Council of the European Union

Brussels, 5 March 2015
(OR. en)

6788/15

Interinstitutional File:
2013/0027 (COD)

LIMITE

TELECOM 59
DATAPROTECT 23
CYBER 13
MI 139
CSC 55
CODEC 279

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	6439/15 TELECOM 45 DATAPROTECT 20 CYBER 9 MI 103 CSC 42 CODEC 229
No. Cion doc.:	6342/13 TELECOM 24 DATAPEOTECT 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 - Examination of amended Presidency consolidated text

1. Following the examination by the WP TELE of all provisions of the above mentioned proposal, as contained in docs. 5257/15, 6372/15 and 6439/15, the Presidency has put together the annexed 5-column document. The 5th column of the annex ("proposed Council position") should be seen as reflecting the results of the discussions in the various meetings of the WP TELE and of the written comments from delegations.

2. As compared to doc. 6439/15, the following changes have been made:

   – Article 1:

      a) 1(2)a: last part of the paragraph has been replaced with "…to adopt a national NIS strategy".

b) 1(2)b: "and develop confidence and trust has been added"

c) 1(4): references to "EU laws on cybercrime" have been inserted.

d) 1(7): "and for the notification of incidents" has been added.

– Article 3:

a) 3(7): the definition of "incident handling" has been re-inserted.

b) 3(8): brackets have been removed.

c) 3(8), 2nd indent: "having" has been replaced by "may have".

d) 3(8), 2nd subparagraph: "potential" has been inserted before "disruptive".

– Article 5(2a): an appropriate reference to ENISA has been accommodated.

– Article 6:

a) 6(2a): "one or more" has been inserted before "national single points of contact" and text has been added to this paragraph ("Where…contact").

b) 6(3): "relevant has been inserted before "competent authorities" and "via" has been replaced with "in".

c) 6(4): "and single points of contact" has been removed.

d) 6(4a): the last part of the paragraph ("At the request of the competent authority, the single point of contact shall forward notifications referred to in the first subparagraph to single points of contact in other affected Member States.") has been tentatively moved to Article 14(2ac), in which context it should be discussed further.

– Article 7

a) 7(1a): the sentence "To the extent necessary to fulfil its tasks, CSIRTs may be granted access to data on incidents notified by operators pursuant to Article 14(2)" has ben removed as already covered by Article 14(2).

b) 7(3): "the designated" has been inserted before "CSIRTs".

c) 7(5c): an appropriate reference to ENISA has been accommodated.

– Article 8a:

a) 8a(1): the wording has been amended for the sake of consistency ("…with a view to achieving a high common level of security of networks and information systems in the Union…").

b) 8a(3)e : the text has been been changed from "Discuss capabilities and preparedness of the Member States, including national strategies of Member States and the effectiveness of the CSIRTs and identify best practices" into "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." As a consequence, the following two paragraphs have been deleted.

c) 8a(3)j: the second part of this paragraph has been deleted;

– Article 8b:

a) 8b(1): the sentence "It shall begin perfoming the tasks under paragraph 3 by [6 months] after the date of entry into force of this Directive" has been removed as it is addressed in Article 20a.

b) 8b(3)c: the text has been changed from "Regularly exchange, and where appropriate, such as in order to raise awareness, publish on a voluntary basis non-confidential information on individual incidents" into "Exchange and make available on a voluntary basis non-confidential information on individual incidents."

c) 8b(3)d: the text has been changed from "At the request of a CSIRT of a Member State discuss…" into "At the request of the representative of the Member State's CSIRT, discuss…".

d) 8b(3)f: "explore" has been inserted before "discuss.

– Article 14:

a) 14(1a) has been changed from "Member States shall ensure that operators take appropriate measures to prevent and minimise the impact of incidents affecting the security of networks and information systems underpinning the essential services they provide and thus ensure the continuity of those services" into "Member States shall ensure that operators take appropriate measures to prevent and minimise the impact of incidents affecting security of the networks and information systems used for the provision of essential services and thus to ensure the continuity of those services."

b) 14(2): the wording on the scope of the notification obligation has been clarified. The sentence "Notifications shall include information to enable the competent authority to determine the significance of any cross-border impact" has been deleted from this paragraph.

c) 14(2ab): the last sentence of this paragraph has been moved to 14(2ac) and the rest of the paragraph has been deleted.

d) 14(2ac): the last sentence of 14(2ab) has been added and text from 6(4a) has been included and should be discussed further.

e) 14(3): "…a Member State…" has been replaced by "…the Union…".

f) 14(4): "…require the operators to do so…" has been re-instated.

– Article 15:

a) 15(2)b: brackets have been removed.

b) 15(3): the word "binding" has been re-instated.

– Article 20a: a new article on "transitional measures" has been introduced.

– Annex II: the Council's position in the previous Coreper mandate has been re-inserted for as far as parts 0. and 0.1 are concerned and the brackets in these parts have all been removed.

3. Following the meeting of the WP TELE on Friday 6 March, at which occasion delegations will be invited to indicate their positions on the above mentioned changes to the text in the 5th column of the annexed document. In view of the Coreper meeting of 11 March, the Presidency will prepare a draft Coreper mandate in the usual format, i.e. a cover Note with an annexed 4-column document, taking into account the results of the discussions in the WP TELE meeting of 6 March.

ANNEX

Proposal for a
Directive of the European Parliament and of the Council
concerning measures **with a view** to **achieving** ~~ensure~~ a high common level of network and information security across the Union

COMMISSION	**EP**	**COUNCIL**	**SUGGESTED COMPROMISE SOLUTIONS**	**PROPOSED COUNCIL POSITION**
Article 1	*Article 1*	*Article 1*		*Article 1*
Subject matter and scope	Subject matter and scope	Subject matter and scope	Subject matter and scope	Subject matter and scope
1. This Directive lays down measures to ensure a high common level of network and information security (hereinafter referred to as "NIS") within the Union.		1. This Directive lays down measures to **seek to achieve and maintain** ~~ensure~~ 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**	**1. The wording "seek to achieve and maintain"** is under discussion with the EP. This wording must be consistent throughout the text (for example, in art. 5(1) and art. 8a (1))	1. This Directive lays down measures **with a view** to **achieving** ~~ensure~~ a high common level of **security of** network**s** and information **systems** ~~security~~ (hereinafter referred to as "NIS") within the Union **so as to improve the functioning of the internal market.**

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
1. To that end, this Directive:		2. To that end, this Directive:		2. To that end, this Directive:
(a) lays down obligations for all Member States concerning the prevention, the handling of and the response to risks and incidents affecting networks and information systems;		(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;	The term "serious" is under discussion with the EP	(a) lays down obligations for all Member States **to adopt a national NIS strategy** ~~concerning the prevention, the handling of and the response to **serious** risks and incidents affecting networks and information systems~~;
(a) 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 and efficient handling of and response to risks and incidents affecting network and information systems;	(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**,** ~~and~~ efficient ***and effective*** handling of and response to risks and incidents affecting network and information systems ***with the participation of relevant stakeholders***; (AM 40)	(b) creates a cooperation **group** ~~mechanism~~ between Member States in order to **support and facilitate strategic cooperation and the exchange of information among Member States** ~~ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems~~;	Provision to be aligned with art. 8a(1) after the agreement on the latter article	(b) creates a cooperation **group** ~~mechanism between Member States~~ in order to **support and facilitate strategic cooperation and the exchange of information among Member States and develop trust and confidence** ~~ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems~~;

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
		ba) creates a CSIRTs ("Computer Security Incident Response Team") network in order to contribute to developing confidence and trust between Member States and to promote swift, effective operational cooperation;	Provision to be aligned with art. 8b(1) after the agreement on the latter article. The EP is still considering the terminology " CSIRT/CERT". The term agreed between co-legislators must be consistent throughout the text	**ba) creates a CSIRTs ("Computer Security Incident Response Team") network in order to contribute to developing confidence and trust between Member States and to promote swift, effective operational cooperation**;
(b) establishes security requirements for market operators and public administrations.	(c) establishes security requirements for market operators. ~~and public administrations.~~ (AM 41)	(c) establishes security **and notification** requirements for ~~market~~ operators ~~and public administrations~~.	Provision to be aligned with the title of art. 14	(c) establishes security **and notification** requirements for ~~market~~ operators ~~and public administrations~~.
		d) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs concerned with the security of network and information systems.	Provision to be aligned with art. 6-7 after the agreement on those provisions.	**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.**

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
2. The security 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 Articles 13a and 13b of that Directive, nor to trust service providers.		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 ~~that~~ Directive **2002/21/EC**, nor to trust service providers **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.**		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 ~~that~~ Directive **2002/21/EC**, nor to trust service providers **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.**

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
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[1]		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.[2]	positions of co-legislators are identical	4. This Directive shall be without prejudice to **Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011on combating the sexual abuse and sexual exploitation of children and child pornography,** ~~EU laws on cybercrime and~~ **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.[3]

1 OJ L 345, 23.12.2008, p. 75.
2 OJ L 345, 23.12.2008, p. 75.
3 OJ L 345, 23.12.2008, p. 75.

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
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[4], 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[5].	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***	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[6], 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].[7].	**EP proposal (in conjunction with Art 1a)**: 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	

4 OJ L 281 , 23/11/1995 p. 31.
5 SEC(2012) 72 final.
6 OJ L 281 , 23/11/1995 p. 31.
7 SEC(2012) 72 final.

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
	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.*** (AM 42)		processing of personal data ***by the Community institutions and bodies*** and on the free movement of such data.	

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
6. The sharing of information within the cooperation network under Chapter III and the notifications of NIS incidents under Article 14 may require the processing of personal data. Such processing, which is necessary to meet the objectives of public interest pursued by this Directive, shall 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.		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 necessary to meet the objectives of public interest pursued by this Directive, shall ~~be authorised by the Member States pursuant to Article 7 of~~ **be carried out in accordance with** Directive 95/46/EC and Directive 2002/58//EC, as implemented in national law. **Such processing is a legitimate processing within the meaning of Article 7 of Directive 95/46/EC.**	**EP proposal (to be read in conjunction with Art 1a)**: deleted	Note: moved to Article 1a(3a).
		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	The final wording of this provision is still under consideration in the Council.	Note: the wording of this provision shall be finalised pending further information from the Commission on professional secrecy. **6a. Without prejudice to Article 346 TFEU, information that is**

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
		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.		**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.**
		6b. This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular their national security, or to protect information the disclosure of which they consider contrary to the essential interests of their security. The provisions of this Directive shall be without prejudice to a Member State's sovereign	The final wording of this provision is still under consideration in the Council.	**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,**

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
		competence in ensuring 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.		**detection and prosecution of criminal offences.**
		[7. If a sector specific Union legal act contains security and notification requirements covering network and information security, the provisions of that sector specific Union legal act shall apply instead of Article 14 of this Directive.]	The final wording of this provision is still under consideration in the Council.	Note: the wording of this provision shall be finalised pending further information from the Commission on NIS requirements in sector-specific legislation. **7. If a sector specific Union legal act contains requirements for security of networks and information systems and for the notification of incidents, the provisions of that sector specific Union legal act shall apply instead of Article 14 of this Directive.**

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
	Article 1a ***Protection and processing of personal data***		**EP proposal:** ***Article 1a*** ***Protection and processing of personal data***	***Article 1a*** ***Protection and processing of personal data***
			EP proposal : ***-1. Data processed pursuant to this Directive shall if possible be kept anonymous.***	
	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.		**EP proposal :** ***1. Processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC [and Directive 2002/58/EC].***	**1. Processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/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.		**EP proposal :** ***2. Processing of personal data by Union institutions and bodies pursuant to this Directive shall be carried out***	**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.**

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
			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.		**EP proposal :** **delete**	
			EP proposal: ***3a. Processing of personal data which is necessary to meet the objectives of public interest pursued by this Directive shall be deemed to be legitimate processing within the meaning of Article 7(e) of Directive 95/46/EC.***	**3a. Processing of personal data which is necessary to meet the objectives of public interest pursued by this Directive shall be deemed to be legitimate processing within the meaning of Article 7(e) of Directive 95/46/EC.**

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
	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.		**EP proposal :** ***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. (AM 43)		**EP proposal:** ***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.***	

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
Article 2	*Article 2*	*[Article 2*		*Article 2*
Minimum harmonisation	Minimum harmonisation	Minimum harmonisation		Minimum harmonisation
Member States shall not be prevented from adopting or maintaining provisions ensuring a higher level of security, without prejudice to their obligations under Union law.		Member States shall not be prevented from adopting or maintaining provisions **seeking to achieve and maintain** ~~ensuring~~ a higher level of **network and information** security, without prejudice to their obligations under Union law.		Member States shall not be prevented from adopting or maintaining provisions **with a view to achieving** ~~ensure~~ a higher level of security **of networks and information systems**, without prejudice to their obligations under Union law.

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
Article 3	*Article 3*	*Article 3*		*Article 3*
Definitions	Definitions	Definitions		Definitions
For the purpose of this Directive, the following definitions shall apply:		For the purpose of this Directive, the following definitions shall apply:		For the purpose of this Directive, the following definitions shall apply:
(1) "network and information system" means:		(1) "network and information system" means:		(1) "network and information system" means:
(a) an electronic communications network within the meaning of Directive 2002/21/EC, and		(a) an electronic communications network within the meaning of **point (a) of Article 2 of** Directive 2002/21/EC, and		(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	(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~~ ***digital*** data, as well as (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 computer data, as well	The expressions “digital data”/ “computer data” are under discussions with the EP	(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** ~~computer~~ data, as well

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
(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.	c) ~~computer~~ ***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. (AM 45)	(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.	The expressions “digital data”/ “computer data” are under discussions with the EP	c) **digital** ~~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.
(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;	(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*** (AM 46)	(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;		(2) "security **of networks and information systems**" means the ability of ~~a~~ network**s** and information system**s** 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 **or processed** data or the related services offered by or accessible via that network and information system**s**;

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
		2a) "essential services" means services essential for the maintenance of critical societal and economic activities.		**2a) "essential services" are services indispensable for the maintenance of critical societal and economic activities**.
(1) "risk" means any circumstance or event having a potential adverse effect on security;	(3) 'risk' means any ***reasonably identifiable*** circumstance or event having a potential adverse effect on security; (AM 47)	(3) "risk" means any circumstance or event having a potential **serious or actual** adverse effect on **network and information** security;	Provision to be discussed in conjunction with point (4) of Article 3	(3) "risk" means any circumstance or event having a potential adverse effect on the security **of networks and information systems**;
(2) "incident" means any circumstance or event having an actual adverse effect on security;	(4) 'incident' means any ~~circumstance or~~ event having an actual adverse effect on security; (AM 48)	(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 of essential services;**		(4) "incident" means any circumstance or event having an actual adverse effect on **the** security **of networks and information systems;**
(5) "information society service" mean service within the meaning of point (2) of Article 1 of Directive 98/34/EC;	***Deleted*** (AM 49)	deleted	deleted	

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
(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;		deleted	deleted	
		(**6a) "National NIS strategy" means a framework providing high-level vision, objectives and priorities on NIS at national level;**	Provision to be read in conjunction with art. 6	(**6a) "National strategy on the security of networks and informations systems ("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;	(7) 'incident handling' means all procedures supporting the ***detection, prevention***, analysis, containment and response to an incident; (AM 50)	(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;	Discussions with the EP on the need to keep the words "detection" and "prevention"	(7) "incident handling" means all procedures supporting the analysis, containment and response to an incident;
(8) "market operator" means:		(8) ~~"market operator" means:~~		

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
(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;	***Deleted*** (AM 51)	deleted	deleted	
(b) operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a non exhaustive list of which is set out in Annex II.	(b) operator of ~~critical~~ infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, ~~stock exchanges~~ ***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)~~ operator **means a public or private entity referred to** in Annex II**, which provides an** essential service in the fields of ~~critical~~ **Internet** infrastructure **and digital service platforms,** ~~that are essential for the maintenance of vital economic and societal activities in the fields of~~ energy, transport, banking, stock exchanges and health, **and water supply and which fulfills all of the following criteria** ~~a non exhaustive list of which is set out in Annex II~~.		**(8) Operator means a public or private entity the type of which is referred to in Annex II, which provides an essential service in the fields of Internet infrastructure and digital service platforms, energy, transport, banking, financial market infrastructures, health and drinking water and which fulfils all of the following criteria:**

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
	(AM 52)			
		- the service depends heavily on network and information systems;		**- the service depends on network and information systems;**
		- an incident to the network and information systems of the service having serious disruptive effects on the provision of that essential service or on public safety.		**- an incident to the network and information systems of the service may have significant disruptive effects on the provision of that essential service or on public safety.**
				Each Member State shall identify the entities, which meet the above definition of operator.

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
		[In addition to the above criteria, entities in the field of digital service platforms shall also fulfil the criterion that a large number of market participants rely on the entity for their trading/economic activities.]		**When determining the significance of a potential disruptive effect, the Member State shall take into account the following factors:**
				- the importance of the particular entity for the provision of the essential service in the sector;
				- the number of users relying on the services provided by the entity;

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
				- the impact on economic and societal activities or public safety where the availability, authenticity, integrity or confidentiality of the service provided by the entity has been compromised, including assessment of the time period before discontinuity would create a negative impact.
		Each Member State shall identify on its territory entities, which meet the above definition of operator.		
	(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; (AM 53)			

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
(9) "standard" means a standard referred to in Regulation (EU) No 1025/2012;		(9) "standard" means a standard referred to in **point (1) of Article 2** of Regulation (EU) No 1025/2012;		(9) "standard" means a standard referred to in **point (1) of Article 2** of Regulation (EU) No 1025/2012;
(10) "specification" means a specification referred to in 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;		(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 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.		(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~~.		(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~~.

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
	(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).*** (AM 54)		Provision linked to the discussion on Annex II	Note: the wording of this provision shall be finalised pending further information from the Commission on NIS requirements in sector-specific legislation (point 4 of Annex II).
	(11b) 'multilateral trading facility (MTF)' means multilateral trading facility as defined in point 15 of Article 4 of Directive 2004/39/EC; (AM 55)		Provision linked to the discussion on Annex II	Note: the wording of this provision shall be finalised pending further information from the Commission on NIS requirements in sector-specific legislation (point 4 of Annex II).

COMMISSION	EP	COUNCIL	SUGGESTED COMPROMISE SOLUTIONS	PROPOSED COUNCIL POSITION
	(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; (AM 56)		Provision linked to the discussion on Annex II	Note: the wording of this provision shall be finalised pending further information from the Commission on NIS requirements in sector-specific legislation (point 4 of Annex II).

Article 4		~~*Article 4*~~		*Article 4*
Principle		~~Principle~~		Principle
Member States shall ensure a high level of security of the network and information systems in their territories in accordance with this Directive.	Deleted	Deleted	Deleted	Deleted

Article 5	*Article 5*	*Article 5*		*Article 5*
National NIS strategy and national NIS cooperation plan	National NIS strategy and national NIS cooperation plan	National NIS strategy ~~and national NIS cooperation plan~~	National NIS strategy	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 achieve and maintain a high level of network and information security. The national NIS strategy shall address in particular the following issues:		1. Each Member State shall adopt a national NIS strategy defining the strategic objectives and concrete policy and regulatory measures to **seek to** 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:	1. Each Member State shall adopt a national NIS strategy defining the strategic objectives and concrete policy and regulatory measures to [**seek to** 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:	1. Each Member State shall adopt a national NIS strategy defining the strategic objectives and concrete policy and regulatory measures **with a view** to achieve**ing** and maintain**ing**-a high level of **security of** networks and information **systems** ~~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 objectives and priorities of the strategy based on an up-to-date risk and incident analysis;		(a) ~~The definition of the~~ **The** objectives and priorities **of the national NIS strategy** ~~based on an up-to-date risk and incident analysis~~;	(a) ~~The definition of the~~ ***The*** objectives and priorities ***of the national NIS strategy*** ~~based on an up-to-date risk and incident analysis~~;	(a) The ~~definition of the~~ objectives and priorities of the **national NIS** strategy ~~based on an up-to-date risk and incident analysis~~;

(b) A governance framework to achieve the strategy objectives and priorities, including a clear definition of the roles and responsibilities of the government bodies and the other relevant actors;		[(b) **The** ~~A~~ governance framework **put in place** to achieve 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~~;]	(b) A governance framework to achieve 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;	(b) A governance framework to achieve 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;		(c) The identification of the general measures on preparedness, response and recovery [, including cooperation mechanisms between the public and private sectors];	(c) The identification of the general measures on preparedness, response and recovery, including ~~cooperation mechanisms between~~ ***those taken jointly by*** the public and private sectors;	(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;		(d) An indication of the education, awareness raising and training programmes **relating to the NIS strategy**;	(d) An indication of the education, awareness raising and training programmes ***relating to the NIS strategy***;	(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.		~~(e) Research and development plans and a description of how these plans reflect the identified priorities.~~	(e) ***An indication of the research*** ~~Research~~ and development plans ***relating to the NIS strategy*** ~~and a description of how these plans reflect the identified priorities~~;	(e) **An indication of the r**esearch-and development plans **relating to the NIS strategy** ~~and a description of how these plans reflect the identified priorities~~;
	(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. (AM 57)		Moved – see Art 5(2a new) below	

2. The national NIS strategy shall include a national NIS cooperation plan complying at least with the following requirements		deleted	deleted	
(a) A risk assessment plan to identify risks and assess the impacts of potential incidents;	a) A risk ~~assessment plan to identify risks and assess~~ ***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***; (AM 58)	(f) A risk assessment plan to identify potential risks ~~and assess the impacts of potential incidents~~;	**EP proposal**: ***(f)*** A risk ~~assessment plan to identify~~ ***management framework to establish methodology for the identification, prioritisation, evaluation , prevention and treatment of*** risks and ~~assess~~ the impacts of potential incidents;	(f) A risk assessment plan to identify **possible** risks ~~and assess the impacts of potential incidents~~;
(b) The definition of the roles and responsibilities of the various actors involved in the implementation of the plan;	(b) The definition of the roles and responsibilities of the various ***authorities and other*** actors involved in the implementation of the ~~plan~~ ***framework***; (AM 59)	(g) ~~The definition of the roles and responsibilities~~ **A list** of the various actors involved in the implementation of the **NIS strategy** ~~plan~~;	(g) ~~The definition of the roles and responsibilities~~ ***A list*** of the various actors involved in the implementation of the ***NIS strategy*** ~~plan~~;	(g) ~~The definition of the roles and responsibilities~~ **A list** of the various actors involved in the implementation of the **NIS strategy** ~~plan~~;

(c) The definition of cooperation and communication processes ensuring prevention, detection, response, repair and recovery, and modulated according to the alert level;		deleted	deleted	
(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.		deleted	deleted	
			2a. Member States may request the assistance of ENISA in developing their national NIS strategies.	**2a. Member States may request the assistance of ENISA in developing national NIS strategies. For the purposes of this paragraph, ENISA shall act within the limits of its mandate set out in Articles 2 and 3 of Regulation 526/2013.**
3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within one month from their adoption.	3. The national NIS strategy and the national NIS cooperation plan shall be communicated to the Commission within ~~one month~~ ***three months*** from their adoption. (AM 60)	3. ~~and the national NIS cooperation plan shall be communicated to the Commission within one month from their adoption~~.	**EP proposal**: 3. The national NIS strategy ~~and the national NIS cooperation plan~~ shall be communicated to the Commission within ~~one month~~ ***three months*** from their adoption.	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~~

			Council possible compromise: 3. The ***Member States shall make available to the Commission, within three months from the adoption of their national NIS strategy, at least the elements of the strategy covering points (a) to (f) of paragraph 1.***	within ~~one month~~ **three** month**s** from their adoption.

Article 6	*Article 6*	*Article 6*	*Article 6*	*Article 6*
National competent authority on the security of network and information systems	National competent ~~authority~~ ***authorities and single points of contact*** on the security of network and information systems (AM 61)	**National competent authorities~~y~~ and single point of contact ~~on the security of network and information systems~~**	**National competent authorit*ies~~y~~* *and single point of contact* ~~on the security of network and information systems~~**	**National competent authorities~~y~~ and single point of contact**
1. Each Member State shall designate a national competent authority on the security of network and information systems (the "competent authority").	1. Each Member State shall designate ~~a~~ ***one or more civilian*** national competent ~~authority~~ ***authorities*** on the security of network and information systems (***hereinafter referred to as*** ~~the~~ 'competent authority***/ies***'). (AM 62)	1. Each Member State shall designate **one or more** ~~a~~ national competent authorit**ies**~~y~~ on the security of network and information systems (the "competent authority"). **Member States may designate this role to an existing authority or authorities**	**EP proposal:** 1. Each Member State shall designate ***one or more*** ~~a~~ national competent authorit***ies***~~y~~ ***which do not fulfil any tasks in the field of intelligence, law enforcement or defence and are not organisationally linked in any form to bodies active in those fields,*** .on the security of network and information systems (the "competent authority"). ***Member States may designate this role to an existing authority or authorities.***	1. Each Member State shall designate **one or more** ~~a~~ national competent authorit**ies**~~y~~ on the security of network and information systems (the "competent authority"). **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 and contribute to its consistent application throughout the Union.		deleted	[2. The competent authorities shall monitor the application of this Directive at national level and contribute to its consistent application throughout the Union.]	2. The competent authorities shall monitor the application of this Directive at national level ~~and contribute to its consistent application throughout the Union~~.

	2a. 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. (AM 63)	**2a. Member States shall designate a national single point of contact on network and information security ("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.**	**EP Proposal:** ***2a. Each Member States shall designate a national single point of contact on network and information security ("single point of contact"), which does not fulfil any tasks in the field of intelligence, law enforcement or defence and are not organisationally linked in any form to bodies active in those fields, Member States may designate this role to an existing authority.***	**2a. Each Member State shall designate one or more national single points 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.**
	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. (AM 64)	**[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.]**	***[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.]***	[covered in 7(1a)]

	2c. The single point of contact shall ensure cross-border cooperation with other single points of contact. (AM 65)			**2c. With a view to the transparent functioning of the cooperation group and the CSIRTs network, the single point of contact shall exercise a liaison function between its Member State and the cooperation group and the CSIRTs network.**
			[2c (new). The single point of contact shall ensure that the relevant designated competent authorities participate in the work of the cooperation group referred to in Article 8a.]	

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 via the network referred to in Article 8.	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 ~~competent authorities~~ ***single points of contact*** via the network referred to in Article 8. (AM 66)	[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 via the ~~network~~ group referred to in Article 8**a**.]	**EP proposal** : 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 ***that*** ~~the~~ effective, efficient and secure cooperation ***between*** ~~of~~ the ***single points of contact takes place*** via the ~~network~~ ***cooperation group*** referred to in Article 8***a***.	3. Member States shall ensure that the **relevant** 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 competent authorities via~~ **in** the ~~network~~ **cooperation group and the CSIRTs network** referred to in Articles 8**a and 8b**.
4. Member States shall ensure that the competent authorities receive the notifications of incidents from public administrations and market operators as specified under Article 14(2) and are granted the implementation and enforcement powers referred to under Article 15.	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 ~~public administrations and~~ market operators as specified under Article 14(2) and are granted the implementation and enforcement powers referred to under Article 15 (AM 67)	deleted	**EP proposal** : 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~~.	4. Member States shall ensure that the competent authorities receive the notifications of incidents from ~~market~~ operators as specified under Article 14(2) **and 14(2ac)** ~~and are granted the implementation and enforcement powers referred to under Article 15~~.

			EP proposal: ***4a (new) Member States shall ensure that the competent authorities and the single points of contact forward notifications of incidents under Art 14(2) to the single point of contact of other Member States, where the incident has a significant cross-border impact***	**4a (new) 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 inform the single points of contact about notifications of incidents under Article 14(2) and 14(2ac) where the incident has a significant cross-border impact.**

	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.(AM 68)		**EP proposal** (depends on agreement between co-legislators on art. 1 (7)) ***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 shall be granted the implementation and enforcement powers referred to in 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 the obligations referred to in Article 14 (2) and Article 15.*** ***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, with the relevant law enforcement national authorities and data protection authorities.	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. (AM 69)	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.	5. The competent authorities ***and single points of contact*** shall, ***whenever appropriate and following the procedures laid down in national law,*** consult and cooperate, ~~whenever appropriate,~~ with the relevant ***national*** law enforcement ~~national~~ authorities and data protection authorities.	5. The competent authority~~ies~~ **and single point of contact** shall, **whenever appropriate and in accordance with national legislation,** consult and cooperate, ~~whenever appropriate,~~ with the relevant **national** law enforcement ~~national~~ authorities and data protection authorities.
6. Each Member State shall notify to the Commission without delay the designation of the competent authority, its tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority.	6. Each Member State shall notify to the Commission without delay the designation of the competent ~~authority~~ ***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 ~~authority~~ ***authorities***. (AM 70)	6. Each Member State shall notify to the Commission without delay the designation of the competent authorit**ies**~~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 authorit**ies**~~y~~ **and single point of contact.**	6. Each Member State shall notify to the Commission without delay the designation of the competent authorit***ies***~~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 authorit***ies***~~y~~ ***and single point of contact*****.**	6. Each Member State shall notify to the Commission without delay the designation of the competent authority **and single point of contact, their** ~~its~~ 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.**

Article 7	*Article 7*	*Article 7*	*Article 7*	*Article 7*
Computer Emergency Response Team	Computer Emergency Response Team	**Computer Security Incident ~~Emergency~~ Response Teams**	The EP is still considering the terminology "CSIRT/CERT". The term agreed between co-legislators must be consistent throughout the text	**Computer Security Incident ~~Emergency~~ Response Teams**
1. Each Member State shall set up a Computer Emergency Response Team (hereinafter: "CERT") 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.	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. (AM 71)	1. Each Member State shall **designate one or more** ~~set up a~~ Computer **Security Incident** ~~Emergency~~ Response Teams (hereinafter: "**CSIRTs** ~~CERTs~~") 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 the competent authority.	1. Each Member State shall ***designate one or more [***Computer Emergency Response Team (hereinafter: 'CERT')] ***covering the fields set out 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.	1. Each Member State shall **designate one or more** ~~set up a~~ Computer **Security Incident** ~~Emergency~~ Response Teams (hereinafter: "**CSIRTs** ~~CERTs~~") **covering at least the fields set out 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 **CSIRT** may be established within the competent authority.

		1a. Where they are separate, the competent authorities, 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. To the extent necessary to fulfil its tasks, CSIRTs may be granted access to data on incidents notified by operators pursuant to Article 14(2).	**1a. Where they are separate, the competent authorities, 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. To the extent necessary to fulfil its tasks, [CSIRTs] may be granted access to data on incidents notified by operators pursuant to Article 14(2).**	**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.**
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.		[2. Member States shall ensure that ***CSIRTs*** ~~CERTs~~ have adequate ~~technical, financial and human~~ resources to effectively carry out their tasks set out in point (2) of Annex I.]	**EP proposal** 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. ***Each Member State shall ensure the effective, efficient and secure cooperation of its [CERTs] via the [CERT] network referred to in Article 8b.***	2. Member States shall ensure that **the designated CSIRTs** ~~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 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.		3. Member States shall ensure that ***CSIRTs*** ~~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~~.	**EP proposal:** 3. Member States shall ensure that [***CSIRTs]*** ~~CERTs~~ ***have access to*** ~~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~~.	3. Member States shall ensure that **the designated CSIRTs** ~~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 resources and mandate as well as the incident handling process of the CERTs.		4. Member States shall inform the Commission about the **remit** ~~resources and mandate as well as the incident handling process~~ of the **CSIRTs** ~~CERTs~~.	Member States shall inform the Commission about the ***remit*** ~~resources and mandate~~ **[**as well as the incident handling process**]** of the [**CSIRTs**] ~~CERTs~~.	4. Member States shall inform the Commission about the **remit** ~~resources and mandate as well as the incident handling process~~ of the **CSIRTs** ~~CERTs~~.
GREEN: agreed in principle (5.12.14) Deleted	5. The CERT***s*** shall act under the supervision of the competent authority ***or the single point of contact***, which shall regularly review the adequacy of ~~its~~ ***their*** resources, ~~its~~ ***mandates*** and the effectiveness of ~~its~~ ***their*** incident-handling process. (AM 72)	deleted	deleted	

	5a. Member States shall ensure that CERTs have adequate human and financial resources to actively participate in international, and in particular Union, cooperation networks. (AM 73)		deleted, subject to agreement on Art. 13	
	5b 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. (AM 74)		deleted, subject to agreement on Art. 13	
	AM75 ***5c. Member States may ask for the assistance of ENISA or of other Member States in developing their national CERTs.***		***5c. Member States may ask for the assistance of ENISA or of other Member States in developing their national CERTs.***	**5c. Member States may request the assistance of ENISA in developing national CSIRTs. For the purposes of this paragraph, ENISA shall act within the limits of its mandate set out in Articles 2 and 3 of Regulation 526/2013.**

Article 8	Article 8	~~Article 8~~	Article 8	Article 8
Cooperation network	Cooperation network	**~~Cooperation network~~**		
Replaced by Article 8a				

		Article 8a	***Article 8a***	***Article 8a***
		Cooperation <u>group</u> ~~network~~	**Cooperation <u>*group*</u> ~~network~~**	**Cooperation group ~~network~~**
		<u>1. In order to support and facilitate strategic cooperation and the exchange of information among Member States, a cooperation group is hereby established.</u>	***<u>1. In order to support and facilitate strategic cooperation among Member States [and with the aim of achieving/ to ensure a high common level] of network and information security in the Union, a cooperation group is hereby established. It shall begin performing the tasks under paragraph 3 by [6 months] after the date of entry into force of this Directive.</u>*** ***<u>The cooperation group shall carry out its tasks in accordance with its [annual/ biennial] work programme as referred to in paragraph 3a (new) of Article 8a.</u>***	**1. In order to support and facilitate strategic cooperation among Member States 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 a roadmap as referred to in Article 8a(3a new).**

		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. The Group may invite representatives from the relevant stakeholders to participate in its meetings.	***2. The cooperation group shall be composed of the Member States' [single points of contact], [the Commission and the European Network and Information Security Agency ("ENISA")]. [The single points of contact shall ensure that the relevant designated competent authorities [referred to in Article 6] participate in the work of cooperation group]. Where appropriate, the cooperation group may invite representatives from the relevant stakeholders to participate in its work.*** ***The Commission shall act as the secretariat of the cooperation group.***	**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, the cooperation group may invite representatives from the relevant stakeholders to participate in its work[8].**
		3. The tasks of the cooperation group shall be to:	***3. The cooperation group shall have the following tasks:***	**3. The cooperation group shall have the following tasks:**

[8] Recital to be added to specify what "relevant stakeholders" is deemed to encompass. Include specifically operators and providers of cybersecurity solutions

			a (new). By [insert date, linked to entry into force] and every [two] year[s] thereafter, establish and publish an [annual/ biennial] work programme including actions to be undertaken to implement the objectives and tasks, which shall be consistent with the objectives of this Directive.	**a. By [insert date, linked to entry into force] and every [two] year[s] thereafter, establish a [biennial] roadmap on actions to be undertaken to implement the objectives and tasks, which shall be consistent with the objectives of this Directive[9].**
		a. Provide guidance for the activities of the CSIRTs network established under Article 8b.	***a. Provide strategic guidelines and recommendations on the activities of the [CSIRTs] network established under Article 8b, taking into account the annual assesments referred to in paragraph 3b of Article 8b.***	**b. Provide strategic guidance for the activities of the CSIRTs network established under Article 8b.**

[9] Recital to be added to specify that the work programme should be consistent with the Union's legislative and policy priorities in the area of NIS.

		ab. Exchange best practice on the exchange of information related to incident notification referred to in Article 14(2b).[10]	***ab. Exchange best practice on the exchange of information related to incident notification referred to in Article 14(2b)***[11]***.***	**c. Exchange best practice on the exchange of information related to incident notification referred to in Article 14(2ac)**
			[ab (new) Draw up guidelines for sector-specific criteria for determining the significance of the impact of an incident, as laid down in Article 14 (2)[12]***.]***	

10 This provisions corresponds to Article 8(3)a in the Commission's proposal.

11 COM proposal for a recital: The respective tasks of the Cooperation Group and the European Network and Information Security Agency ("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 526/2013 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 under Article 8a (3)(ab new).

12 COM proposal for a recital: "The NIS public-private platform ("NIS Platform"), launched in 2013 as part of the European Strategy for Cybersecurity, is tasked to identify and develop incentives to adopt good cybersecurity practices and promote the development and the adoption of secure ICT solutions. The NIS Platform will issue voluntary guidance on risk management and information-sharing, including incident notification, which will feed into Commission recommendations on good cybersecurity practices to be adopted in 2015. Member States may use those recommendations to support the process of transposing this Directive into national law, and subsequently to help the organisations concerned to comply with the relevant national provisions. The NIS Platform may also contribute to the development of guidelines for sector-specific criteria for determining the significance of the impact of an incident under Article 8a(ab(new)).

		b. Exchange best practices between Member States and, in collaboration with ENISA, assist Member States in building capacity in NIS;[13]	***b. Exchange best practices between Member States and assist Member States in building capacity in NIS;***	**d. Exchange best practices between Member States and, in collaboration with ENISA, assist Member States 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;[14]	**EP proposal:** ***Discuss capabilities and preparedness of Member States, including national strategies of Member States and the effectiveness of the CSIRTs through regular peer reviews/ and identify best practices on that basis.***	**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.**
		d. At the request of a Member State discuss the national NIS strategy of that same Member State;[15]	***d. At the request of a Member State discuss the national NIS strategy of that same Member State;***	

[13] This provisions corresponds to Article 8(3)g in the Commission's proposal.
[14] This provisions corresponds to Article 8(3)h in the Commission's proposal.
[15] This provisions corresponds to Article 8(3)d in the Commission's proposal.

		e. At the request of a Member State discuss the effectiveness of the CSIRT of that same Member State.[16]	***e. At the request of a Member State discuss the effectiveness of the [CSIRT] of that same Member State.***	
		f. Exchange information and best practice on awareness raising and training.	***f. Exchange information and best practice on awareness raising and training.***	**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	***g. Exchange information and best practice on research and development on network and information security.***	**g. Exchange information and best practice on research and development on network and information security.**

[16] This provisions corresponds to Article 8(3)e in the Commission's proposal.

			EP proposal: ***g (new) Where relevant, cooperate and exchange expertise/experiences on matters concerning NIS, in particular in the fields covered by Annex II/ data protection, energy, transport, banking, financial markets and health with relevant Union bodies/ institutions, bodies, offices and agencies, including the European Cybercrime Centre within Europol and Union data protection authorities.***	**h. Where relevant, exchange experiences on matters concerning NIS with relevant Union bodies, offices and agencies.** 17

17 EP proposal for a recital "To ensure that it fully achieves its objectives, the cooperation group should liaise with relevant bodies, to exchange know-how and best practices and to provide advice on NIS aspects that might have an impact on their work. The cooperation group should aim to achieve synergies between the efforts of those bodies and its own efforts to promote advanced network and information security. In liaising 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."

Possible revision of EP recital by the Council : **In order to promote advanced network and information security** ~~To ensure that it fully achieves its objectives~~, the cooperation group should **cooperate** ~~liaise~~ with relevant **Union institutions**, bodies**, offices and agencies, including the European Cybercrime Centre within Europol and Union data protection authorities**, 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**. ~~The cooperation group should aim to achieve synergies between the efforts of those bodies and its own efforts to promote advanced network and information security~~. **[**In **cooperating** ~~liaising~~ 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.**]**

		h. With representatives from the relevant European Standards Organisations, discuss the standards referred to in Article 16.	***h. Discuss, with representatives from the relevant European Standardisation Organisations, the standards referred to in Article 16.***	**i. Discuss, with representatives from the relevant European Standardisation Organisations, the standards referred to in Article 16.**
		i. Collect best practice information on risks and incidents affecting network and information systems and, where appropriate, exchange relevant unrestricted information with operators with respect to the risks and incidents affecting their network and information systems;	***i. Collect best practice information on risks and incidents affecting network and information systems and, where appropriate, exchange relevant unrestricted information with operators with respect to the risks and incidents affecting their network and information systems;***	**j. Collect best practice information on risks and incidents affecting network and information systems;**
			EP proposal: ***i. (new) Examine on an annual basis the summary reports of the notifications received and the actions taken as referred to in the fifth subparagraph of Article 14 (4). The report shall be shared with the [CSIRT] network.***	**k. Examine on an annual basis the anonymised summary reports referred to in Article 14 (4).**

		j. In collaboration with ENISA, agree a roadmap for NIS exercises, education programmes and training.	***j. Agree on a strategic approach to NIS exercises[18], education programmes and training, taking into account the work undertaken by ENISA.***	**l. Discuss the work undertaken with regard to NIS exercises, education programmes and training, including the work by ENISA.**
		k. With ENISA´s assistance, exchange best practices with regard to the identification of operators by the Member States.		**m. With ENISA´s assistance, exchange best practices with regard to the identification of operators by the Member States, including in relation to cross-border dependencies regarding NIS risks and incidents.**
		l. Discuss cross-border dependencies regarding NIS risks and incidents	***l. Discuss cross-border dependencies regarding NIS risks and incidents***	

[18] Recital to be added

			(new) ***[Develop/ Discuss] the practical arrangments for reporting notifications of incidents referred to in Article 14(2) where the incident has a significant cross-border impact, including through the [CSIRT]network. [These arrangements shall preserve the confidentiality of that information as well as the operator's security and commercial interests.]***	**n. Discuss modalities for reporting notifications of incidents referred to in Article 14.**

			3b. The cooperation group shall carry out an assessment of the experience gained with the strategic cooperation pursued under this Article, at least every two years.	
		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. Taking into account the assessment referred to in paragraph 3b of this Article, and as input to the Commission's periodic review of the functioning of this Directive, the cooperation group shall produce a report. The report shall be submitted to the European Parliament, the Council and the Commission.***	**4. As input to the Commission's periodic review of the functioning of this Directive, the cooperation group shall every [1 ½][19] years produce a report assessing the experience gained with the strategic cooperation pursued under this Article.**
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).	4. The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between ~~competent authorities and~~ ***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 ~~consultation~~ ***examination*** procedure referred to in	4. The Commission shall **establish**, by means of implementing acts, **procedural arrangements necessary for the functioning of the Cooperation Group.** ~~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	***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 [advisory/ examination] procedure referred to in [Article 19(2)].***	**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(2).**

[19] Depends on the final text of Article 20.

	Article 19~~(2).~~ (***3***). (AM 80)	the consultation procedure referred to in Article 19(2).		

		Article 8b		***Article 8b***
		CSIRTs network		**CSIRTs network**
		1. In order to contribute to developing confidence and trust between the Member States and to promote swift, effective operational cooperation, a network of the national CSIRTs is hereby established.	***1. In order to contribute to developing confidence and trust between the Member States and to promote swift, effective operational cooperation in relation to risks and incidents, [particularly in the fields covered by Annex II], a network of the national CSIRTs is hereby established. It shall begin perfoming the tasks under paragraph 3 by [6 months] after the date of entry into force of this Directive.***	**1. In order to contribute to developing confidence and trust between the Member States and to promote swift, effective operational cooperation, a network of the national CSIRTs is hereby established.**
		2. The CSIRTs network shall be composed of representatives from the national CSIRTs. The [Commission], CERT-EU and the European Network and Information Security Agency ("ENISA") shall participate in the CSIRTs network as observers. ENISA shall provide the secretariat functions.	***2. The CSIRTs network shall be composed of [representatives of the Member States'CERTS/ the CSIRTs], CERT-EU and the European Network and Information Security Agency (ENISA). The Commission shall participate in the CSIRTs network as an observer. [Member States shall designate one CSIRT as a permanent representative in the CSIRT network. This CSIRT shall ensure that the***	**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. The European Network and Information Security Agency (ENISA) shall provide secretariat functions.**

			relevant designated CSIRT [referred to in Article 7] participate in its work.]	
		3. The CSIRTs network shall have the following tasks:	***3. The CSIRTs network shall have the following tasks:***	**3. The CSIRTs network shall have the following tasks:**
		a. Exchange high-level information on CSIRTs services, operations and cooperation capabilities.	***a. Exchange information on CSIRTs services, operations and cooperation capabilities.***	**a. Exchange information on CSIRTs services, operations and cooperation capabilities.**
		b. At the request of a Member State potentially affected by an incident, exchange and discuss non-commercially sensitive information related to risks and on-going incidents. Any Member State may refuse to contribute to that discussion for reasons directly relating to national security or ongoing investigations	***[b. At the request of a Member State potentially affected by an incident, discuss and exchange information related to risks and on-going incidents.]***	**b. At the request 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 publish on a voluntary basis anonymised information on incidents, which occurred in the past.	***[c. Regularly exchange, and where appropriate, such as in order to raise awareness, publish non-confidential, anonymised information on individual incidents on a common website.[20]]***	**c. Exchange and make available on a voluntary basis non-confidential information on individual incidents.[21]**
		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.	***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.***	**d. At the request of the representative of the 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.**

[20] Proposal for a recital by Commission: "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 should 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 should provide the information to be published in this website. This website should not include confidential or sensitive information."

[21] Proposal for a recital by Commission: "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 should 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 should provide the information to be published in this website. This website should not include confidential or sensitive information."

		e. Assist each other in cross-border incidents on the basis of voluntary mutual assistance.	***e. Assist Member States in adressing cross-border incidents on the basis of voluntary mutual assistance.***	**e. Support Member States in adressing cross-border incidents on the basis of their voluntary mutual assistance.**
		f. Explore further forms of operational cooperation, such as voluntary mechanisms for cross-border alerts and for mutual assistance.	***f. [Identify/ Discuss/ Discuss and explore] more extensive [forms of] [operational/ voluntary] cooperation, including in relation to:***	**f. Discuss and explore further forms of operational cooperation, including as regards:**
			(i) categories of risks and incidents, which could be subject to further operational cooperation;	**(i) categories of risks and incidents**
			(ii) early warnings of risk and incidents, the criteria for their use and modalities for their circulation;	**(ii) early warnings**
			(iii) mutual assistance for prevention, detection, mitigation, response and recovery on-going risks and incidents;	**(iii) mutual assistance**
			(iv) criteria and modalities for a coordinated response 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 3a, and request guidance related thereto.	***g. Inform the Cooperation Group of its activities and about more extensive operational cooperation [identified] pursuant to point (f), and, where necessary, request guidelines related thereto.***	**g. Inform the Cooperation Group on its activities and on the further forms of operational cooperation discussed pursuant to paragraph 3f, and request guidance related thereto.**
		h. Discuss further forms of operational cooperation, including as regards:	Deleted – merged with Art 8b (3) (f) above	
		(1) categories of risks and incidents, which could be subject to further operational cooperation;		
		(2) early warnings, the criteria for their use and modalities for their circulation;		
		(3) mutual assistance for prevention, detection, mitigation, response and recovery on actual risks and incidents.		
			h. Contribute to the carrying out of NIS exercises in accordance with the strategic approach agreed by the cooperation group under point (j) of Article 8a(3).[22]	**h. Discuss lessons learnt from NIS exercises, including from those organised by ENISA.**

[22] COM proposal for recital: "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

			EP proposal: ***i. Discuss capabilities and preparedness of the CSIRTS [through regular peer reviews/ and identify best practices on that basis] and at the request of an individual CSIRT, discuss the capabilities and preparedness of that same CSIRT***	**i. At the request of an individual CSIRT, discuss the capabilities and preparedness of that same CSIRT.**
		i. Issue guidelines in order to facilitate the convergence of (operational) practices with regard to the application of the provisions of this Directive concerning operational cooperation.	**EP proposal:** ***j. In order to facilitate the convergence of operational practices with regard to the application of this Article, develop recommendations for [individual] CSIRTs.***	**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**.

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 (Article 3(1) (b) (v) of Regulation (EU) 534 2013), support the organisation and running of Union-wide exercises by providing its expertise and advice to the Cooperation Group and the CSIRTs network."

			3a The CSIRTs network shall carry out annual assessments of the experience gained with the operational cooperation pursued under this Directive, [which shall include conclusions of the discussions pursuant to point (f) of paragraph 3. Those conclusions shall guide the work of the CERT network for the subsequent year.] The annual assessments shall be submitted to the Cooperation Group.	

		4. As input to the Commission's periodic review of the functioning of this Directive, the CSIRTs network shall produce a report on the experience gained with the operational cooperation pursued under this Directive.	**EP proposal:** ***4. As input to the Commission's periodic review of the functioning of this Directive, the CSIRTs network shall produce a report on the experience gained with the operational cooperation pursued under this Directive and shall make recommendations for more extensive operational cooperation identified pursuant to point (f) of paragraph 3 . These recommendations shall take into account the assessment referred to in paragraph 3b of this Article and the guidelines provided by the cooperation group in accordance with point (a) of Article 8a (3), and shall be reviewed regularly in light of subsequent annual assessments.***	**4. As input to the Commission's periodic review of the functioning of this Directive, the CSIRTs network shall every [1 ½][23] years produce a report assessing the experience gained with the operational cooperation pursued under this article. That report shall als be submitted to the cooperation group.**

[23] Depends on the final text of Article 20.

		5. The CSIRTs network shall define its own rules of procedure.	**EP proposal:** ***5. The Commission shall adopt, by means of implementing acts, procedural arrangements necessary for the functioning of the CSIRT network. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(2).***	**5. The CSIRTs network shall define its own rules of procedure.**

Article 9	*Article 9*	~~*Article 9*~~	*Article 9*	~~*Article 9*~~
Secure information-sharing system	Secure information-sharing system	~~Secure information-sharing system~~	Deleted	
Deleted with some provisions accommodated in articles 8a/8b				

Article 10	Article 10	~~Article 10~~	~~Article 10~~	~~Article 10~~
Early warnings	Early warnings	~~**Early warnings**~~[24]	Deleted	
Deleted with some provisions accommodated in articles 8a/8b				

[24] EP AMs related to "early warnings" are relevant to the Council's text in regard of Article 14.

Article 11	Article 11	~~Article 11~~	~~Article 11~~	~~Article 11~~
Coordinated response	Coordinated response	~~Coordinated response~~	~~Coordinated response~~	
Deleted with some provisions accommodated in articles 8a/8b				

Article 12	Article 12	~~Article 12~~	~~Article 12~~	~~Article 12~~
Union NIS cooperation plan	Union NIS cooperation plan	~~Union NIS cooperation plan~~		
Deleted with some provisions accommodated in articles 8a/8b				

Article 13	*Article 13*	*Article 13*		*Article 13*
International cooperation	International cooperation	International cooperation		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 network. Such agreement shall take into account the need to ensure adequate protection of the personal data circulating on the cooperation network.	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.*** (AM 94)	[Without prejudice to the possibility for the cooperation network to have informal 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** ~~network~~. Such agreement shall take into account the need to ensure adequate protection of **sensitive data, including** ~~the~~ personal data circulating **within** ~~on~~ the cooperation **group** ~~network~~.]	**EP proposal :** [Without prejudice to the possibility for the cooperation ~~network~~ ***group*** to have informal international cooperation, ***and for the CERT network and national CERTS to cooperate with the CERTs of third countries and of [multi- and] international institutions such as NATO and the UN,*** 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*** ~~network~~. Such agreement shall take into account the need to ensure adequate protection of ***[sensitive data, including]*** the personal data circulating ~~on~~ ***within*** the cooperation ~~network~~ ***group. Any transfer of personal data to recipients located in third countries shall be conducted in***	~~Without prejudice to the possibility for the cooperation network to have informal 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** ~~network~~. Such agreement shall take into account the need to ensure adequate protection of **sensitive data, including** ~~the~~ personal data circulating **within** ~~on~~ the cooperation **group** ~~network~~.

			accordance with Articles 25 and 26 of Directive 95/46/EC and Article 9 of Regulation (EC) No 45/2001.]	

Article 13 a (new)	*Article 13 a (new)*	*Article 13 a (new)*		
Level of criticality of market operators	Level of criticality of market operators	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. (AM 95)			

Article 14	*Article 14*	*Article 14*	*Article 14*	
Security requirements and incident notification	Security requirements and incident notification	Security requirements and incident notification	Security requirements and incident notification	Security requirements and incident notification
1. Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to 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, these measures shall guarantee a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of incidents affecting their network and information system on the	1. Member States shall ensure that ~~public administrations and~~ 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, ~~these~~ ***those*** measures shall ~~guarantee~~ ***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	1. Member States shall **require** ~~ensure~~ that ~~market~~ operators~~ and public administrations~~ take appropriate **and proportionate, sector-specific** technical and organisational measures to manage the risks posed to ~~the security of the~~ networks 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.	1. Member States shall [ensure] that ~~market~~ operators ~~and public administrations~~ take appropriate ***and proportionate*** technical and organisational measures to manage the risks posed to ~~the security of the~~ network**s** and information ***security*[25] *of*** systems which they control and use in their operations. Having regard to the state of the art, ***those*** measures shall [***ensure***] ~~guarantee~~ a level of ***network and information*** security appropriate to the risk presented.	1. Member States shall ensure that ~~market~~ operators ~~and public administrations~~ take appropriate **and proportionate** technical and organisational measures to manage the risks posed to the security of ~~the~~ network**s** and information systems which they control and use in their operations. Having regard to the state of the art, **those** measures shall **ensure** ~~guarantee~~ a level of security **of networks and information systems** appropriate to the risk presented.

[25] Further discussions on terms "network and information security" and "security" are needed.

core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.	***the security of*** their network and information ~~system~~ ***systems*** on the core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems. (AM 96)			
		1a ~~In particular,~~ **Member States shall require that operators take appropriate** measures ~~shall be taken~~ to prevent and minimise the impact of incidents affecting ~~their~~ network and information **security** ~~system on~~ **of** the **essential** ~~core~~ services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.		**1a** ~~In particular,~~ **Member States shall ensure that operators take appropriate** measures ~~shall be taken~~ to prevent and minimise the impact of incidents affecting ~~their~~ **security of the** network**s** and information systems ~~on~~ **used for the provision of** ~~the~~ **essential** ~~core~~ services ~~they provide~~ and thus **to** ensure the continuity of **those** ~~the~~ services ~~underpinned by those networks and information systems~~.

2. Member States shall ensure that public administrations and market operators notify to the competent authority incidents having a significant impact on the ***security*** of the core services they provide.	2. Member States shall ensure that ~~public administrations and~~ market operators notify ***without undue delay*** to the competent authority ***or to the single point of contact*** incidents having a significant impact on the ~~security~~ ***continuity*** of the core services they provide. ***Notification shall not expose the notifying party to increased liability.***	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 having a significant impact on the **continuity** ~~security~~ of the **essential** ~~core~~ services they provide.	**EP proposal:** 2. Member States shall ensure that ~~public administrations and~~ market operators notify ***without undue delay*** to the competent authority ***or to the single point of contact*** incidents having a significant impact on the ~~security~~ ***continuity***[26] of the core services they provide. ***Notifications shall include information to enable the competent authority to determine the significance of any cross-border impact.*** ***Notification shall not expose the notifying party to increased liability***[27]**.**	2. Member States shall **provide for a reporting scheme pursuant to which** ~~ensure that public administrations and market~~ operators **shall** notify **without undue delay** to the competent authority **or to the CSIRT** incidents having a significant impact on ~~the security of~~ **networks and information systems used for the provision of** ~~the core~~ **essential** services ~~they provide~~**. Notification shall not expose the notifying party to increased liability.**

26 COM points out that only the continuity but also security needs to be addressed as well. Follows art. 13a of the FD.

27 EP to re-draft the wording of the last sentence.

	To determine the significance of the impact of an incident, the following parameters shall inter alia be taken into account: (AM 97)	**2a To determine the significance of the impact of an incident, the following parameters in particular shall be taken into account**		**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 whose core service is affected; (AM 98)	**a) the number of users affected by the disruption of the essential service;**		**a) the number of users affected by the disruption of the essential service;**
	(b) the duration of the incident; (AM 99)	**b) the duration of the incident;**		**b) the duration of the incident;**
	(c) geographic spread with regard to the area affected by the incident. (AM 100)	**(c) the geographical spread with regard to the area affected by the incident.**[28]		**(c) the geographical spread with regard to the area affected by the incident.**[29]

[28] The Council requires further consideration of this provision, including the question whether the substance of the provision should be moved to a recital or whether the provision should be supplemented by a recital explaining inter alia the meaning of "significant impact".

[29] The Council requires further consideration of this provision, including the question whether the substance of the provision should be moved to a recital or whether the provision should be supplemented by a recital explaining inter alia the meaning of "significant impact".

	Those parameters shall be further specified in accordance with point (ib) of Article 8(3). (AM 101)		**EP proposal:** ***Those parameters shall be further specified in accordance with point (ab new) of Article 8a(3).***	

	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. (AM 102)		**EP proposal to cover the situation of operator active in more than one Member States:** ***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.***	

		2b When notifying an incident to its national competent authority, an operator shall include relevant information allowing the competent authority to determine the cross-border effect of that incident. Based on the information provided by the operator, the competent authority or the single point of contact shall inform the Member State(s) if the incident has a significant impact. In doing so, the competent authority or the single point of contact will preserve the operator's security and commercial interests as well as the confidentiality of the information provided by the operator.	**EP proposal to deal with the situation of the cross-border effect of the incident (the operator is active in one MS):** move provisions obliging operator to provide relevant information to Art 14(2) and obligation to inform other MS if incident has significant cross-border impact to Art 8a (modalities) and Art 6 or 7 (information provision). Role of ENISA to be considered further.	**2ac When notifying an incident to its national competent authority or CSIRT, an operator shall include relevant information allowing the competent authority or CSIRT to determine the cross-border effect of that incident. Based on the information provided by the operator, the competent authority or CSIRT shall inform the other afected Member State(s) if the incident has a significant impact. In doing so, the competent authority or CSIRT shall preserve the operator's security and commercial interests as well as the confidentiality of the information provided by the operator.** **The operator shall be informed, as soon as possible, about any undertaken steps, results and any other information with relevance to the incident.** **[At the request of the competent authority, the single point of contact shall**

				forward notifications referred to in the first subparagraph to single points of contact in other affected Member States.]
	2b. 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. (AM 103)		Delete	
	2c. Market operators not covered by Annex II may report incidents as specified in Article 14(2) on a voluntary basis. ***(AM 104)***			
3. The requirements under paragraphs 1 and 2 apply to all market operators providing services within the European Union.		3. The requirements under paragraphs 1 **to** ~~and~~ 2**b** apply to all ~~market~~ operators providing services within the European Union.		3. The requirements under paragraphs 1 **to** ~~and~~ 2**b** apply to ~~all~~ ~~market~~ **the following** operators**:** **- operators that are**

				established in a Member State; and **- operators that are not established in the Union but direct their activities to one or several Member States** ~~providing services within the European Union~~. [30]

[30] This text provides for a first tentative compromise to solve the issue of territorial applications in particular as far as internet enablers are concerned. This text takes into account two precedents, i.e. Council General Approach for a proposal for a Directive on package travel and assisted travel arrangements (document 16054/14, see articles 15(1) and 17(1) and recital 40b)and proposal for General Data Protection Regulation (document 15395/14, see Article 3 and recital 20). Given these precedents, a possible explanatory recital for Article 14(3) should be considered

4. The competent authority may inform the public, or require the public administrations and market operators to do so, where it determines that disclosure of the incident is in the public interest.	4. ~~The~~ ***After consultation with the notified*** competent authority ***and the market operator concerned, the single point of contact*** may inform the public ~~, or require the public administrations and operators to do so, where it determines that~~ ***about individual incidents, where it determines that public awareness is necessary to prevent an incident or deal with an on-going 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.*** ~~of the incident is in the public interest~~	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**[31] summary report to the cooperation **group** ~~network~~ on the notifications received and the action taken in accordance with this paragraph.	**EP proposal :** ~~The~~ ***After consultation with the notified*** competent authority ***and the market operator concerned, the single point of contact*** may inform the public, ~~or require the public administrations and operators to do so, where it determines that~~ ***about individual incidents, where it determines that public awareness is necessary to prevent an incident or deal with an on-going 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.*** ~~of the incident is in the public interest~~	4. **After consulting the operator concerned,** ~~The~~ the **notified** competent authority **or CSIRT** 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~~.

[31] The anonymity aspect might be addressed by means of a recital.

	Before any public disclosure ***~~of the incident is in the public interest~~, 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 competent authority shall submit a summary report to the cooperation network on the notifications received and the action taken in accordance with this paragraph.	Once a year, the ~~competent authority~~ ***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. (AM 105)		**EP proposal:** Once a year, the ~~competent authority~~ ***single point of contact*** shall submit a ***an [anonymised]*** summary report to the cooperation network on the notifications received***, including the number and the nature of notifications and regarding the incident parameters as listed in paragraph 2 of this Article,*** and the action taken in accordance with this paragraph.	Once a year, the **single point of contact** ~~competent authority~~ shall submit **an anonymised**[32] summary report to the cooperation **group** ~~network~~ on the notifications received and the action taken in accordance with ~~this~~ **paragraphs 2 and 2ac** ~~paragraph~~.
	4a. Member States shall encourage market operators to make public incidents involving their business in their financial reports on a voluntary basis. (AM 106)			

[32] The anonymity aspect might be addressed by means of a recital.

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.	~~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.~~ (AM 107)	deleted	deleted	
6. ***Subject to any delegated act adopted under paragraph 5, the competent authorities*** may adopt guidelines ***and, where necessary, issue instructions*** concerning the circumstances in which ***public administrations and*** market operators are required to notify incidents.	6. ~~Subject to any delegated act adopted under paragraph 5, the competent authorities~~ ***The competent authorities or the single points of contact*** may adopt guidelines ~~and, where necessary, issue instructions~~ concerning the circumstances in which ~~public administrations and~~ market operators are required to notify incidents. (AM 108)	[6. ~~Subject to any delegated act adopted under paragraph 5, t~~**T**he 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.]	**EP proposal:** 6. ~~Subject to any delegated act adopted under paragraph 5, the competent authorities~~ ***The competent authorities or the single points of contact***[33]***, when requested with the assistance of ENISA,*** may adopt guidelines ~~and, where necessary, issue instructions~~ concerning the circumstances in which ~~public administrations and~~ market operators are required to notify incidents.	6. ~~Subject to any delegated act adopted under paragraph 5, the competent authorities~~ **The competent authorities, when requested with the assistance of ENISA,** may adopt guidelines ~~and, where necessary, issue instructions~~ concerning the circumstances in which ~~public administrations and~~ ~~market~~ operators are required to notify incidents.

[33] Inclusion of SPC subject to further discussion regarding the role of the SPC vs CA.

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).		deleted	**EP proposal:** 7. The Commission shall be empowered to define, by means of implementing acts, the formats and procedures applicable for the purpose of paragraph 2. ***The formats shall take into account/be consistent with the formats used for notifications of personal data breaches under Union law on data protection***. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).	

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[34].	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. (AM 109)	deleted		
	8a. Member States may decide to apply this Article and Article 15 to public administrations mutatis mutandis. (AM 110)			

34 OJ L 124, 20.5.2003, p. 36.

Article 15	*Article 15*	*Article 15*		*Article 15*
Implementation and enforcement	Implementation and enforcement	Implementation and enforcement.		Implementation and enforcement.
1. Member States shall ensure that the competent authorities have all the powers necessary to investigate cases of non-compliance of public administrations or market operators with their obligations under Article 14 and the effects thereof on the security of networks and information systems.	1. Member States shall ensure that the competent authorities ~~have all~~ ***and the single points of contact have*** the powers necessary to ~~investigate cases of non-compliance of public administrations or~~ ***ensure compliance*** of market operators with their obligations under Article 14 and the effects thereof on the security of networks and information systems. (AM 111)	[1. Member States shall ensure that the competent authorities have ~~all~~ the ~~powers~~ necessary **means** to **assess** ~~investigate~~ **the** ~~cases of non-~~compliance of ~~public administrations or market~~ operators ~~and~~ with their obligations under Article 14 and the effects thereof on the security of networks and information systems]		1. Member States shall ensure that the competent authorities have ~~all~~ the ~~powers~~ necessary **means** to **assess** ~~investigate~~ **the** ~~cases of non-~~compliance of ~~public administrations or market~~ operators ~~and~~ 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 authorities have the power to require market operators and public administrations to:	2. Member States shall ensure that the competent authorities ***and the single points of contact*** have the power to require market operators ~~and public administrations~~ to: (AM 112)	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:		2. Member States shall ensure that the competent authority~~ies~~ has~~ve~~ the **means** ~~power~~ to require ~~market~~ operators ~~and public administrations~~ to:
(a) provide information needed to assess the security of their networks and information systems, including documented		(a) provide information needed to assess the security of their networks and information systems, including documented		(a) provide information needed to assess the security of their networks and information systems, including documented

security policies;		security policies;		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.	(b) ~~undergo~~ ***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 ~~results thereof~~ ***evidence*** available to the competent authority ***or to the single point of contact***. (AM 113)	(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.]		(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.
	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. (AM 114)			

3. Member States shall ensure that competent authorities have the power to issue binding instructions to market operators and public administrations.	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 ~~and public administrations~~.	3. ~~Member States shall ensure that~~ **Following the assessment of information or results of security audits referred to in paragraph 2,** the competent authorities ~~have the power to~~ **may issue** ~~binding~~ instructions to the ~~market~~ operators ~~and public administrations~~ **to remedy their operations.**		3. ~~Member States shall ensure that~~ **Following the assessment of information or results of security audits referred to in paragraph 2,** the competent authorit**y**~~ies~~ ~~have the power to~~ **may issue** binding instructions to the ~~market~~ operators ~~and public administrations~~ **to remedy their operations.**
	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. (AM 116)			
4. The competent authorities shall notify incidents of a suspected serious criminal nature to law enforcement authorities.	4. The competent authorities ~~shall notify incidents of a suspected serious~~ criminal ~~nature to~~ ***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. (AM 117)	deleted		
5. The competent authorities shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.	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***	5. [The competent authorities shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.]		5. The competent authorit~~y~~**ies** shall work in close cooperation with personal data protection authorities when addressing incidents resulting in personal data breaches.

	notifications under Article 14(2) of this Directive and other Union law on data protection. (AM 118)			
6. Member States shall ensure that any obligations imposed on public administrations and market operators under this Chapter may be subject to judicial review.	6. Member States shall ensure that any obligations imposed on ~~public administrations and~~ market operators under this Chapter may be subject to judicial review. (AM 119)	6. [Member States shall ensure that any obligations imposed on ~~market~~ operators ~~and public administrations~~ under this Chapter may be subject to judicial review.]		
	6a. Member States may decide to apply Article 14 and this Article to public administrations mutatis mutandis. (AM 120)			

Article 16	*Article 16*	*Article 16*	*Article 16*	*Article 16*
Standardisation	Standardisation	Standardisation		Standardisation
1. To ensure convergent implementation of Article 14(1), Member States shall encourage the use of standards and/or specifications relevant to networks and information security.	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. (AM 121)	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 **European or internationally accepted** standards and/or specifications relevant to networks and information security.		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 **European or internationally accepted** standards and/or specifications relevant to networks and information security.
		[**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.]**		**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.	2. The Commission shall ***give a mandate to a relevant European standardisation body to**, **in consultation with relevant stakeholders,*** draw up~~, by means of implementing acts~~ 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. (AM 122)	deleted		

Article 17	*Article 17*	*Article 17*		*Article 17*
Sanctions	*Sanctions*	*Sanctions*		*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.		[1. Member States shall lay down rules on sanctions applicable to infringements of the national provisions adopted pursuant to **Article 14 of** 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.]]		1. Member States shall lay down rules on sanctions applicable to infringements of the national provisions adopted pursuant to **Articles 14 and 15 of** 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.~~

	1a. 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. (AM 123)			
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[35].		[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.]]	**EP proposal :** *2. Member States shall ensure that when a security incident involves personal data, the ~~sanctions foreseen~~* ***penalties laid down in national law*** *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[36].*	

[35] SEC(2012) 72 final

[36] SEC(2012) 72 final

Article 18	Article 18	~~Article 18~~	Article 18	
Exercise of the delegation	Exercise of the delegation	~~Exercise of the delegation~~	Exercise of the delegation	
Deleted				

Article 19	Article 19	Article 19		
Committee procedure	Committee procedure	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.		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.		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.		deleted		
3. Where reference is made to this paragraph, Article 5 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.		3. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 20	*Article 20*	*Article 20*		*Article 20*
Review	Review	Review		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. For this purpose, the Commission may request Member States to provide information without undue delay.	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. (AM 126)	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 advance the strategic and operational cooperation**, the Commission **shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The Commission** may **also** request Member States to provide information without undue delay.		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** ~~three~~ years after the date ~~of transposition~~ referred to in Article 21(2). **Thereafter, the Commission shall periodically review this Directive.** For this purpose **and with a view to further advance the strategic and operational cooperation**, the Commission **shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level.** ~~may request Member States to provide information without undue delay~~.

Article 20a				***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).
				2. By (the date referred to in Article 21(2)) and for the purposes of this Article, Member States shall ensure appropriate representation in the Cooperation Group and the CSIRTs Network.

Article 21	*Article 21*	*Article 21*		*Article 21*
Transposition	Transposition	Transposition		Transposition
4. Member States shall adopt and publish, by [one year and a half after adoption] 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.		[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.]		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.
They shall apply those measures from [one year and a half after adoption].		**2**. They shall apply those measures from **[two years** ~~one year~~ and a half after ~~adoption~~ the **date of entry into force of this Directive].**		**2**. They shall apply those measures from **two years** ~~one year~~ and a half after ~~adoption~~ the **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.		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.		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.

5. 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.		**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	*Article 22*	*Article 22*		*Article 22*
Entry into force	Entry into force	Entry into force		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.*		This Directive shall enter into force on the [twentieth] day following that of its publication in the *Official Journal of the European Union.*		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	*Article 23*	*Article 23*	*Article 23*	*Article 23*
Addressees	Addressees	Addressees	Addressees	Addressees
This Directive is addressed to the Member States.	This Directive is addressed to the Member States.,	This Directive is addressed to the Member States.		This Directive is addressed to the Member States.
Done at Brussels	Done at Brussels	Done at Brussels		Done at Brussels

ANNEX I	ANNEX I	ANNEX I		ANNEX I
Requirements and tasks of the Computer Emergency Response Team (CERT)	Requirements and tasks of the Computer Emergency Response ~~Team~~ ***Teams (CERTs)*** (AM 127)	**Requirements and tasks of the Computer Security Incident ~~Emergency~~ Response Team (CSIRT)**		Requirements and tasks of the Computer **Security Incident** ~~Emergency~~ **Response** Team **(CSIRT)** ~~(CERT)~~
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:		The requirements and tasks of the **CSIRT** ~~CERT~~ shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following elements:		The requirements and tasks of the **CSIRT** ~~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		(1) Requirements for the **CSIRT** ~~CERT~~		(1) Requirements for the **CSIRT** ~~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.	(a) The ~~CERT~~ ***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. (AM 128)	(a) The **CSIRT** ~~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.		(a) The **CSIRT** ~~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.

(b) The CERT shall implement and manage security measures to ensure the confidentiality, integrity, availability and authenticity of information it receives and treats.		(b) The **CSIRT** ~~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**.**	(c) The offices of the ~~CERT~~ ***CERTs*** and the supporting information systems shall be located in secure sites ***with secured network information systems.*** (AM 129)	(c) The offices of the **CSIRT** ~~CERT~~ and the supporting information systems shall be located in secure sites.		(c) The offices of the **CSIRT** ~~CERT~~ and the supporting information systems shall be located in secure sites.
(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.		(d) A service management quality system shall be created to follow-up on the performance of the **CSIRT** ~~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:		(e) Business continuity:		(e) Business continuity:
- The CERT shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers,		- The **CSIRT** ~~CERT~~ shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers,		- The **CSIRT** ~~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 **CSIRT** ~~CERT~~ shall be adequately staffed to ensure availability at all times,		- The **CSIRT** ~~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.		- The **CSIRT** ~~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 **CSIRT** ~~CERT~~ to ensure permanent access to the means of communication.		- The **CSIRT** ~~CERT~~ shall rely on an infrastructure whose continuity is ensured. To this end, redundant systems and backup working space shall be **available** ~~set up for the CERT to ensure permanent access to the means of communication~~.
(2) Tasks of the CERT		(2) Tasks of the **CSIRT** ~~CERT~~		(2) Tasks of the **CSIRT** ~~CERT~~
(a) Tasks of the CERT shall include at least the following:		(a) Tasks of the **CSIRT** ~~CERT~~ shall include at least the following:		(a) Tasks of the **CSIRT** ~~CERT~~ shall include at least the following:
- Monitoring incidents at a national level,	- ***Detecting and*** monitoring incidents at a national level, (AM 130)	- Monitoring incidents at a national level,		- Monitoring incidents at a national level,
- Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents,		- Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents,		- Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents,
- Responding to incidents,		- Responding to incidents,		- Responding to incidents,

- Providing dynamic risk and incident analysis and situational awareness,		- Providing dynamic risk and incident analysis and situational awareness,		- Providing dynamic risk and incident analysis and situational awareness,
- Building broad public awareness of the risks associated with online activities,		~~- Building broad public awareness of the risks associated with online activities,~~		
	- Actively participating in Union and international CERT cooperation networks (AM 131)		**EP proposal :** ***- Actively participating in the CERT network and, where possible, other international [CERT] cooperation networks***	**- Participating in the CSIRTs network.**
- Organising campaigns on NIS;		~~Organising campaigns on NIS;~~		
(b) The CERT shall establish cooperative relationships with private sector.		(b) The **CSIRT** ~~CERT~~ shall establish cooperative relationships with private sector.		(b) The **CSIRT** ~~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:		(c) To facilitate cooperation, the **CSIRT** ~~CERT~~ shall promote the adoption and use of common or standardised practises for:		(c) To facilitate cooperation, the **CSIRT** ~~CERT~~ shall promote the adoption and use of common or standardised practises for:
- incident and risk handling procedures,		- incident and risk handling procedures,		- incident and risk handling procedures,

- incident, risk and information classification schemes,		- incident, risk and information classification schemes,		- incident, risk and information classification schemes,
- taxonomies for metrics,		- taxonomies for metrics,		
- information exchange formats on risks, incidents, and system naming conventions.		- information exchange formats on risks, incidents, and system naming conventions.		

ANNEX II	ANNEX II	**ANNEX II**[37]		
List of market operators	List of market operators	**List of ~~market~~ ~~operators~~ types of entities for the purposes of Article 3(8)**		**List of types of entities for the purposes of Article 3(8) operators**
Referred to in Article 3(8) a):	~~Referred to in Article 3(8) a):~~	~~Referred to in Article 3(8) a):~~ **0. In the field of Internet infrastructure**:		**0. In the field of Internet infrastructure**:
		Internet exchange points[38]	***Internet exchange points***	**Internet exchange points**
		national domain name registries, domain name system service providers		**national domain name registries, domain name system service providers**
Referred to in Article 3(8) b):		**0.1 In the field of digital service platforms**[39]		**01 In the field of digital service platforms:**
1. e-commerce platforms	~~1. e-commerce platforms~~	1. - e-commerce platforms		**(a)** e-commerce platforms
2. Internet payment gateways	~~2. Internet payment gateways~~	2.-. [Internet payment gate ways]		**(b)** Internet payment gateways

[37] In the understanding of the Council and as far as the list of (sub) sectors in Annex II is concerned, the purpose here is to achieve minimum harmonisation: Member States may add additional (sub)sectors (i.e. types of entities) to the list (and even add additional fields). Furthermore, a Member State, following the assessment on the basis of Article 3(8), may decide that, on its territory, not all entities listed in Annex II fulfil those criteria and therefore there is no risk for this or that (sub) sector. It should be noted further that it is largely immaterial whether the content of Annex II is located in an Annex or as part of art. 3, as long as the Annex may only be amended through the full legislative procedure.

[38] To the extent that they are not covered by the FD.

[39] The bracketed sub-sectors 2, 3 and 6 are being considered in the Council to be deleted, whereas for sub-sectors 1, 4 and 5 further clarification and justification, e.g. in the form of recital text, is needed before considering whether or not to maintain these sub-sectors.

3. Social networks	~~3. Social networks~~	3.-. [Social networks]		**(c)** Social networks
4. Search engines	~~4. Search engines~~	4.-. Search engines		**(d)** Search engines
5. Cloud computing services	~~5. Cloud computing services~~	-. Cloud computing services**, including web hosting services**[40]		**(e)** Cloud computing services
6. Application stores	~~6. Application stores~~	6.-[Application stores]		**(f)** Application stores
Referred to in Article (3(8) b):	~~Referred to in Article (3(8) b):~~ (AM 132)	~~Referred to in Article (3(8) b):~~		
List of market operators	List of market operators	~~List of market operators~~		
1. Energy	1. Energy	1. **In the field** of energy		**1. Energy**

[40] The following text for a new Recital has been suggested: "Cloud computing services may comprise "infrastructure as a service" (i.e. enterprise infrastructure such as private clouds and virtual local area networks, in which a business can store its data and run the applications needed for its daily operation; and "cloud hosting", the hosting of websites on virtual servers which are founded upon pooled resources from underlying physical servers) or "platform as a service" (i.e. online computing platforms which typically include operating system, programming language execution environment, database and web server). Except where already provided for in contractual obligations between the relevant parties, a cloud computing service should be considered to fall within scope of the requirements of this Directive when it is used by an operator in the provision of an essential service. A cloud computing service provided directly to an end user other than a market operator as defined in Article 3(8) may also fall within scope of the requirements of this Directive to the extent that a Member State identifies it as a service platform underpinning the Internet that meets the definition of market operator."

	(a) Electricity			***(a) Electricity***
- Electricity and gas suppliers	~~– Electricity and gas -~~ Suppliers	- Electricity and gas suppliers		**- Suppliers**
- Electricity and/or gas distribution system operators and retailers for final consumers	~~- Electricity and/or gas~~ - Distribution system operators and retailers for final consumers	- Electricity and/or gas distribution system operators ~~and retailers for final consumer~~		**- Distribution system operators and retailers for final consumers**
- Natural gas transmission system operators, storage operators and LNG operators	~~- Natural gas transmission system operators, storage~~ ~~operators and LNG operators~~	- Natural gas transmission system operators, storage operators and LNG operators		
- Transmission system operators in electricity	- Transmission system operators in electricity	- Transmission system operators in electricity		**- Transmission system operators in electricity**
	(b) Oil			***(b) Oil***
- Oil transmission pipelines and oil storage	- Oil transmission pipelines and oil storage	- Oil transmission pipelines and oil storage		**- Oil transmission pipelines and oil storage**
	- Operators of oil production, refining and treatment facilities, storage and transmission			**- Operators of oil production, refining and treatment facilities, storage and transmission**
	(c) Gas			***(c) Gas***

- Electricity and gas market operators	- ~~Electricity and gas market operators~~ ***Suppliers***	- Electricity and gas market operators		**- Suppliers**
	- Distribution system operators and retailers for final consumers			**- Distribution system operators and retailers for final consumers**
	- Natural gas transmission system operators, storage system operators and LNG system operators			**- Natural gas transmission system operators, storage system operators and LNG system operators**
- Operators of oil and natural gas production, refining and treatment facilities	- Operators of ~~oil~~ natural gas production, refining, ~~and~~ treatment facilities, ***storage*** facilities ***and transmission***	- Operators of oil and natural gas production, refining and treatment facilities		**- Operators of natural gas production, refining, treatment facilities, *storage* facilities *and transmission***
	- Gas market operators (AM 133)			**- Gas market operators**
2. Transport	2. Transport	2. **In the field** of transport :		**2. Transport**
				(a) Air transport
- Air carriers (freight and passenger air transport)	~~- Air carriers (freight and passenger air transport)~~	- Air carriers (freight and passenger air transport)		**- Air carriers (freight and passenger air transport)**
				- Airports
				- Traffic management control operators

- Maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies)	~~- Maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies)~~ ***(i) Traffic management control operators***	- Maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies)		***(b) Rail transport***
- Railways (infrastructure managers, integrated companies and railway transport operators)	~~- Railways (infrastructure managers, integrated companies and railway transport operators)~~ ***(ii) Auxiliary logistics services:***	- Railways (infrastructure managers, integrated companies and railway transport operator)		**- Railways (infrastructure managers, integrated companies and railway transport operators)**
- Airports	~~- Airports~~ ***- warehousing and storage,***	- Airports		**- Traffic management control operators**
- Ports	~~- Ports~~ ***- cargo handling, and***	- Ports		***(c) Maritime transport***
- Traffic management control operators	~~- Traffic management control operators -~~ ***other transportation support activities***	- Traffic management control operators		**(i) Maritime carriers (inland, sea and coastal passenger water transport companies and inland, sea and coastal freight water transport companies)**
- Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation support activities)	~~- Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation support activities)~~ ***(b) Rail transport***	~~- Auxiliary logistics services (a) warehousing and storage, b) cargo handling and c) other transportation support activities)~~		

	(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) (AM 134)			
3. Banking: credit institutions in accordance with Article 4.1 of Directive 2006/48/CE.		3**.** **In the field of** banking: credit institutions in accordance with Article 4.1 of Directive 2006/48/CE.		3. Banking: credit institutions in accordance with Article 4.1 of Directive 2006/48/CE.

4. Financial market infrastructures: stock exchanges and central counterparty clearing houses	4. Financial market infrastructures: ***regulated markets, multilateral trading facilities, organised trading facilities*** ~~stock exchanges~~ and central counterparty clearing houses (AM 135)	4. **In the field of** financial market infrastructures: stock exchanges and central counterparty clearing houses		4. Financial market infrastructures: stock exchanges and central counterparty clearing houses.
5. Health sector: health care settings (including hospitals and private clinics) and other entities involved in health care provisions		[5. **In the field of** health sector: health care settings (including hospitals and private clinics) and other entities involved in health care provision.][41]]		5. Health sector: healthcare ~~settings~~ **providers** (including hospitals ~~and private clinics~~) ~~and other entities involved in health care provisons~~ **as defined in Article 3(g) of Directive 2011/24/EU**.
	5a. Water production and supply (AM 136)	**6. In the field of water supply: [types of entities to be further considered].**		**6. Drinking water production and supply sector.**

[41] It has been suggested to amend this indent with the following: "Healthcare settings and other entities involved in healthcare provision, which handle a significant amount of vital patient information".

	5b. Food supply chain (AM 137)			
	5c. Internet exchange points(AM 138)			