EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2013/0027(COD)

15.1.2014

OPINION

of the Committee on Civil Liberties, Justice and Home Affairs

for the Committee on the Internal Market and Consumer Protection

on the 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
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Rapporteur: Carl Schlyter

PA_Legam

SHORT JUSTIFICATION

The proposal aims at achieving a high common level of network and information security within the EU. Your rapporteur supports the objectives pursued by the proposal, recommending amendments that will improve legal certainty and strengthen the safeguards and protections of individuals and their privacy, in order to ensure that individuals are in control of their personal data and trust in the digital environment, and in order to create a culture of risk management and improvement of information sharing between private and public parties.

The amendments proposed regard strengthening reference to data protection legislation, clarifying that 'critical infrastructure' should not include social networks and application stores (see amended list in Annex II) and making sure proportionality is respected, by underlining the civil aspect of the undertaking: most disruptions and common causes of system failures are not intentional cyber attacks by terrorists, criminals or foreign spies, but unintentional, human error and natural causes. It is of crucial importance that the EU distinguishes the implementation of the proposed legislation from any militarisation of the subject, excluding the security and surveillance industry's goals, taking into consideration the context of a globalised digital market.

A major concern that remains regards the relationship of the proposed system to the notification system proposed under the general data protection regulation, and their effective coexistence, which is one of the reasons we highlight the fact that any EU cybersecurity legislation should follow the adoption of the General Data Protection Regulation, not precede it. Furthermore, the real financial and administrative implications should be considered, including the total societal costs and not only costs of making a notification. Software companies that do sloppy programming, thus saving money by exposing their customers can not in all cases be protected by the standard in users' conditions that deny any responsibilities for malfunction of their software. They need to have incentives to make sure they are reasonably safe. Finally, key concepts should be clarified and not left open to interpretation by Member States (such as the meaning of 'public administrations', 'significant impact' and a concrete definition of 'cybercrime').

AMENDMENTS

The Committee on Civil Liberties, Justice and Home Affairs calls on the Committee on the Internal Market and Consumer Protection, as the committee responsible, to incorporate the following amendments in its report:

Amendment 1

Proposal for a directive
Recital 1

Text proposed by the Commission	*Amendment*
(1) Network and information systems and services play a vital role in the society. Their reliability and security are essential to economic activities ***and*** social welfare***, and in particular to the functioning of the internal market.***	(1) Network and information systems and services play a vital role in the society. Their reliability and security are essential to economic activities***,*** social welfare ***and communications and exchanges between people, civil-society organisations and undertakings, as well as protection of, and respect for, private life and personal data.***

Amendment 2

Proposal for a directive
Recital 2

Text proposed by the Commission	*Amendment*
(2) The magnitude and frequency of deliberate or accidental security incidents is increasing and represents a major threat to the functioning of networks and information systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.	(2) The magnitude and frequency of deliberate or accidental security incidents is increasing and represents a major threat to the functioning of networks and information systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union. ***There has been a growing recognition that control systems are vulnerable to cyber-attacks from numerous sources, including hostile governments, terrorist groups and other malicious intruders. Smart attacks and coordinated attacks could have severe impacts to the stability, performance, and economics of the infrastructure.***

Amendment 3

Proposal for a directive
Recital 3

Text proposed by the Commission	*Amendment*
(3) As a communication instrument	(3) As a communication instrument

without frontiers, digital information systems, and primarily the Internet play an essential role in facilitating the cross-border movement of goods, services and people. Due to that transnational nature, substantial disruption of those systems in one Member State can also affect other Member States and the Union as a whole. The resilience and stability of network and information systems is therefore essential to the smooth functioning of the internal market.	without frontiers, digital information systems, and primarily the Internet play an essential role in facilitating the cross-border movement of goods, services and people. Due to that transnational nature, substantial disruption of those systems in one Member State can also affect other Member States and the Union as a whole. The resilience and stability of network and information systems is therefore essential to the smooth functioning of the internal market ***and to communications and exchanges between people, civil-society organisations and undertakings***.

Amendment 4

Proposal for a directive
Recital 3 a (new)

Text proposed by the Commission	*Amendment*
	(3a) Since the more common causes of system failures continue to be unintentional, such as natural causes or human error, infrastructure should be resilient both to intentional and unintentional disruptions, and operators of critical infrastructure should design resilience based systems that are operational even when other systems beyond their control fail.

Amendment 5

Proposal for a directive
Recital 6 a (new)

Text proposed by the Commission	*Amendment*
	(6a) It is vital to acknowledge the uncertainty inherent in the complex systems that sustain us. This requires better shared understanding of what is critical between those who protect an organization and those who set its

strategic direction.

Amendment 6

Proposal for a directive
Recital 8

Text proposed by the Commission	*Amendment*
(8) The provisions of this Directive should be without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of its essential security interests, to safeguard public policy and public security, and to permit the investigation, detection and prosecution of criminal offences. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security.	(8) The provisions of this Directive should be without prejudice to the possibility for each Member State to take the necessary measures to ensure the protection of its essential security interests, to safeguard public policy and public security, and to permit the investigation, detection and prosecution of criminal offences***, with the proviso that they should not take this as a pretext for failing to comply with their more general obligations with regard to respect for the protection of private life and personal data***. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security.

Amendment 7

Proposal for a directive
Recital 9

Text proposed by the Commission	*Amendment*
(9) To achieve and maintain a common high level of security of network and information systems, each Member State should have a national NIS strategy defining the strategic objectives and concrete policy actions to be implemented. NIS cooperation plans complying with essential requirements need to be developed at national level in order to reach capacity response levels allowing for effective and efficient cooperation at national and Union level in case of	(9) To achieve and maintain a common high level of security of network and information systems, each Member State should have a national NIS strategy defining the strategic objectives and concrete policy actions to be implemented. NIS cooperation plans complying with essential requirements need to be developed at national level in order to reach capacity response levels allowing for effective and efficient cooperation at national and Union level in case of

incidents.	incidents***, respecting and protecting private life and personal data***.

Amendment 8

Proposal for a directive
Recital 10

Text proposed by the Commission	*Amendment*
(10) To allow for the effective implementation of the provisions adopted pursuant to this Directive, ***a body*** responsible for coordinating NIS issues and acting as a focal point for cross-border cooperation at Union level should be established or identified in each Member State. These bodies should be given the adequate technical, financial and human resources to ensure that they can carry out in an effective and efficient manner the tasks assigned to them and thus achieve the objectives of this Directive.	(10) To allow for the effective implementation of the provisions adopted pursuant to this Directive, ***a national competent authority under civilian control with full democratic oversight and transparency in their operations being*** responsible for coordinating NIS issues and acting as a focal point for cross-border cooperation at Union level should be established or identified in each Member State. These bodies should be given the adequate technical, financial and human resources to ensure that they can carry out in an effective and efficient manner the tasks assigned to them and thus achieve the objectives of this Directive.

Amendment 9

Proposal for a directive
Recital 14 a (new)

Text proposed by the Commission	*Amendment*
	(14a) More sectors adopt cloud services in their computing environment such as IT services operating critical infrastructure. Sufficient security measures need to ensure the confidentiality, integrity and availability of the data in the cloud. Hosting infrastructure services, and storing sensitive data in the cloud environment brings with it security and resilience requirements that existing cloud services are not well placed to address. Therefore, there needs to be an

	assurance that the cloud computing environment can provide proficient protection of the sensitive critical infrastructure data.

Amendment 10

Proposal for a directive
Recital 15

Text proposed by the Commission	*Amendment*
(15) As most network and information systems are privately operated, cooperation between the public and private sector is essential. Market operators should be encouraged to pursue their own informal cooperation mechanisms to ensure NIS. They should also cooperate with the public sector and share information and best practices ***in exchange of*** operational support in case of incidents.	(15) As most network and information systems are privately operated, cooperation between the public and private sector is essential. Market operators should be encouraged to pursue their own informal cooperation mechanisms to ensure NIS. They should also cooperate with the public sector and ***mutually*** share information and best practices ***as well as reciprocal*** operational support ***as needed*** in case of incidents.

Amendment 11

Proposal for a directive
Recital 15 a (new)

Text proposed by the Commission	*Amendment*
	(15a) Already existing national cooperation mechanisms between public and private operators should be fully respected when possible and in accordance with Directive 95/46/EC and the provisions stipulated in this Directive should not undermine such established cooperation arrangements.

Amendment 12

Proposal for a directive
Recital 16

Text proposed by the Commission	*Amendment*
(16) To ensure transparency and properly inform EU citizens and market operators, the competent authorities should set up a common website to publish non confidential information on the incidents and risks.	(16) To ensure transparency and properly inform EU citizens and market operators, the competent authorities should set up a common website to publish***, promptly, comprehensive*** non confidential information on the incidents and risks.

Amendment 13

Proposal for a directive
Recital 21

Text proposed by the Commission	*Amendment*
(21) Given the global nature of NIS problems, there is a need for closer international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues.	(21) Given the global nature of NIS problems, there is a need for closer international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues***, with the proviso that the States with which this cooperation is planned have data control and protection instruments which ensure the same level of security as those of the EU***.

Amendment 14

Proposal for a directive
Recital 22

Text proposed by the Commission	*Amendment*
(22) Responsibilities in ensuring NIS lie to a great extent on public administrations and ***market operators***. A culture of risk management, involving risk assessment and the implementation of security measures ***appropriate to the risks faced*** should be promoted and developed through appropriate regulatory requirements and voluntary industry practices. Establishing a level playing field is also essential to the	(22) Responsibilities in ensuring NIS lie to a great extent on public administrations and ***undertakings***. A culture of risk management, involving risk assessment and the implementation of security measures ***which seek to anticipate security incidents, whether deliberate or accidental,*** should be promoted and developed through appropriate regulatory requirements and voluntary industry

effective functioning of the cooperation network to ensure effective cooperation from all Member States.

practices. ***Where such a culture of risk management already exists, and, in particular, where it relies on voluntary practices, it should be supported, strengthened and shared.*** Establishing a level playing field is also essential to the effective functioning of the cooperation network to ensure effective cooperation from all Member States.

Amendment 15

Proposal for a directive
Recital 22 a (new)

Text proposed by the Commission	*Amendment*
	(22a) Public administrations and private undertakings, including network service-providers and suppliers of information and software, should regard the protection of their information systems and of the data which they contain as forming part of their duty of care. Appropriate levels of protection should be provided against reasonably identifiable threats and areas of vulnerability. The cost and burden of such protection should reflect the likely damage which a cyber-attack would cause to those affected.

Amendment 16

Proposal for a directive
Recital 26 a (new)

Text proposed by the Commission	*Amendment*
	(26a) Children are exposed to internet and other modern technology from the very early stage of their lives as well as to threats that come with it. A proper governance of child-friendly online space is crucial to mitigate harm and ensure that the protection of children and their

rights are not compromised;

Amendment 17

Proposal for a directive
Recital 28

Text proposed by the Commission	*Amendment*
(28) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing between market operators and between the public and the private sectors. Publicity of incidents reported to the competent authorities should ***duly balance*** the interest of the public in being informed about threats ***with possible reputational and commercial damages for the public administrations and market operators reporting incidents. In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes.***	(28) Competent authorities should pay due attention to preserving informal and trusted channels of information-sharing between market operators and between the public and the private sectors. Publicity of incidents reported to the competent authorities should ***assign precedence to*** the interest of the public in being informed about threats ***rather than to short-term economic considerations.***

Amendment 18

Proposal for a directive
Recital 29 a (new)

Text proposed by the Commission	*Amendment*
	(29a) A fraudulent use of the internet enables organised crime to expand its activities online for the purposes of money laundering, counterfeiting and other IPR infringing products and services as well as to experiment with new criminal activities, thereby revealing a fearsome ability to adapt to modern technology;

Amendment 19

Proposal for a directive
Recital 30 a (new)

Text proposed by the Commission	*Amendment*
	(30a) Cybercrime is creating increasingly significant economic and social damage affecting millions of consumers and is causing annual losses estimated at EUR 290 billion[4a];
	[4a] According to the Norton Cybercrime Report 2012.

Amendment 20

Proposal for a directive
Recital 33

Text proposed by the Commission	*Amendment*
(33) The Commission should periodically review this Directive, in particular with a view to determining the need for modification in the light of changing technological or market conditions.	(33) The Commission should periodically review this Directive, in particular with a view to determining the need for modification in the light of changing technological or market conditions ***and of obligations geared to the highest level of security and integrity of networks and information and protection of private life and personal data***.

Amendment 21

Proposal for a directive
Recital 39

Text proposed by the Commission	*Amendment*
(39) The sharing of information on risks and incidents within the cooperation network and compliance with the requirements to notify incidents to the	(39) The sharing of information on risks and incidents within the cooperation network and compliance with the requirements to notify incidents to the

national competent authorities may require the processing of personal data. Such a processing of personal data is necessary to meet the objectives of public interest pursued by this Directive ***and is thus*** legitimate under Article 7 of Directive 95/46/EC. It does not ***constitute, in relation to these legitimate aims, a disproportionate and intolerable interference impairing the very substance of*** the right to the protection of personal data guaranteed by Article 8 of the Charter of fundamental rights. In the application of this Directive, Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents[31] should apply as appropriate. When data are processed by Union institutions and bodies, such processing for the purpose of implementing this Directive should comply with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[31] OJ L 145, 31.05.01, p. 43.

national competent authorities may require the processing of personal data. ***Where*** such a processing of personal data is necessary to meet the objectives of public interest pursued by this Directive***, it may be*** legitimate under Article 7 of Directive 95/46/EC. It does not***, however, relieve the competent authorities of the obligation to act proportionately, in a way which is likely not to impair*** the right to the protection of personal data guaranteed by Article 8 of the Charter of fundamental rights. In the application of this Directive, Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents should apply as appropriate[31]. When data are processed by Union institutions and bodies, such processing for the purpose of implementing this Directive should comply with Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[31] OJ L 145, 31.05.01, p. 43.

Amendment 22

Proposal for a directive
Recital 41 a (new)

Text proposed by the Commission	*Amendment*
	(41a) In the case of all measures, fundamental human rights, particularly those referred to in the European Convention on Human Rights (Article 8, respect for private life), should be protected and the principle of

proportionality must be respected.

Amendment 23

Proposal for a directive
Article 1 – paragraph 5

Text proposed by the Commission	*Amendment*
5. This Directive shall ***also be without prejudice to*** Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 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. This Directive shall ***fully respect*** Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and 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 Regulation ***(EC) No 45/2001*** of the European Parliament and of the Council ***of 18 December 2000*** on the protection of individuals with regard to the processing of personal data ***by the Community institutions and bodies*** and on the free movement of such data.

Amendment 24

Proposal for a directive
Article 2

Text proposed by the Commission	*Amendment*
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 ensuring a higher level of security, without prejudice to their obligations under Union law***, but such provisions must comply with the common minimum expectations applicable in this case which are enshrined in this Directive***.

Amendment 25

Proposal for a directive
Article 3 – point 2

Text proposed by the Commission	*Amendment*
(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 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;

Amendment 26

Proposal for a directive
Article 3 – paragraph 2 – point a (new)

Text proposed by the Commission	*Amendment*
	"cyber resilience" means the ability of a network and information system to resist and recover to full operational capacity after incidents, including but not limited to; technical malfunction, power failure or security incidents;

Amendment 27

Proposal for a directive
Article 3 –paragraph 4

Text proposed by the Commission	*Amendment*
"incident" means any circumstance or event having an actual adverse effect on security;	"incident" means any circumstance or event having an actual adverse effect on security ***and the provision of core services***;

Amendment 28

Proposal for a directive

Article 3 – point 8 – point b

Text proposed by the Commission	*Amendment*
(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 ***societal and economic*** activities in the fields of energy, transport, banking, stock exchanges***, food supply chain*** and health, a non-exhaustive list of which is set out in Annex II.

Amendment 29

Proposal for a directive
Article 5 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) A risk assessment ***plan*** to identify risks and assess the impacts of potential incidents;	(a) A risk ***management framework incorporating, at the minimum, regular*** assessment to identify risks and assess the impacts of potential incidents***, and measures to preserve the security and integrity of information, including early warning***;

Justification

An assessment plan is not sufficient, and does not include other measures necessary for the purpose of managing network and information security risks. The EDPS recommends establishing a risk management framework which includes risk assessment.

Amendment 30

Proposal for a directive
Article 5 – paragraph 3

Text proposed by the Commission	*Amendment*
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***, the European Parliament, the Council and the European Data Protection Supervisor*** within one month from their adoption,

which shall be not later than 12 months after the entry into force of this Directive.

Amendment 31

Proposal for a directive
Article 5 – paragraph 3 a (new)

Text proposed by the Commission	*Amendment*
	(3a) The Commission shall summarise the NIS strategies of all the Member States and forward them to all Member States in an organised form.

Justification

It will be useful if the Member States also see one another's plans. It will help them to determine their approaches, and there may even be opportunities for exchanges of best practices.

Amendment 32

Proposal for a directive
Article 5 – paragraph 3 b (new)

Text proposed by the Commission	*Amendment*
	(3b) Within six months after the adoption of this Directive, the Commission shall compile a guide to the structure of the NIS strategy. Its aim shall be to help Member States to draft and adopt documents with approximately the same structure.

Justification

The work of organisation and summarising at Community level may be more effective if the 28 documents on which it is based adhere to a certain general structure. Although the Commission's guide would not be binding, it would still have the effect of inducing Member States to adhere to this recommended model/structure when drafting their own national strategies.

Amendment 33

Proposal for a directive
Article 6 – paragraph 1

Text proposed by the Commission	*Amendment*
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 ***civil*** national competent authority on the security of network and information systems (the "competent authority").

Amendment 34

Proposal for a directive
Article 6 – paragraph 5

Text proposed by the Commission	*Amendment*
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 shall consult and cooperate ***closely*** with the ***competent*** law enforcement national authorities and data protection authorities***, whenever appropriate and taking into account the principle of proportionality***.

Amendment 35

Proposal for a directive
Article 6 – paragraph 5 (new)

Text proposed by the Commission	*Amendment*
	5a. The competent authorities shall comply, as regards the information collected, processed and exchanged, with the requirements on the protection of personal data as set out in Article 17 of Directive 95/46/EC.

Amendment 36

Proposal for a directive
Article 7 – paragraph 1

Text proposed by the Commission	*Amendment*
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 Computer Emergency Response ***Teams*** (hereinafter: '***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. ***Where appropriate, a*** CERT ***shall*** be established within the competent authority.

Amendment 37

Proposal for a directive
Article 8 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The cooperation network shall bring into permanent communication the Commission and the competent authorities. When requested, the European Network and Information Security Agency ('ENISA') shall assist the cooperation network by providing ***its expertise and advice***.	2. The cooperation network shall bring into permanent communication the Commission and the competent authorities. When requested, the European Network and Information Security Agency ('ENISA') shall assist the cooperation network by providing ***technology neutral guidance with suitable measures for both public and private sectors***.

Amendment 38

Proposal for a directive
Article 9 – paragraph 2 – point b a (new)

Text proposed by the Commission	*Amendment*
	(ba) the criteria for the participation of Member States in the secure information sharing system to ensure that a high level of security and resilience is guaranteed by all participants at all steps of the processing, including by appropriate confidentiality and security measures in accordance with Articles 16 and 17 of Directive 95/46/EC and Articles 21 and 22

of Regulation (EC) No 45/2001.

Amendment 39

Proposal for a directive
Article 9 – paragraph 3

Text proposed by the Commission	*Amendment*
3. The Commission shall adopt, by means of implementing acts, decisions on the access of the Member States to this secure infrastructure, pursuant to the criteria referred to in paragraph 2 and 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19(3).	***deleted***

Amendment 40

Proposal for a directive
Article 12 – paragraph 2 – point a – indent 2

Text proposed by the Commission	*Amendment*
– a definition of the ***procedures and the*** criteria for the assessment of the risks and incidents by the cooperation network.	– a definition of the criteria for the assessment of the risks and incidents by the cooperation network.

Amendment 41

Proposal for a directive
Article 13

Text proposed by the Commission	*Amendment*
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***	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 ***only be concluded if a level of*** protection

adequate protection of the personal data circulating on the cooperation network.	of the personal data circulating on the cooperation network ***can be ensured which is adequate and comparable to that of the Union.***

Amendment 42

Proposal for a directive
Article 14 – paragraph 1

Text proposed by the Commission	*Amendment*
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 core services they provide and thus ensure the continuity of the services underpinned by those networks and information systems.	1. Member States shall ensure that public administrations and market operators take appropriate technical and organisational measures to ***detect, effectively*** manage ***and limit*** 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 ***and proportional*** 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 core services they provide and thus ensure the continuity of the services ***and security of the data*** underpinned by those networks and information systems.

Amendment 43

Proposal for a directive
Article 14 – paragraph 2 point a (new)

	Amendment
	(a) Commercial software producers shall be held responsible despite non liability clauses in users' agreement in case of gross negligence regarding safety and security.

Justification

In the license agreement, commercial software producers absolve themselves from all liability that may arise due to a poor security mind-set and inferior programming. To promote the software producers to invest in security measures, a different culture is required. It can only be realised if the software producers are held responsible for any shortcomings in security.

Amendment 44

Proposal for a directive
Article 14 – paragraph 3

Text proposed by the Commission	*Amendment*
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 and 2 apply to all market operators ***and software producers*** providing services within the European Union.

Amendment 45

Proposal for a directive
Article 14 – paragraph 6

Text proposed by the Commission	*Amendment*
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.	***deleted***

Amendment 46

Proposal for a directive
Article 15 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that the competent authorities have ***all*** the powers necessary to investigate cases of non-compliance of public administrations or	1. Member States shall ensure that the competent authorities have 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.	market operators with their obligations under Article 14 and the effects thereof on the security of networks and information systems.

Amendment 47

Proposal for a directive
Article 15 – paragraph 5

Text proposed by the Commission	*Amendment*
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 law, and in full consultation with the relevant data controllers and processors,*** 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.

Amendment 48

Proposal for a directive
Article 19 a (new)

Text proposed by the Commission	*Amendment*
	Article 19a
	Protection and processing of personal data
	1. Any processing of personal data in the Member States pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC and Directive 2002/58/EC.
	2. Any processing of personal data by the Commission and ENISA pursuant to this Regulation shall be carried out in accordance with Regulation (EC) No 45/2001.
	3. Any processing of personal data by the

	CyberCrime Center within Europol for the purposes of this Directive shall be carried out pursuant to Decision 2009/371/JHA.
	4. The processing of personal data shall be fair and lawful and strictly limited to the minimum data needed for the purposes for which they are processed. They shall be kept in a form which permits the identification of data subjects for no longer than necessary for the purpose for which the personal data are processed.
	5. Incident notifications referred to in Article 14 shall be without prejudice to the provisions and obligations regarding personal data breach notifications set out in Article 4 of Directive 2002/58/EC and in Regulation (EU) No 611/2013.
	6. References to Directive 95/46/EC shall be construed as references 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 (General Data Protection Regulation) once it will be in force.

Amendment 49

Proposal for a directive
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
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 and report to the European Parliament and the Council. The first report shall be submitted no later than ***two*** 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.

Amendment 50

Proposal for a directive
Annex 1 – paragraph 1 – point 1 – point b

Text proposed by the Commission	*Amendment*
(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 CERT shall implement and manage security measures to ensure the confidentiality, integrity, availability and authenticity of information it receives and treats ***and ensure data protection***.

Amendment 51

Proposal for a directive
Annex 2 – paragraph 1

Text proposed by the Commission	*Amendment*
List of market operators	List of market operators
Referred to in Article 3(8)a)	Referred to in Article 3(8)a)
1. e-commerce platforms	1. e-commerce platforms
2. Internet payment gateways	2. Internet payment gateways
3. Social networks	
4. Search engines	***3***. Search engines
5. Cloud computing services	***4.*** Cloud computing services ***that store critical infrastructure data of the European Union***
6. Application stores	

Amendment 52

Proposal for a directive
Annex 2 – paragraph 2 – point 5 a (new)

Text proposed by the Commission	*Amendment*
	5a. Food supply chain

PROCEDURE

Title	High common level of network and information security across the Union
References	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Committee responsible Date announced in plenary	IMCO 15.4.2013
Opinion by Date announced in plenary	LIBE 15.4.2013
Associated committee(s) - date announced in plenary	12.9.2013
Rapporteur Date appointed	Carl Schlyter 7.3.2013
Discussed in committee	25.4.2013 18.9.2013 4.11.2013 13.1.2014
Date adopted	13.1.2014
Result of final vote	+: 36 –: 6 0: 0
Members present for the final vote	Jan Philipp Albrecht, Roberta Angelilli, Edit Bauer, Rita Borsellino, Arkadiusz Tomasz Bratkowski, Philip Claeys, Frank Engel, Cornelia Ernst, Tanja Fajon, Monika Flašíková Beňová, Kinga Gál, Kinga Göncz, Salvatore Iacolino, Sophia in ‘t Veld, Timothy Kirkhope, Juan Fernando López Aguilar, Baroness Sarah Ludford, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Anthea McIntyre, Nuno Melo, Roberta Metsola, Claude Moraes, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Renate Sommer, Axel Voss, Renate Weber, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra
Substitute(s) present for the final vote	Monika Hohlmeier, Jean Lambert, Ulrike Lunacek, Jan Mulder, Carl Schlyter, Marco Scurria
Substitute(s) under Rule 187(2) present for the final vote	Katarína Neveďalová