Executive summary of the 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 full text of this Opinion can be found in English, French and German on the EDPS website: http://www.edps.europa.eu)

(2014/C 32/10)

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' ([1]) (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 common level of network and information security across the Union ([2]) (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.

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.

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

([1]) JOIN(2013) 1 final.
([2]) COM(2013) 48 final.

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 cyber-defence, 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 at Brussels, 14 June 2013.

Peter HUSTINX

European Data Protection Supervisor