EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2013/0027(COD)

2.9.2013

DRAFT 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 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.

Or. en

Amendment 2

Proposal for a directive
Recital 32 a (new)

Text proposed by the Commission	*Amendment*
	(32a) Adopting at EU level general data protection legislation should precede the adoption of cybersecurity legislation at EU level. Therefore, the NIS directive should be adopted only after the General Data Protection Regulation has been adopted.

Or. en

Amendment 3

Proposal for a directive
Article 1 – paragraph 5

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

Or. en

Justification

Although reference to Regulation (EC) No 45/2001 exists in Recital 39, it is necessary here as well, in accordance with EDPS opinion.

Amendment 4

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;

Or. en

Amendment 5

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***;

Or. en

Amendment 6

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;***

Or. en

Justification

The obligation to establish a "risk assessment plan" is too narrow as such wording does not include other activities required when managing information security risks. The EDPS recommends setting up and maintaining a risk management framework, which of course implies also a risk assessment phase.

Amendment 7

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").

Or. en

Amendment 8

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.

Or. en

Amendment 9

Proposal for a directive
Article 8 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
Within the cooperation network the competent authorities shall:	Within the cooperation network the competent authorities***, ensuring that only the data strictly necessary for the purpose to be achieved are collected and processed and that the provisions in the General Data Protection Regulation are complied with,*** shall:

Or. en

Amendment 10

Proposal for a directive
Article 9 – paragraph 1 a (new)

Text proposed by the Commission	*Amendment*
	1a. Personal data shall be only disclosed to recipients who need to process these data for the performance of their tasks in accordance with an appropriate legal basis. The disclosed data shall be limited to what is necessary for the performance of their tasks. Compliance with the purpose limitation principle shall be ensured. The time limit for the retention of these data shall be specified for the purposes set out in this Directive.

Or. en

Amendment 11

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.

Or. en

Amendment 12

Proposal for a directive
Article 10 – paragraph 2

Text proposed by the Commission	*Amendment*
2. In the early warnings, the competent authorities and the Commission shall communicate any relevant information in their possession that may be useful for assessing the risk or incident.	2. In the early warnings, the competent authorities and the Commission shall communicate any relevant information in their possession that may be useful for assessing the risk or incident, ***in accordance with the provisions of the General Data Protection Regulation.***

Or. en

Amendment 13

Proposal for a directive
Article 10 – paragraph 3

Text proposed by the Commission	*Amendment*
3. At the request of a Member State, or on its own initiative, the Commission may request a Member State to provide any relevant information on a specific risk or incident.	3. At the request of a Member State, or on its own initiative, the Commission may request a Member State to provide any relevant information on a specific risk or incident, ***in accordance with the provisions of the General Data Protection Regulation.***

Or. en

Amendment 14

Proposal for a directive
Article 10 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Where the risk or incident subject to an early warning is of a suspected criminal nature, the competent authorities or the Commission shall inform the European	4. Where the risk or incident subject to an early warning is of a suspected criminal nature, the competent authorities or the Commission shall inform the European

Cybercrime Centre within Europol	Cybercrime Centre within Europol***, in accordance with the provisions in the General Data Protection Regulation.***

Or. en

Amendment 15

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

Text proposed by the Commission	*Amendment*
	2a. Software producers shall be responsible for correcting security breaches, within 24 hours of being informed for serious cases, and 72 hours for cases were the effects are unlikely to result in any significant financial loss or serious breach of privacy.

Or. en

Amendment 16

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

Text proposed by the Commission	*Amendment*
	2b. Commercial software producers shall not be protected from "no-liability" clauses when it can be demonstrated that their products are not properly designed to handle foreseeable security threats.

Or. en

Amendment 17

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. ***Incident notifications under paragraph 2 shall apply without prejudice to personal data breach notification obligations in accordance with applicable data protection law.***

Or. en

Amendment 18

Proposal for a directive
Annex I – paragraph 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***, complying with data protection requirements***.

Or. en

Amendment 19

Proposal for a directive
Annex II

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
6. Application stores	

Or. en