any undertaken steps, results and any other information with relevance to the incident.

[68]

[69]

---

[67] **AM 97:** 2. Member States shall ensure that market operators notify ***without undue delay*** to the competent authority ***or to the single point of contact*** incidents having a significant impact on the ***continuity*** of the core services they provide. ***Notification shall not expose the notifying party to increased liability.***
To determine the significance of the impact of an incident, the following parameters shall inter alia be taken into account:

[68] **AM 98: 2*(a)(new) the number of users whose core service is affected;***

[69] **AM 99: 2*(b)(new) the duration of the incident;***

[70]

[71]

[72]

[73]

[74]

3. The requirements under paragraphs 1 to ~~and~~ 2b apply to all ~~market~~ operators providing services within the European Union.

---

[70] **AM 100: 2*(c)(new) geographic spread with regard to the area affected by the incident.***

[71] **AM 101: *2.1a(new) Those parameters shall be further specified in accordance with point (ib) of Article 8(3).***

[72] **AM 102: *2(a)(new) 2a. Market operators shall notify the incidents referred to in paragraphs 1 and 2 to the competent authority or the single point of contact in the Member State where the core service is affected. Where core services in more than one Member State are affected, the single point of contact which has received the notification shall, based on the information provided by the market operator, alert the other single points of contact concerned. The market operator shall be informed, as soon as possible, which other single points of contact have been informed of the incident, as well as of any undertaken steps, results and any other information with relevance to the incident.***

[73] **AM 103: *2b. (new)Where the notification contains personal data, it shall be only disclosed to recipients within the notified competent authority or single point of contact who need to process those data for the performance of their tasks in accordance with data protection rules. The disclosed data shall be limited to what is necessary for the performance of their tasks.***

[74] **AM 104: *2c. (new) Market operators not covered by Annex II may report incidents as specified in Article 14(2) on a voluntary basis.***

4. After consultation between the competent authority and the ~~market~~ operator concerned, ~~The~~ the single point of contact ~~competent authority~~ may inform the public, or require the ~~**market**~~ operators ~~**and public administrations**~~ to do so, about individual incidents, where public awareness is necessary to prevent ~~it determines that disclosure of the~~ an incident or deal with an ongoing incident ~~is in the public interest~~. Once a year, the single point of contact ~~competent authority~~ shall submit an anonymised summary report to the cooperation group ~~network~~ on the notifications received and the action taken in accordance with this paragraph. [75]

[75] **AM 105:** 4. ***After consultation with the notified*** competent authority ***and the market operator concerned, the single point of contact*** may inform the public ***about individual incidents, where it determines that public awareness is necessary to prevent an incident or deal with an ongoing incident, or where that*** market ***operator, subject to an incident, has refused to address a serious structural vulnerability related to that incident without undue delay.***
Before any public disclosure***, the notified competent authority shall ensure that the market operator concerned has the possibility to be heard and that the decision for public disclosure is duly balanced with the public interest***.
Where information about individual incidents is made public, the notified competent authority or the single point of contact shall ensure that it is made as anonymous as possible.
The competent authority or the single point of contact shall, if reasonably possible, provide the market operator concerned with information that supports the effective handling of the notified incident.
Once a year, the ***single point of contact*** shall submit a summary report to the cooperation network on the notifications received***, including the number of notifications and regarding the incident parameters as listed in paragraph 2 of this Article,*** and the action taken in accordance with this paragraph.

[76]

~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 18 concerning the definition of circumstances in which public administrations and market operators are required to notify incidents.~~[77]

[6. ~~Subject to any delegated act adopted under paragraph 5, t~~The competent authorities, **when requested** with the assistance of ENISA, may adopt guidelines ~~and, where necessary, issue instructions~~ concerning the circumstances in which **market** operators ~~**and public administrations**~~ are required to notify incidents.][78]

~~7. The Commission shall be empowered to define, by means of implementing acts, the formats and procedures applicable for the purpose of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).~~

~~**8. Paragraphs 1 to and 2b shall not apply to microenterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.**~~[79]

---

[76] **AM 106:** ***4a. (new) Member States shall encourage market operators to make public incidents involving their business in their financial reports on a voluntary basis.***

[77] **AM 107:** ***deleted***

[78] **AM 108:** 6. ***The competent authorities or the single points of contact*** may adopt guidelines concerning the circumstances in which market operators are required to notify incidents.

[79] **AM 109:** 8. Paragraphs 1 and 2 shall not apply to microenterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises[35], ***unless the microenterprise acts as subsidiary for a market operator as defined in point (b) of Article 3(8)***.
[35] OJ L 124, 20.5.2003, p. 36.

[80]

Article 15

Implementation and enforcement

1. Member States shall ensure that the competent authorities have ~~all~~ the ~~powers~~ necessary means to **assess** ~~investigate~~ the ~~cases of non-~~compliance of ~~**market**~~ operators ~~**and public administrations**~~ with their obligations under Article 14 and the effects thereof on the security of networks and information systems.[81]

2. Member States shall ensure that the competent authorities or the single points of contact have the means ~~power~~ to require ~~**market**~~ operators ~~**and public administrations**~~ to:[82]

   (a) provide information needed to assess the security of their networks and information systems, including documented security policies;

   (b) [undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.][83]

[84]

---

80 **AM 110:** ***8a. (new) Member States may decide to apply this Article and Article 15 to public administrations mutatis mutandis.***

81 **AM 111:** 1. Member States shall ensure that the competent authorities ***and the single points of contact have*** the powers necessary to ***ensure compliance*** of market operators with their obligations under Article 14 and the effects thereof on the security of networks and information systems.

82 **AM 112:** 2. Member States shall ensure that the competent authorities ***and the single points of contact*** have the power to require market operators to:

83 **AM 113:** (b) ***provide evidence of effective implementation of security policies, such as the results of*** a security audit carried out by a qualified independent body or national authority***,*** and make the ***evidence*** available to the competent authority ***or to the single point of contact***.

84 **AM 114: 1a(new)** ***When sending that request, the competent authorities and the single points of contact shall state the purpose of the request and sufficiently specify what information is required.***

3. Following the assessment of information or results of security audits referred to in paragraph 2, ~~Member States shall ensure that~~ the competent authorities ~~have the power to~~ may issue ~~binding~~ instructions to the ~~**market**~~ operators ~~**and public administrations**~~ to remedy their operations.[85]

[86]

~~4. The competent authorities shall notify incidents of a suspected serious criminal nature to law enforcement authorities.~~[87]

5. [The competent authorities shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.][88]

---

[85] **AM 115:** 3. Member States shall ensure that ***the*** competent authorities ***and the single points of contact*** have the power to issue binding instructions to market operators.

[86] **AM 116:** ***3a. By way of derogation from point (b) of paragraph 2 of this Article, Member States may decide that the competent authorities or the single points of contact, as applicable, are to apply a different procedure to particular market operators, based on their level of criticality determined in accordance with Article 13a. In the event that Member States so decide:***
(a) competent authorities or the single points of contact, as applicable, shall have the power to submit a sufficiently specific request to market operators requiring them to provide evidence of effective implementation of security policies, such as the results of a security audit carried out by a qualified internal auditor, and make the evidence available to the competent authority or to the single point of contact;
(b) where necessary, following the submission by the market operator of the request referred to in point (a), the competent authority or the single point of contact may require additional evidence or an additional audit to be carried out by a qualified independent body or national authority.
3b. Member States may decide to reduce the number and intensity of audits for a concerned market operator, where its security audit has indicated compliance with Chapter IV in a consistent manner.

[87] **AM 117:** 4. The competent authorities ***and the single points of contact shall inform the market operators concerned about the possibility of reporting incidents of a suspected serious criminal nature to the*** law enforcement authorities.

[88] **AM 118:** 5. ***Without prejudice to applicable data protection rules the*** competent authorities ***and the single points of contact*** shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches. ***The single points of contact and the data protection authorities shall develop, in cooperation with ENISA, information exchange mechanisms and a single template to be used both for notifications under Article 14(2) of this Directive and other Union law on data protection.***

6. [Member States shall ensure that any obligations imposed on ~~**market**~~ operators ~~**and public administrations**~~ under this Chapter may be subject to judicial review.][89]

[90]

Article 16

Standardisation

1. To promote ~~ensure~~ convergent implementation of Article 14(1) **and 14(1a)** Member States shall, without prejudice to technological neutrality, encourage the use of internationally accepted standards and/or specifications relevant to networks and information security. [91]

[1a. The European Network and Information Security Agency ("ENISA"), in collaboration with Member States, may elaborate recommendations 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.]

~~2. The Commission shall draw up, by means of implementing acts a list of the standards referred to in paragraph 1. The list shall be published in the Official Journal of the European Union.~~ [92]

---

89 **AM 119:** 6. Member States shall ensure that any obligations imposed on market operators under this Chapter may be subject to judicial review.

90 **AM 120:** ***6a.* (new)** ***Member States may decide to apply Article 14 and this Article to public administrations mutatis mutandis.***

91 **AM 121:** 1. To ensure convergent implementation of Article 14(1), Member States***, without prescribing the use of any particular technology,*** shall encourage the use ***of European or international interoperable*** standards and/or specifications relevant to networks and information security.

92 **AM 122:** 2. The Commission shall ***give a mandate to a relevant European standardisation body to***, ***in consultation with relevant stakeholders,*** draw up a list of the standards ***and/or specifications*** referred to in paragraph 1. The list shall be published in the Official Journal of the European Union.

CHAPTER V

FINAL PROVISIONS

Article 17

Sanctions

1. Member States shall lay down rules on sanctions 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 sanctions provided for must be effective, proportionate and dissuasive. [The Member States shall notify those provisions to the Commission by the date of transposition of this Directive at the latest and shall notify it without delay of any subsequent amendment affecting them.]

93

[2. Member states shall ensure that when a security incident involves personal data, the sanctions foreseen are consistent with the sanctions provided by the **[**Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.**]]**

~~*Article 18*~~

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

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

---

93 **AM 123**: ***1a. (new)Member States shall ensure that the penalties referred to in paragraph 1 of this Article only apply where the market operator has failed to fulfil its obligations under Chapter IV with intent or as a result of gross negligence.***

~~2. The power to adopt delegated acts referred to in Articles 9(2), 10(5) and 14(5) shall be conferred on the Commission. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.~~

~~3. The delegation of powers referred to in Articles 9(2), 10(5) and 14(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the powers specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated act already in force.~~ [94]

~~4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.~~

~~5. A delegated act adopted pursuant to Articles 9(2), 10(5) and 14(5) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.~~ [95]

---

[94] **AM 124:** 3. The delegation of ***power*** referred to in ***Article*** 9(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the powers specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated act already in force.

[95] **AM 125:** 5. A delegated act adopted pursuant to ***Article*** 9(2) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 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.

~~[2. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.]~~

~~3~~**2**. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 20

Review

The Commission shall periodically review the functioning of this Directive and report to the European Parliament and the Council. The first report shall be submitted no later than three years after the date of transposition referred to in Article 21**(2).** Thereafter, the Commission shall review the functioning of this Directive every [3] years. For this purpose **and with a view to further enhance the strategic and operational cooperation**, the Commission **shall take into account the reports of the Cooperation Group and the CERTs network on the experience gained at a strategic and operational level. The Commission** may **also** request Member States to provide information without undue delay. [96]

[96] **AM 126:** The Commission shall periodically review the functioning of this Directive***, in particular the list contained in Annex II,*** and report to the European Parliament and the Council. The first report shall be submitted no later than ***three*** years after the date of transposition referred to in Article 21. For this purpose, the Commission may request Member States to provide information without undue delay.

Article 21

Transposition

1. Member States shall adopt and publish, by [two years ~~one year and a half after adoption~~. **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 [two years ~~one year~~ and a half after ~~adoption~~**date of entry into force of this Directive**].

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.

3. Member States **may ~~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 Brussels,

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

ANNEX I

Requirements and tasks of the Computer Security Incident ~~Emergency~~ Response Team (CSI~~E~~RT)[97]

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

(1) Requirements for the CERT

(a) The CERT 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. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.[98]

(b) The CERT shall implement and manage security measures to ensure the confidentiality, integrity, availability and authenticity of information it receives and treats.

(c) The offices of the CERT and the supporting information systems shall be located in secure sites.[99]

(d) A service management quality system shall be created to follow-up on the performance of the CERT and ensure a steady process of improvement. It shall be based on clearly defined metrics that include formal service levels and key performance indicators.

(e) Business continuity:

- The CERT shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers,

- The CERT shall be adequately staffed to ensure availability at all times,

- The CERT shall rely on an infrastructure whose continuity is ensured. To this end, redundant systems and backup working space shall be set up for the CERT to ensure permanent access to the means of communication.

---

97 **AM 127:** Requirements and tasks of the Computer Emergency Response ***Teams (CERTs)***

98 **AM 128:** (a) The ***CERTs*** 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.

99 **AM 129:** (c) The offices of the ***CERTs*** and the supporting information systems shall be located in secure sites ***with secured network information systems.***

(2) Tasks of the CERT

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

- Monitoring incidents at a national level,[100]

- 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,

[- Building broad public awareness of the risks associated with online activities,**]**

[101]

[- Organising campaigns on NIS;**]**

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

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

- incident and risk handling procedures,

- incident, risk and information classification schemes,

- taxonomies for metrics,

- information exchange formats on risks, incidents, and system naming conventions.

---

[100] **AM 130:** – ***Detecting and*** monitoring incidents at a national level,

[101] **AM 131:** ***- Actively participating in Union and international CERT cooperation networks***

ANNEX II

List of ~~market~~ ~~operators~~ types of entities for the purposes of Article 3(8)

~~**Referred to in Article 3(8) a):**~~

0. In the field of information society:

– e-commerce platforms

– Internet payment gateways

– Social networks

– Search engines

– Cloud computing services

– Application stores

~~**Referred to in Article (3(8) b):**~~

1. **In the field of** energy[102]:

- Electricity and gas suppliers[103]
- Electricity and/or gas distribution system operators ~~and retailers for final consumers~~ [104]
- Natural gas transmission system operators, storage operators and LNG operators
- Transmission system operators in electricity[105]

[102] **AM 133:** 1. Energy
(a) Electricity

[103] **AM 133: -** Suppliers

[104] **AM 133: -** Distribution system operators and retailers for final consumers

[105] **AM 133:** - Transmission system operators in electricity
(b) Oil

- Oil transmission pipelines and oil storage[106]

- [Electricity and gas market operators] [107]

- Operators of oil and natural gas production, refining and treatment facilities[108]

2. **In the field of** transport :

- Air carriers (freight and passenger air transport)[109]

- Maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies)[110]

- Railways (infrastructure managers, integrated companies and railway transport operators) [111]

- Airports [112]

- Ports[113]

---

[106] **AM 133:** - Oil transmission pipelines and oil storage
- Operators of oil production, refining and treatment facilities, storage and transmission
(c) Gas

[107] **AM 133:** ***- Suppliers***
- Distribution system operators and retailers for final consumers
- Natural gas transmission system operators, storage system operators and LNG system operators

[108] **AM 133:** - Operators of natural gas production, refining, treatment facilities, ***storage*** facilities ***and transmission***
- Gas market operators

[109] **AM 134:** ***(a) Road transport***

[110] **AM 134:** ***(i) Traffic management control operators***

[111] **AM 134:** ***(ii) Auxiliary logistics services:***

[112] **AM 134:** ***- warehousing and storage,***

[113] **AM 134:** ***- cargo handling, and***

- Traffic management control operators[114]

- Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation support activities) [115]

[116]

3. **In the field of** banking: credit institutions in accordance with Article 4.1 of Directive 2006/48/CE.

4. **In the field of** financial market infrastructures: stock exchanges and central counterparty clearing houses[117]

5. **In the field of** health sector: health care settings (including hospitals and private clinics) and other entities involved in health care provision.

---

[114] **AM 134: -** ***other transportation support activities***

[115] **AM 134:** ***(b) Rail transport***

[116] **AM 134:** ***(i) Railways (infrastructure managers, integrated companies and railway transport operators)***
(ii) Traffic management control operators
(iii) Auxiliary logistics services:
- warehousing and storage,
- cargo handling, and
- other transportation support activities
(c) Air transport
(i) Air carriers (freight and passenger air transport)
(ii) Airports
(iii) Traffic management control operators
(iv) Auxiliary logistics services:
- warehousing,
- cargo handling, and
- other transportation support activities
(d) Maritime transport
(i) Maritime carriers (inland, sea and coastal passenger water transport companies and inland, sea and coastal freight water transport companies)

[117] **AM 135:** 4. Financial market infrastructures: ***regulated markets, multilateral trading facilities, organised trading facilities*** and central counterparty clearing houses

6. In the field of water supply: [types of entities to be further considered].

[118]

[119]

[120]

---

[118] **AM 136**: *5a. Water production and supply*
[119] **AM 137**: *5b. Food supply chain*
[120] **AM 138**: *5c. Internet exchange points*