Opinion of the European Data Protection Supervisor

on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard 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[1],

Having regard to 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[2], and in particular Article 28(2) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 7 February 2013, the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy adopted a Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a "Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace"[3] (hereafter 'the Joint Communication', 'the Cyber Security Strategy' or 'the Strategy').

2. On the same date, the Commission adopted a proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] JOIN (2013) 1 final.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

common level of network and information security across the Union[4] (hereafter 'the proposed Directive' or 'the Proposal'). This Proposal was sent to the EDPS for consultation on 7 February 2013.

3. Before the adoption of the Joint Communication and of the Proposal, the EDPS was given the possibility to provide informal comments to the Commission. He welcomes that some of his comments have been taken into account in the Joint Communication and in the Proposal.

1.2. Objectives of the Cyber Security Strategy and of the proposed Directive

4. The Joint Communication establishes the cyber-security strategy of the EU and provides the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks[5]. It identifies five strategic priorities and actions:

   - Achieving cyber resilience[6];
   - Drastically reducing cybercrime[7];
   - Developing cyber defence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP)[8];
   - Developing the industrial and technological resources for cyber-security;
   - Establishing a coherent international cyberspace policy for the European Union and promoting EU core values.

5. Section 1.2 of the Joint Communication provides that actions identified in the Cyber Security Strategy will be guided by the respect of EU core values and the protection of the fundamental rights and freedoms enshrined in the Charter of Fundamental Rights of the EU, in particular personal data and privacy.

6. The Joint Communication puts forward a shared agenda for Member States, the Commission, the European Parliament, the Council, ENISA, Europol and the industry, in working together on the goals of the Strategy. It proposes to gather all relevant parties in a high-level conference and assess progress in 12 months.

---

[4] COM (2013) 48 final.

[5] See European Commission and European Union External Action press release IP/13/94, 7 February 2013.

[6] The concept of 'cyber resilience' is not defined in the Joint Communication or the proposed Directive on NIS. It may however be understood within the meaning of security as defined in the proposed Directive, possibly with the additional element of the ability of a system to recover from the effects of a security incident to full operational capacity. The lack of clarity of this central term of the Communication is regrettable and constitutes an important weakness of the strategy.

[7] 'Cybercrime' is defined in footnote 5 of the Joint Communication as *"commonly refer[ring] to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)."*

[8] There is no definition of 'cyber defence' in the Joint Communication. The actions planned in that field aim at increasing the resilience of the communication and information systems supporting Member States' defence and national security interests.

7. The proposed Directive is put forward as one of the main measures that will help implementing action 1 of the Cyber Security Strategy, the aim of which is to help 'Achieving cyber resilience'. The objective of the Proposal is to ensure a high common level of network and information security (NIS) across the EU. In particular, the Proposal provides for:

    - mandatory measures upon Member States to prevent, manage and respond to risks and incidents affecting network and information systems;
    - the creation of a cooperation mechanism among Member States and the Commission to share, in a coordinated and efficient manner through a secure infrastructure, early warnings on risks and incidents, as well as to cooperate and to organise regular peer reviews; and
    - the obligation for market operators and public administrations to adopt risk management practices and to report major security incidents on their core services.

1.3. Relevance of data protection for the Cyber Security package and aim of the EDPS Opinion

8. The EDPS welcomes that the EU has put forward a comprehensive strategy on increasing security on the Internet[9], complemented by a proposed Directive on measures to ensure a high common level of network and information security (NIS) across the EU. Several regions in the world have or are in the process of adopting cyber security strategies to tackle the risks and threats occurring over the Internet. It became essential that the EU adopted its own strategy to face these issues in a manner that also takes consideration of the international dimension of the security challenges that are being faced in cyberspace.

9. The Cyber Security Strategy is in continuity with the policy that has been developed by the EU in the area of Network and Information Security (NIS): in 2001, the Commission issued a Communication on "Network and Information Security: Proposal for a European Policy Approach"[10] and in 2006 it released a Strategy for a Secure Information Society[11]. For many years, the focus of the EU policy in the area of NIS has been put primarily on security. In that context, the rights to privacy and data protection have long been perceived as conflicting with the objective of security ("security v privacy"), so that they have been addressed until now only marginally in the EU policy on NIS. From this perspective, the EDPS welcomes the explicit recognition of privacy and data protection in the Strategy and the fact that they are being considered as core values which should guide cyber security policy in the EU and internationally[12].

[9] The lack of a comprehensive EU internal security strategy was notably raised in the EDPS Opinion on the Communication from the Commission to the European Parliament and the Council - "EU Internal Security Strategy in action: five steps towards a more secure Europe", issued on 17 December 2010, OJ C 101/6.
[10] COM(2001)298.
[11] COM(2006)251.
[12] See section 1.2. page 3.

10. Due to the ever growing use of Information and Communication Technologies (ICT), the EDPS believes that measures aimed at ensuring a high level of security on the Internet should help improve the security of all the information processed therein, including personal data. The EDPS underlines that security of data processing has always been a crucial element of data protection[13]. In such context, the adoption by the EU of a Cyber Security Strategy and of a proposed Directive on a high common level of NIS can play a fundamental role in contributing to ensuring the protection of individuals' rights to privacy and data protection in the online environment[14].

11. On the other hand, the EDPS underlines that the pursuance of the objective of cyber security may lead to deploying measures that interfere with individuals' rights to privacy and the protection of their personal data, as guaranteed in the European Convention on Human Rights, the Treaty on the Functioning of the EU and the Charter of Fundamental Rights of the EU[15]. The EDPS recalls that any interference with, or limitation to, the fundamental rights of individuals must comply with Article 52(1) of the Charter of Fundamental Rights of the EU. Considering that a growing amount of personal data is being processed through information systems and networks, it must be ensured that all the measures implemented in the frame of the Cyber Security Strategy to monitor and improve the security of information systems and networks do not lead to intruding in the privacy of individuals in a disproportionate manner, for instance by unduly accessing their personal data.

12. As a result, the EDPS underlines the importance that all relevant fundamental rights are properly taken into account in the Cyber Security Strategy and in all its implementing actions, including, on the one hand, the protection of individuals against cyber security threats and, on the other hand, the protection of their privacy and of the right to the protection of their personal data. The EDPS stresses that any policy implemented in the EU as regards cyber security, and any measure thereof, should be carefully crafted so as to avoid any unlawful interference with individuals' rights to privacy and data protection, in particular by ensuring that they respect the principles of necessity and proportionality as well as applicable data protection law.

13. The EDPS takes note that the explanatory memorandum of the proposed Directive recognizes in its section 1.3 that all players that are data controllers are obliged by the data protection framework to put in place security measures to protect personal data, and that this obligation is being developed further with the ongoing reform of the data protection framework, including a notification obligation for breaches. The Cyber Security Strategy in its section

[13] Security requirements are contained in Articles 22 and 35 of Regulation (EC) No 45/2001, Articles 16 and 17 of Directive 95/46/EC and Articles 4 and 5 of Directive 2002/58/EC, as well as in Article 7 of the Convention on Data Protection, adopted in 1981 in the context of the Council of Europe and by now ratified by all EU Member States.

[14] See also speech by Ms. Viviane Reding, Vice-President of the European Commission, "The EU's data protection rules and the Cyber Security Strategy: two sides of the same coin", 19 May 2013, http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm?locale=en

[15] See Article 8 ECHR, Article 16 TFEU and Articles 7 and 8 of the Charter.

2.1 also recognises that the current data protection framework requires data controllers to ensure data protection requirements and safeguards, including measures related to security. Given that a huge part of all network and information operations considered in the Strategy and the proposed Directive will concern the processing of personal data, the obligation set forth in data protection law is probably the most comprehensive network and information security obligation under EU law. It must also be noted that the principles for setting up the appropriate technical and organisational security measures, based on risk assessment and management, and considering the state of the art and cost of the measure, put forward in the proposed Directive are the same as those already set forth in data protection legislation.

14. It is, however, regrettable that the Cyber Security Strategy and the proposed Directive do not underline better the contribution of existing and forthcoming data protection law to security and fail to fully ensure that any obligations resulting from the proposed Directive or other elements of the Strategy are complementary with data protection obligations and do not overlap or contradict each other. The important role of DPAs in implementation and enforcement of these obligations is not properly considered either. These aspects will be analysed further in chapters 2 and 3 below as regards, on the one hand, the EU Cyber Security Strategy and, on the other hand, the proposed Directive on NIS.

2. ANALYSIS OF THE EU CYBER SECURITY STRATEGY

2.1. General comments on the EU Cyber Security Strategy

15. The EDPS notes that the proposed General Data Protection Regulation[16] has not been taken into account in the Cyber Security Strategy. Also the ongoing initiative for a Regulation on electronic identification and trust services for electronic transactions in the internal market[17] has not been considered in the Cyber Security Strategy. It is only indirectly referred to in the proposed Directive through the exclusion of trust service providers from its scope. It is regrettable that the role of trust services and secure electronic identification services has not been properly analysed in the preparation of the Cyber Security Strategy[18].

16. Due to the lack of a careful consideration and taking full account of other parallel Commission initiatives and ongoing legislative procedures, such as the Data Protection Reform and the proposed Regulation on electronic identification and trust services, the Cyber Security Strategy fails to provide a really comprehensive and holistic view of cyber security in the EU and risks to perpetuate a fragmented and compartmentalised approach.

[16] COM (2012) 11 final
[17] COM (2012) 238 final
[18] The data protection issues raised in this context are underlined in the EDPS opinion of 27 September 2012 on the Commission proposal for a Regulation of the European Parliament and of the Council on trust and confidence in electronic transactions in the internal market (Electronic Trust Services Regulation), available on the Consultation section of the EDPS website at: www.edps.europa.eu.

17. The Joint Communication underlines a number of principles, including the rights to privacy and data protection, which should guide cyber security policy in the EU and internationally. It acknowledges that, at an international level, the EU has a role to play by promoting freedom online and ensuring respect of fundamental rights online[19]. The EDPS welcomes that the protection of the fundamental rights to privacy and data protection has been explicitly mentioned as one of the guiding principles of the Cyber Security Strategy.

18. The EDPS also notes with satisfaction that explicit references to privacy and data protection requirements have been included in several actions of the Strategy. For instance:
    - The Joint Communication explicitly indicates, on page 4, that 'any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU law and take full account of the individuals' rights in this field';
    - Footnote 7 on page 4 indicates that the actions of the Strategy related to information sharing should be compliant with EU data protection law when personal data is at stake;
    - In section 2.5 there is an explicit mention of the need for appropriate guarantees for the transfer of personal data to third countries;
    - Security obligations stemming from applicable data protection legislations are explicitly mentioned in section 2.1;
    - Privacy by design is considered in section 2.4 as an incentive that will be encouraged from ICT product manufacturers and service providers.

19. The EDPS, however, notes that there is no specific mention of privacy and data protection requirements in the sections relating to the fight against cyber criminality and the cyber defence policy. In any case, as will be developed further below in section 2.1.2, privacy and data protection requirements must also be taken into consideration in these fields of action.

20. It is welcomed that the role and involvement of data protection authorities in the fight for cyber security is underlined in section 2.1 in relation to awareness raising actions and to the proposed Directive on NIS, and in section 3.2 with respect to incidents having compromised personal data. However, the EDPS emphasises that data protection authorities have a role to play in all actions of the Cyber Security Strategy and not only in the ones where this role has been explicitly mentioned. This will be developed further in section 2.1.3 below.

2.2. Specific comments on the EU Cyber Security Strategy

2.2.1. Delineating the scope of the actions planned in the Cyber Security Strategy

21. The Cyber Security Strategy aims at establishing a holistic approach to 'cyber security' by tackling different aspects of it in various areas such as cyber resilience, cybercrime, and cyberdefence. The EDPS acknowledges that many policy aspects, including technical security aspects and beyond, need to be carefully considered in order to ensure an appropriate protection of network

[19] See Joint Communication, p.3.

and information systems as well as of the information transmitted therein. From a data protection perspective, the EDPS believes that, by contributing to enhancing the security in the digital space, actions planned for the purpose of strengthening cyber resilience and the fight against cybercrime can particularly help protect personal data in cyberspace.

22. With regard to taxonomy - and especially the definition of 'cyber security', 'cyber resilience', 'cybercrime' and 'cyberdefence' - the EDPS notes that an effort has been made by the Commission to define some of these concepts for the purpose of the Joint Communication (in particular in footnotes 4 and 5 thereof). However, as can be inferred from the footnotes in section 1.2 above, the notions of 'cyber resilience', 'cybercrime' and 'cyberdefence' are not necessarily self explanatory or clearly defined. As a result, it is not always clear what they mean and, as a result, what the scope of the actions planned in the Joint Communication is. Although the Communication is a non-binding policy document, it would have been helpful to define these notions more precisely so that there is a clear common understanding of what is being referred to and a clear common understanding of the scope of the actions planned in the Joint Communication.

23. From a data protection perspective, the issue of taxonomy is particularly important since these terms are being used as a justification for certain special measures which could cause interference with fundamental rights, including the rights to privacy and data protection. This is especially the case as regards actions in the field of 'cyber resilience' and 'cybercrime'.

24. With regard to actions aimed at improving 'cyber resilience', the EDPS welcomes that the Joint Communication makes reference to applicable and proposed EU legislation in the field of Network and Information Security. One of the main actions of the Joint Communication in that area consists in the proposed Directive on NIS, which aims at establishing an integrated EU approach to security. The EDPS notes that the actions planned in that area would take place within the (current or future) EU legal framework, and that their scope would therefore be clearly circumscribed by law[20].

25. In respect of actions aimed at reducing 'cybercrime', the Joint Communication attempts to provide a definition of the term 'cybercrime' in a footnote at the bottom of page 3. The EDPS supports this attempt to define the notion for obvious reasons of legal certainty. However, in the EDPS' view, the definition adopted for the purpose of the Strategy is still quite vague and broad, as it generally encompasses any type of *'criminal activities where computers and information systems are involved either as a primary tool or as a primary target. (...)*'. The Joint Communication further makes reference, in a non-exhaustive manner, to several EU legal instruments in that field[21]. However, it must be noted that EU legislation tackles only very specific aspects of crimes

[20] It must be noted that proposed legislation in that field, such as the Proposal for a Directive on NIS that has been put forward in connection with the Strategy, may have an impact on data protection and must therefore be carefully crafted so as to avoid any unlawful interference with privacy and data protection rights.

[21] See in particular section 2.2., "Strong and effective legislation", p. 9

committed online[22], and that there is not yet a single legal framework providing for a comprehensive definition of the offences that are being referred to by the term 'cybercrime'. In the absence of a common definition of the notion of 'cybercrime' in the legal framework of the EU, several measures planned in the Strategy relating to the fight against 'cybercrime' (such as measures to strengthen cooperation amongst law enforcement bodies) are not clearly linked to precise and well-defined offences.

26. The Joint Communication also makes reference to the provisions of the Council of Europe 2001 Budapest Convention on Cybercrime as providing an effective framework for the adoption of national legislation to tackle cybercrime. The Budapest Convention lists a number of offences that would fall within the notion of 'cybercrime', such as offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; offences related to infringements of copyright and related rights. However, in addition to the fact that this list remains very broad, as pointed out in the Joint Communication, the Budapest Convention has not been ratified by all Member States yet, and therefore the offences covered under the term 'cybercrime' are not harmonised in the criminal laws of the Member States of the EU. Considering, furthermore, that measures taken in the area of law enforcement are more likely to interfere with individuals' rights, it would be preferable to have a clear and *restrictive* definition of 'cybercrime' rather than an overreaching one.

2.2.2. Applicability of data protection law to all areas of action of the EU Cyber Security Strategy

27. Whenever EU policies and legislation touch upon the functioning and use of network and information systems, through which an ever growing amount of personal data is processed, it must be acknowledged that privacy and data protection legal requirements play an essential role therein and that they must necessarily be taken in due consideration.

28. As mentioned in point 18 above, the EDPS welcomes that reference is made to privacy and data protection legal requirements in several places of the Joint Communication: they are mentioned at the beginning of the Strategy, as guiding principles for cybersecurity policy, as well as in specific actions, such as those relating to cyber resilience, the development of industrial and technological resources for cybersecurity, and the establishment of a coherent international cyberspace policy for the European Union.

[22] For instance, Council Framework Decision 2005/222/JHA on attacks against information systems[22]; Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography; Council Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment.

29. However, the EDPS notes with regret the absence of a specific reference to data protection law in the sections relating to the fight against cybercrime (section 2.2)[23] and to developing a cyberdefence policy (section 2.3). Although the Strategy does not clearly state it, the EDPS notes that many of the actions planned in those areas will likely involve the processing and exchange of personal data.

30. With respect to the fight against cybercrime, the EDPS underlines that the measures that are planned in the Strategy will often require collecting, exchanging and assessing personal data of individuals (such as names and IP addresses), including those of victims of crime and of suspected offenders, whose processing entails specific risks for the privacy and data protection of these individuals. This is likely the case, for example, as regards measures aimed at enhancing operational capability and coordination between law enforcement bodies. The processing of personal data in the area of police and judicial cooperation in criminal matters requires a high level of data protection due to its intrusive nature and the major impact such processing may have on the individual's life.

31. The exchanges of personal data between law enforcement authorities in the EU in the context of investigation and prosecution of crimes must currently respect the data protection requirements laid down in Council Decision 2008/977/JHA[24]. A proposal for a Directive governing the processing of personal data in the area of police and judicial cooperation in criminal matters is currently being examined by the European Parliament and the Council[25], which is meant to replace the Council Framework Decision. This instrument will become the data protection norm applicable to the processing of data by law enforcement authorities in the EU, governing both the processing of personal data by those authorities and their exchange of personal data with other recipients.

32. As underlined in previous opinions[26], the EDPS is convinced that actions to fight cybercrime must be deployed with carefully drafted data protection safeguards, to ensure that the monitoring and processing of personal data by law enforcement will only be done in a strictly targeted way, in a proportionate manner, and with an appropriate consideration of data subjects' rights. For instance, measures aimed at enhancing operational capability between law enforcement agencies, including the European Cybercrime

[23] Except for the specific case of ICANN, where measures to increase the accountability of registrars of domain names and ensure accuracy of information on website ownership should be in compliance with EU law, including the rules on data protection, see page 10.

[24] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30/12/2008 p.0060-0071.

[25] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data, COM (2010) 010 final.

[26] See in particular EDPS Opinion on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre, 29 June 2012, available on the Consultation section of the EDPS website at: www.edps.europa.eu.

Centre, should be deployed only in accordance with a clear legal basis defining with sufficient precision the extent of the operational capability to be deployed (such as the types of crimes targeted, the types of operational tools, whether they involve processing personal data and the modalities of such processing)[27]. Any such measure should be deployed only after having met the conditions of necessity and proportionality.

33. With regard to the area of the defence policy, the EDPS notes that several actions will likely involve, to some extent, the processing of personal data. This is for example likely the case as concerns measures such as improving information sharing, information exchange and early warning or incident response between civilian and military actors in the EU, which may allow the exchange of personal data (such as IP addresses and names of contact persons within organisations concerned). The processing of personal data in that area falls within the scope of Directive 95/46/EC. Specific exemptions to restrict the scope of the obligations and rights in that case can be applied pursuant to its Article 13, where necessary.

34. Finally, and more generally, the EDPS underlines the importance of defining appropriate data protection safeguards when implementing measures aimed at improving the coordination of various stakeholders. The strengthening of coordination between stakeholders is envisaged in many areas of the Strategy, such as cybercrime, cyberdefence, and EU external relations. It must be particularly clarified whether or not, and if so, with which modalities, such coordination may require the exchange of personal data of individuals (e.g. between competent authorities only or with private sector; based within the EU or outside the EU). It must be ensured that any processing of personal data carried out in the context of coordination mechanisms is respectful of individuals' rights to privacy and data protection. Some account has been taken in the Strategy of the need to respect a high level of data protection for transfers of personal data to third countries (section 2.5), which is welcomed. However, more efforts need to be made when putting into place the coordination mechanisms envisaged in the Strategy, so that appropriate data protection safeguards are defined as concerns the modalities for exchanging personal data.

2.2.3. Role of Data Protection Authorities in the protection of Cyber Security

35. Data Protection Authorities (DPAs) play an important role in the context of Cyber Security. As guardians of the privacy and data protection rights of individuals, DPAs are actively engaged in the protection of their personal data, both offline and online. As part of their mandate, they carry out investigations, handle complaints, perform prior checking and provide opinions on data processing operations, including those taking place online and through electronic communication networks[28]. In this respect, it must be underlined that the security of personal data is an important component of their tasks (for instance, in supervising compliance with Article 17 of Directive 95/46/EC).

[27] See also EDPS Opinion on the European Cybercrime Centre, *ibid*.
[28] Their tasks and powers are defined in Article 28 of Directive 95/46/EC.

They will furthermore play a role in supervising the processing of personal data carried out by the players involved in the implementation of the Cyber Security Strategy.

36. The EDPS therefore regrets that DPAs are not mentioned as relevant players in the field of cyber security in section 3 of the Strategy and in the picture showing the main actors on page 17. Amongst others, section 3 lists NIS authorities/CERTs, law enforcement and defence authorities, ENISA as having a special role and responsibility either at national, European or international level. However, as underlined above, DPAs also play a role in enhancing cyber security. This requires that DPAs are appropriately involved by the players mentioned above but also independently of them in view of their mandate.

37. This means that, on the one hand, DPAs should be appropriately involved, in their capacity of supervisory bodies, as concerns implementing measures that involve the processing of personal data. For instance, measures to be deployed pursuant to section 2.1 on 'Achieving cyber resilience' include the launch of an EU pilot project on fighting botnets and malware. Given that measures in this context could affect privacy and the protection of personal data of individuals, the EDPS advises that the implementation of the pilot project should take place under the supervision of the competent data protection supervisory authorities.

38. On the other hand, DPAs should be recognised as relevant players in the area of cyber security, so that the cooperation envisaged between the different players mentioned in section 3 of the Strategy also extends to them. The Strategy recognises to some extent the need for such cooperation with DPAs in case where a security incident seems to have compromised personal data[29]. However, such cooperation should not be restricted to the mandate of DPAs in the field of the investigation and supervision of personal data breaches. NIS competent authorities, CERTs, ENISA, and law enforcement bodies should generally cooperate with DPAs in the exchange of best practices as well as in awareness raising actions in the field of cyber security. Similarly, the EDPS and national DPAs should be appropriately involved in the high-level conference that will be convened in 2014 to assess progress on the implementation of the Strategy, since they are relevant actors in that field.

3. ANALYSIS OF THE PROPOSED DIRECTIVE

3.1. General comments on the proposed Directive

3.1.1. Ensuring that the deployment of NIS is in full compliance with data protection law

39. The EDPS welcomes the explicit reference in Article 1(5) of the Proposal to the currently applicable data protection framework in the EU, in particular

[29] See p. 19.

Directive 95/46/EC and Directive 2002/58/EC[30]. He also welcomes the fact that recital 41 of the Proposal provides that the implementation of the proposed Directive must be in line with the Charter of Fundamental Rights of the European Union and in particular with the rights to the respect for private life, communications, and the protection of personal data. He notes that although recital 39 mentions compliance with Regulation (EC) No 45/2001 as concerns the processing of personal data by EU institutions and bodies, such a reference is omitted in Article 1(5). The EDPS advises the legislators to also include a reference to Regulation (EC) No 45/2001 in Article 1(5) of the Proposal.

40. The EDPS further welcomes that the Proposal takes some account[31] of the proposed Data Protection Regulation[32], which will replace Directive 95/46/EC in setting forth the general rules applicable to data processing operations by private sector and public administrations. Article 1(5) of the Proposal stresses that compliance with those rules will have to be ensured when the proposed Data Protection Regulation comes into force. Article 17 requires Member States to ensure that the sanctions to be laid down in case of a security incident which involves personal data are consistent with the sanctions set forth in the then binding Data Protection Regulation.

41. It is, however, regrettable that the interaction of the current and future data protection legal frameworks with the proposed Directive on NIS has not been analysed in greater details and that it has not been more clearly spelled out in the Proposal how this interaction would work. As will be analysed in further details in the sections below, the Proposal leaves many questions opened on issues such as:

- the relationship between the security obligations contained therein and other security obligations laid down in other legal instruments (such as the current and future data protection frameworks, the telecom framework, and the proposed Regulation on electronic identification and trust services for electronic transactions) and the level of security to be applied by the concerned operators;
- the obligations of NIS competent authorities as to the level of confidentiality and security that they should ensure to the data they receive under the new incident notification procedure;
- the content of the incident notification, and whether and which personal data it may include (left to be decided through delegated acts);
- the modalities of the interaction of NIS competent authorities with DPAs, and with ENISA, in case the incident involves personal.

[30] 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 (so called 'ePrivacy Directive').
[31] See Articles 1(5) and 17 of the proposed Directive.
[32] COM (2012) 11 final.

42. Furthermore, the EDPS underlines the necessity - stemming from the current data protection framework as well as the proposed Data Protection Regulation - to embed privacy/data protection by design and by default[33] in the design and operation of the mechanisms provided for by the proposed Directive[34]. The EDPS therefore advises inserting a provision in the Proposal requiring to consider data protection from the early stage of the design of the mechanisms established in the Proposal and through the whole lifecycle of processes, procedures, organisations, techniques and infrastructures involved. A recital should be added to explain this need also in the context of the proposed Data Protection Regulation.

3.1.2. The scope of the Proposal

43. The proposed Directive requires, amongst others, Member States to impose security obligations upon public administrations and on those 'market operators' defined in Article 3(8). The definition of 'market operators' refers to key providers of information society services and operators of critical infrastructures in the field of energy, transport, banking, stock exchanges, internet services and health. A non-exhaustive list of the market operators that fall within the scope of the Proposal is set out in Annex II, which specifically lists the following key providers of information services: e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services, and application stores.

44. Although the obligation set forth in the Proposal to ensure that private sector and public administration respect minimum security requirements is welcomed, the EDPS notes that several security obligations are already set forth in the applicable EU legal framework upon providers of electronic communications networks and services under the Framework Directive 2002/21/EC and upon data controllers under data protection law[35]. The EDPS believes that an integrated approach to security is necessary to mitigate risks in respect of NIS, which in turn also contributes to mitigating risks to privacy and data protection. This is all the more important in increasingly interconnected digital environments where accidental and intentional disruptions can easily propagate from one system to another. The EDPS is of the view, as noted in point 13 above, that the security obligation set forth in data protection law is probably the most comprehensive network and information security obligation under EU law. In that regard, the proposed Directive does not yet offer a fully integrated approach to security, as will be demonstrated further below.

45. First, it is not clearly defined in an exhaustive manner in the Proposal which market operators would fall within the scope of the Proposal. The Proposal defines a non-exhaustive list of the market operators concerned, which may be extended further to other players, in a non-harmonised manner, by Member

[33] See Article 23 of the proposed General Data Protection Regulation.
[34] See also EDPS Opinion on the Communication from the Commission on 'The Digital Agenda for Europe - Driving European growth digitally', 10 April 2013, available on the Consultation section of the EDPS website at: www.edps.europa.eu.
[35] See footnote 13.

States. It can also be questioned why certain sectors that play an important role in network and information security have not been included in the list, such as manufacturers of hardware and software or providers of security software and services. Furthermore, the current drafting of the Proposal is not fully clear about whether or not EU institutions and bodies fall within the scope of the Proposal. Recital 39 seems to imply that they do, however that should be made clearer in Article 1 of the Proposal. The EDPS therefore advises the legislators to provide more clarity and certainty in Article 3(8) on the definition of the market operators that fall within the scope of the Proposal, and that they set up an exhaustive list that includes all relevant stakeholders, with a view to ensuring a fully harmonised and integrated approach to security within the EU. The EDPS further advises to clarify in Article 1(2)(c) that the Proposal also applies to EU institutions and bodies.

46. Second, the adoption of an integrated approach to security is also challenged by the fact that several operators are expressly excluded from the scope of the Proposal. Article 1(3)[36] of the Proposal takes account of current legal obligations already imposed on public communication networks and publicly available electronic communication services, as defined in Directive 2002/21/EC. Article 1(3) therefore excludes them from the scope of the Proposal. Article 1(3) also excludes trust service providers from the scope of the Proposal, as they will become subject to the obligations set forth in the proposed Regulation on electronic identification and trust services for electronic transactions in the internal market[37]. Such exclusions can appear confusing since they let several legal frameworks coexist, without clarifying how they interact with each other. In particular, it should be clarified whether the level of security required in Directive 2002/21/EC should also be applicable to the operators falling within the scope of the proposed Directive. The EDPS recommends that a more horizontal role for this Proposal is acknowledged in respect of security requirements, by explicitly providing in Article 1 that it should apply without prejudice to existing or future more detailed rules in specific areas (such as those to be set forth upon trust service providers in the proposed Regulation on electronic identification).

3.2. Specific comments on the proposed Directive

3.2.1. On the definitions provided in the proposed Directive

47. It should be clarified whether the definition of 'network and information system' in Article 3(1) is intended to cover private local networks that are not connected to the Internet. Since the Commission does not provide any justification for imposing obligations covering isolated private networks, this would seem to imply that private networks are out of the scope of the Proposal. This should be clarified in Article 3(1).

[36] See also recital 5.
[37] See *ibid.*

48. The definition of 'incident' in Article 3(4) should be further clarified, also in relation to the definition of security in Article 3(2) and the definition of risk in Article 3(3). For example, it is not clear whether an attack on an information system should be considered an incident if the attacker does not succeed in compromising its security. In this view, account could be taken of the definition of a personal data breach in Article 2(i) of the ePrivacy Directive[38] and in Article 4(9) of the proposed Data Protection Regulation, where the breach must lead to a consequence (such as alteration, loss, etc).

3.2.2. On the obligations upon Member States concerning the prevention, the handling of and the response to risks and incidents

49. Articles 5(1) and (2) require Member States to adopt a national NIS strategy and a national NIS cooperation plan. Article 5(2) specifies the requirements for national NIS cooperation plans. In particular, it requires establishing a risk assessment plan to identify risks and to assess the impact of potential incidents. The EDPS believes that the obligation to establish a «risk assessment plan» is too narrow as such wording does not include the other activities required when managing the information security risks[39], such as, just to mention the most important ones, the risk prioritisation and treatment (transfer, avoidance mitigation etc.), including the criteria for the choice of possible countermeasures and the acceptance of the residual risks. Instead, to use a wording including all the needed actions, the EDPS recommends that such a requirement should consist of «setting up and maintaining a risk management framework» (which of course implies also a risk assessment phase).

50. Article 6(1) of the Proposal provides for the establishment of a national competent authority on the security of network and information systems (hereafter 'NIS competent authority'). The EDPS welcomes the explicit obligation in Article 6(5) and in Article 15(5) for the national NIS competent authority to, whenever appropriate, consult and cooperate with the national data protection authority. The EDPS believes that this cooperation is fundamental to ensure on the one hand that a high level of security is achieved, and on the other hand that privacy and data protection are appropriately considered in the actions deployed for purpose of protecting the security of networks and information systems. He further calls for the involvement, in practice and where relevant, of data protection authorities in the definition and implementation of national NIS strategies and cooperation plans.

51. Article 7 requires the setting up by each Member State of a Computer Emergency Response Team (CERT), which may be established within the competent authority. The EDPS advises to make clear in Annex I that data protection requirements are also part of the essential requirements that CERTs

[38] Article 2(i) of Directive 2002/58/EC, as amended by Directive 2009/136/EC, provides that a personal data breach "means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community".

[39] See e.g. standard ISO/IEC 27005:2008 on Information security risk management

must comply with. The EDPS further notes with satisfaction that, through the national competent authority that supervises them, CERTs may always seek specific cooperation from data protection authorities as regards the protection of personal data in the performance of their duties when needed, in accordance with Article 6(5) of the Proposal.

3.2.3. On proposed security requirements for market operators and public administrations

52. The EDPS welcomes that security and notification obligations are imposed upon market operators and public administrations in Article 14, which aim at promoting a culture of risk management and at ensuring that the most serious incidents are reported.
53. Article 14(2) requires market operators and public administrations to notify the NIS competent authority of incidents having a significant impact on the security of the core services they provide. However, the circumstances when a notification is required as well as the content and format of the notification are not defined in the Proposal itself, but will be defined through delegated acts and implementing acts. The EDPS underlines that by omitting to include substantive provisions on these aspects, the text of the Proposal lacks sufficient legal certainty for market operators and public administrations that fall within the scope of such notification. Furthermore, it should be clarified in the Proposal what types of personal data may be collected (such as the name of staff members in charge of security), and whether or not the notification and its supporting documents will include details of personal data affected by a specific security incident, and if so, to what extent. The EDPS recalls that personal data should only be transmitted where strictly necessary for the management of the incident. The EDPS recommends that these aspects of the notification are set forth in more detail in the text of the Proposal itself (see more detailed analysis in section 3.2.4.), and that appropriate safeguards are set forth to ensure the adequate protection of the data processed by NIS competent authorities (whether they are personal data, sensitive data, or confidential data).

54. The EDPS welcomes that Article 15(5) expressly provides for the close cooperation of NIS competent authorities with data protection authorities when addressing incidents resulting in personal data breaches. The EDPS recommends clarifying in Article 14 that incident notifications pursuant to Article 14(2) should apply without prejudice to personal data breach notification obligations pursuant to applicable data protection law (i.e. the ePrivacy Directive and the proposed General Data Protection Regulation). A similar provision is present in Article 15(2) of the proposed Regulation on electronic identification and trust services for electronic transactions in the internal market[40]. In addition, the EDPS advises that the main modalities of the notification to NIS competent authorities of security incidents involving a personal data breach are expressly set forth in a provision of the Proposal (see further comments in section 3.2.4.). It must be ensured that the procedure is

[40] COM (2012) 238 final, op.cit.

respectful of the competence of data protection authorities (or other national regulatory bodies set forth pursuant to the ePrivacy Directive) in such case.

55. The Proposal further establishes the disclosure to the public of information concerning the incident. Article 14(4) provides that " (*...) 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 (...)*". The EDPS considers that, in principle, such information should not contain any personal data of individuals involved in the incident. For the purpose of Article 14(4), in most cases the public interest would be effectively pursued by disclosing only anonymous or effectively anonymised information. However, if such information were to include personal data, the EDPS points out that the decision to disclose personal data should be based on a proper balancing of the different interests at stake. In this respect, the Court of Justice, in *Schecke*[41], underlined that the publication of personal data (such as the names and precise amounts received by the beneficiaries of EU funds) may create an interference with the rights to privacy and data protection of the individuals concerned, and can only be done where a test of necessity and proportionality has been fulfilled in view of the purpose pursued.

56. Finally, the EDPS notes that Article 14(8) excludes microenterprises from the obligations on security and incident notification set forth in Articles 14(1) and (2). The EDPS points out that some of the market operators listed in Annex II of the proposed Directive could be start-up enterprises rapidly increasing their operations as providers of information society services (e.g. new social networks) and already playing a major role in their market sector. The current definition of microenterprises[42] might not account for some of them. The EDPS advises the legislators to amend Article 14(8) so that the exclusion for microenterprises does not apply to those operators that play a crucial role in the provision of information society services, for instance in view of the nature of the information they process (e.g. biometric data or sensitive data).

3.2.4. *On the sharing of information about NIS incidents and threats with the NIS competent authority and within the cooperation network*

57. Pursuant to the notification obligation of Article 14, market operators and public administrations are required to share information about NIS incidents with the NIS competent authority. While the content of such notification, and the types of data to be communicated to the NIS competent authority, are not specified in the Proposal, it can be anticipated that the notification would contain information that is considered as confidential as well as personal data, including sensitive ones.

[41] Joined Cases C-92/09 and C-93/09, *Schecke*, paras 56-64.
[42] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, which defines a microenterprise as "*an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million*".

58. Personal data exchanged with NIS competent authorities may for example include names and contact details of the security personnel at the notifying organisations as well as IP addresses that are provided as part of the technical data relating to the incident. These IP addresses may relate to the individuals affected by the incident as well as to individuals who may be at some point suspected of being responsible for the incident. Although the notifying organisation and the NIS competent authority would not necessarily be able to directly link the IP address to an identified individual, these IP addresses would nonetheless constitute personal data insofar as they allow *indirect* identification of the individuals behind them (through the Internet Service Provider or otherwise). Besides, such identification could be requested at some stage of the investigation, whether by the NIS competent authority or by the law enforcement authorities to whom such data may be further transmitted pursuant to Articles 10(4) and 15(4). The EDPS underlines that the processing of personal data by NIS competent authorities can only be considered lawful provided that it relies on an appropriate legal basis pursuant to Article 7 of Directive 95/46/EC and it is not excessive in view of the purposes to be achieved (proportionality principle). This will be analysed further below.

59. The EDPS further notes that any information gathered by NIS competent authorities may be further shared with other recipients. Article 15(4) provides that NIS competent authorities must notify incidents of a suspected serious criminal nature to law enforcement authorities. Information gathered by NIS competent authorities may also be shared within a cooperation network, composed of the NIS competent authorities in the EU as well as the Commission. The aim of this cooperation network is to enable structured and coordinated information exchange as well as coordinated detection (through an 'early warnings' procedure under Article 10) and response (through a coordinated response procedure under Article 11) regarding NIS. Other relevant EU bodies including ENISA (Article 8(2)), the European Cybercrime Centre within Europol and data protection authorities (Article 8(3)(f)) may be required to assist the cooperation network and information may also be shared with them. It will be assessed further below whether there is a sufficient legal basis for the sharing of personal data with these further recipients and what are the safeguards that should be implemented to protect individuals' rights in the context of such exchanges.

The legal basis for the processing and sharing of personal data under the proposed Directive

60. Article 1(6) of the proposed Directive acknowledges that the notification of NIS incidents and the sharing of information within the cooperation network may require the processing of personal data. According to these provisions, the processing of personal data for these purposes is justified under Article 7 of Directive 95/46/EC as being "*necessary to meet the objectives of public interest pursued by this Directive (...)*". Recital 39 of the proposed Directive adds that the processing "*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 (...).*" As a result, Article 1(6) provides that such processing "*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."

61. Article 7 of Directive 95/46/EC lists six specific and exclusive legal grounds that may justify the processing of personal data. However, recital 39 and Article 1(6) of the Proposal do not specify which of these legal grounds would justify the processing of personal data by competent authorities for the purpose of handling NIS incidents and for the purpose of sharing information with other competent authorities. In the view of the EDPS, such processing may be justified under Article 7(e) of Directive 95/46/EC insofar as it is "*necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed*." He therefore recommends specifying in Article 1(6) of the Proposal that the processing would be justified under Article 7(e) of Directive 95/46/EC insofar as it is necessary to meet the objectives of public interest pursued by the proposed Directive.

62. The EDPS, however, insists that due respect of the principles of necessity and proportionality must be ensured, so that only the data strictly necessary for the purpose to be achieved are processed. This must be ensured not only by the public administrations and market operators that are experiencing the incident and processing data about it but also (i) at the point of collection of personal data by the NIS competent authorities (i.e. in the incident notification form), (ii) in the design of the structured exchange of information through the cooperation network, and (iii) for the further transmission of personal data to other recipients (in particular to national and EU competent authorities).

Ensuring the proportionality of the processing and sharing of personal data

63. At the point of collection, the notification form should specify the personal data to be collected structurally (for example the name of the person responsible for security within the organisation). It should also clarify if, and under what conditions, organisations should include details of the IP addresses obtained in the technical reports describing what happened on IT systems and networks at the time of the incident. Furthermore, it should provide an indication as to whether personal data have been compromised.

64. If personal data have been compromised, specific procedures should be put in place to guide the handling of these cases by the NIS competent authorities together with data protection authorities. In the EDPS' view, it must be ensured that the extent of the personal data processing undertaken by NIS competent authorities fits within their mandate and does not interfere with the tasks of data protection authorities. While data protection authorities are entitled, as part of their mandate, to have access to personal data where necessary[43] to help evaluate and remedy a personal data breach, the tasks of NIS competent authorities may not necessarily require knowing all details of the personal data that have been compromised. Considering that the processing

[43] As laid down in particular in Article 28(3) of Directive 95/46/EC setting forth the powers of DPAs and in Article 15(a)(3) of the ePrivacy Directive 2002/58/EC as amended by Directive 2009/136/EC.

of personal data by DPAs in the context of data breach investigations only takes place where necessary, *a fortiori* NIS competent authorities - whose mandate is not to investigate personal data breaches - should only be allowed to collect and process personal data in the framework of a security incident only where this is strictly necessary.

65. The EDPS recommends that all the above-mentioned aspects are clarified in the Proposal, in any case in main lines. Currently, Article 14(7) foresees that the Commission may adopt implementing acts defining the format and procedures applicable to the notification. However, specific requirements should be included in Article 14 to (i) specify the types of personal data that should be notified to NIS competent authorities (as mentioned in points 53 and 63 above), (ii) provide safeguards as to the processing of personal data by NIS competent authorities, so that it remains proportionate to the aim pursued, and (iii) provide some details of the procedures for the cooperation of NIS competent authorities with DPAs in cases where the incident involves personal data (e.g. how DPAs are informed; what information should be provided to them; how they should coordinate their response to the incident and possible sanctions).

66. As concerns the further exchange of personal data by NIS competent authorities with other recipients (within or outside the cooperation network), it must be ensured that (i) personal data are only disclosed to recipients whose processing is necessary for the performance of their tasks in accordance with an appropriate legal basis and that (ii) such information is limited to what is necessary for the performance of their tasks. In this respect, the disclosure by the NIS competent authority of some or all the personal data in its possession may not always be necessary for the cooperation with other competent authorities in view of their tasks and mandate. An appropriate assessment must be conducted on a case by case basis by the NIS competent authority before disclosing any personal data to an external recipient to identify whether and to what extent personal data should be communicated to that recipient. The EDPS recommends adding specific provisions in the Proposal underlining these principles.

67. Furthermore, specific attention should be paid to the respect of the principle of purpose limitation. If the entity originally providing data to the information sharing network cannot with sufficient certainty determine the purposes for which the information will be processed and be subject to onward transfers, it may be obliged to restrict the provision of personal data in incident related information very strictly in the first instance, and could release further details only in response to individual justified requests. This could reduce the usefulness of the network considerably.

Other requirements for the processing and exchange of information

68. The EDPS underlines that other data protection requirements, as set out in applicable law, must also be satisfied. Many of these requirements would need to be explicitly set out in the Proposal so as to provide for effective guarantees. For example, NIS competent authorities must ensure that personal data are

kept for no longer than is necessary to achieve the purposes for which they were collected. This will require defining an appropriate time limit for the retention of personal data for the purposes set forth in the proposed Directive, in particular as concerns the retention by NIS competent authorities and within the secure infrastructure of the cooperation network.

69. In addition, the information to data subjects provided for in Articles 10 and 11 of Directive 95/46/EC about the identity of the data controller, purpose of the processing, types of data processed, recipients of the data, and their data protection rights, would be better achieved if clear modalities on these aspects were defined in the text of the Proposal itself. Such details should be added in the Proposal, together with a notice reminding NIS competent authorities that they remain responsible for making such information about the processing of personal data easily accessible, for example by posting a privacy policy on their website.

70. Furthermore, the EDPS considers that it is of the utmost importance that the data processed by NIS competent authorities, and that are further shared with other recipients, are appropriately secured at all times of the processing. The EDPS welcomes that Article 9 provides for the setup of a secure information-sharing system to support the cooperation network in the exchange of sensitive and confidential information. However, the EDPS regrets that the Proposal does not contain any specific provision regarding the level of security to be complied with by NIS competent authorities as regards their processing of the data. The EDPS advises the legislators to include a specific provision in the Proposal dealing with the security of the information collected, processed, and exchanged by NIS competent authorities. A reference to the security requirements of Article 17 of Directive 95/46/EC should be specifically included as regards the protection of personal data by NIS competent authorities.

71. Pursuant to Article 9(2), criteria regarding the participation of Member States in the secure information-sharing system may be defined by the Commission through delegated acts. The EDPS underlines that criteria should be defined which ensure that a high level of security and resilience is guaranteed by all the participants in the information-sharing systems at all steps of the processing. The EDPS underlines that the Commission should also be bound by these criteria for its participation as a controller in the secure information-sharing system (in particular since pursuant to Article 8, the Commission will be actively participating in the network by receiving and exchanging information). Amongst these criteria, appropriate confidentiality and security measures should be implemented by Member States and by the Commission to protect personal data processed within the system, in accordance with Articles 16 and 17 of Directive 95/46/EC and Articles 21 and 22 of Regulation (EC) No 45/2001. The EDPS recommends that this is emphasised in Article 9 of the Proposal.

72. The EDPS notes that the proposed Directive does not explicitly establish the modalities for the setup, operation and management of the information-sharing system. It should, amongst others, be clarified whether the Commission will play a role in the establishment, operation and maintenance of the secure infrastructure. This will also have an impact on the Commission's responsibilities with respect to any personal data processing performed through that infrastructure, pursuant to Regulation (EC) No 45/2001. As a result, the EDPS recommends adding in Article 9 a description of the respective roles and responsibilities of the Commission and of the Member States in the setup, operation and maintenance of the secure information-sharing system. The EDPS recommends that the Proposal establishes minimal security requirements and data protection principles for data quality in respect of the operation of the information-sharing system. The EDPS further suggests that the Proposal should explicitly provide that the design of the system should be done in accordance with the principles of data protection by-design and by-default and of security-by-design[44].

73. Finally, the EDPS welcomes that Article 13 provides that any cooperation of members of the cooperation network with international partners should take place on the basis of international agreements, which should ensure adequate protection of the personal data circulating on the cooperation network. The EDPS recalls that any transfer of personal data to recipients located in countries outside the EU should be conducted in accordance with Articles 25 and 26 of Directive 95/46/EC and Article 9 of Regulation (EC) No 45/2001.

4. CONCLUSIONS

74. The EDPS welcomes that the Commission and the High Representative of the EU for Foreign Affairs and Security Policy have put forward a comprehensive Cyber Security Strategy complemented by a proposal for a Directive on measures to ensure a high common level of network and information security (NIS) across the EU. The Strategy complements the policy actions already developed by the EU in the area of Network and Information Security.

75. The EDPS welcomes that the Strategy goes beyond the traditional approach of opposing security to privacy by providing for the explicit recognition of privacy and data protection as core values which should guide cyber security policy in the EU and internationally. The EDPS notes that the Cyber Security Strategy and the proposed Directive on NIS can play a fundamental role in contributing to ensure the protection of individuals' rights to privacy and data protection in the online environment. At the same time, it must be ensured that they do not lead to measures that would constitute unlawful interferences with individuals' rights to privacy and data protection.

[44] See text of the Joint Communication at page 28 as to the recommendations to public and private stakeholders on the adoption of security-by-design and privacy-by-design principles.

76. The EDPS also welcomes that data protection is mentioned in several parts of the Strategy and is taken into account in the proposed Directive on NIS. However, he regrets that the Strategy and the proposed Directive do not underline better the contribution of existing and forthcoming data protection law to security and fail to fully ensure that any obligations resulting from the proposed Directive or other elements of the Strategy are complementary with data protection obligations and do not overlap or contradict each other.

77. Furthermore, the EDPS notes that due to the lack of consideration and taking full account of other parallel Commission initiatives and ongoing legislative procedures, such as the Data Protection Reform and the proposed Regulation on electronic identification and trust services, the Cyber Security Strategy fails to provide a really comprehensive and holistic view of cyber security in the EU and risks to perpetuate a fragmented and compartmentalised approach. The EDPS also notes that the proposed Directive on NIS does not yet permit a comprehensive approach of security in the EU either and that the obligation set forth in data protection law is probably the most comprehensive network and security obligation under EU law.

78. The EDPS also regrets that the important role of data protection authorities in the implementation and enforcement of security obligations and in enhancing cyber security is not properly considered either.

79. As to the Cyber Security Strategy, the EDPS underlines that:

- A clear definition of the terms 'cyber-resilience', 'cybercrime' and 'cyber-defence' is particularly important since these terms are used as a justification for certain special measures which could cause interference with fundamental rights, including the rights to privacy and data protection. However, the definitions of 'cybercrime' provided in the Strategy and in the Cybercrime Convention remain very broad. It would be advisable to have a clear and *restrictive* definition of 'cybercrime' rather than an overreaching one;

- Data protection law should apply to all actions of the Strategy whenever they concern measures that entail the processing of personal data. Although data protection law is not mentioned specifically in the sections relating to cybercrime and cyberdefence, the EDPS underlines that many of the actions planned in those areas would involve the processing of personal data and would therefore fall within the scope of applicable data protection law. He also notes that many actions consist in the setting up of coordination mechanisms, which will require the implementation of appropriate data protection safeguards as to the modalities for exchanging personal data;

- Data Protection Authorities (DPAs) play an important role in the context of Cyber Security. As guardians of the privacy and data protection rights of individuals, DPAs are actively engaged in the protection of their personal data, both offline and online. They should therefore be appropriately involved in their capacity of supervisory bodies with respect

to implementing measures that involve the processing of personal data (such as the launch of the EU pilot project on fighting botnets and malware). Other players in the field of cyber security should also cooperate with them in the performance of their tasks, for instance in the exchange of best practices and awareness raising actions. The EDPS and national DPAs should also be appropriately involved in the high-level conference that will be convened in 2014 to assess progress on the implementation of the Strategy.

80. As to the proposed Directive on NIS, the EDPS advises the legislators to:

- Provide more clarity and certainty in Article 3(8) on the definition of the market operators that fall within the scope of the Proposal, and to set up an exhaustive list that includes all relevant stakeholders, with a view to ensuring a fully harmonised and integrated approach to security within the EU;

- Clarify in Article 1(2)(c) that the proposed Directive applies to EU institutions and bodies, and to include a reference to Regulation (EC) No 45/2001 in Article 1(5) of the Proposal;

- Recognise a more horizontal role for this Proposal in respect of security, by explicitly providing in Article 1 that it should apply without prejudice to existing or future more detailed rules in specific areas (such as those to be set forth upon trust service providers in the proposed Regulation on electronic identification);

- Add a recital to explain the need to embed data protection by design and by default from the early stage of the design of the mechanisms established in the Proposal and through the whole lifecycle of processes, procedures, organisations, techniques and infrastructures involved, taking into account the proposed Data Protection Regulation;

- Clarify the definitions of 'network and information system' in Article 3(1) and of 'incident' in Article 3(4), and replace in Article 5(2) the obligation to establish a «risk assessment plan» by «setting up and maintaining a risk management framework»;

- Specify in Article 1(6) that the processing of personal data would be justified under Article 7(e) of Directive 95/46/EC insofar as it is necessary to meet the objectives of public interest pursued by the proposed Directive. However, due respect of the principles of necessity and proportionality must be ensured, so that only the data strictly necessary for the purpose to be achieved are processed;

- Lay down in Article 14 the circumstances when a notification is required as well as the content and format of the notification, including the types of personal data that should be notified and whether or not, and to which extent, the notification and its supporting documents will include details of personal data affected by a specific security incident (such as IP

addresses). Account must be taken of the fact that NIS competent authorities should be allowed to collect and process personal data in the framework of a security incident only where this is strictly necessary. Appropriate safeguards should also be set forth in the Proposal to ensure the adequate protection of the data processed by NIS competent authorities;

- Clarify in Article 14 that incident notifications pursuant to Article 14(2) should apply without prejudice to personal data breach notification obligations pursuant to applicable data protection law. The main aspects of the procedure for the cooperation of NIS competent authorities with DPAs in cases where the security incident involves a personal data breach should be set forth in the Proposal;

- Amend Article 14(8) so that the exclusion of microenterprises from the scope of the notification does not apply to those operators that play a crucial role in the provision of information society services, for instance in view of the nature of the information they process (e.g. biometric data or sensitive data);

- Add provisions in the Proposal governing the further exchange of personal data by NIS competent authorities with other recipients, to ensure that (i) personal data are only disclosed to recipients whose processing is necessary for the performance of their tasks in accordance with an appropriate legal basis and (ii) such information is limited to what is necessary for the performance of their tasks. Consideration should also be given as to how entities providing data to the information sharing network ensure compliance with the purpose limitation principle;

- Specify the time limit for the retention of personal data for the purposes set forth in the proposed Directive, in particular as concerns the retention by NIS competent authorities and within the secure infrastructure of the cooperation network;

- Remind NIS competent authorities of their duty to provide appropriate information to data subjects on the processing of personal data, for example by posting a privacy policy on their website;

- Add a provision regarding the level of security to be complied with by NIS competent authorities as regards the information collected, processed, and exchanged. A reference to the security requirements of Article 17 of Directive 95/46/EC should be specifically included as regards the protection of personal data by NIS competent authorities;

- Clarify in Article 9(2) that the criteria for the participation of Member States in the secure information-sharing system should ensure that a high level of security and resilience is guaranteed by all the participants in the information-sharing systems at all steps of the processing. These criteria should include 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. The Commission should be expressly bound by these criteria for its participation as a controller in the secure information-sharing system;

- Add in Article 9 a description of the roles and responsibilities of the Commission and of the Member States in the setup, operation and maintenance of the secure information-sharing system, and provide that the design of the system should be done in accordance with the principles of data protection by-design and by-default and of security-by-design; and

- Add in Article 13 that any transfer of personal data to recipients located in countries outside the EU should take place in accordance with Articles 25 and 26 of Directive 95/46/EC and Article 9 of Regulation (EC) No 45/2001.

Done in Brussels, 14 June 2013

(**signed**)

Peter HUSTINX
European Data Protection Supervisor