EDPS COMMENTS ON DG CONNECT'S PUBLIC CONSULTATION ON IMPROVING NETWORK AND INFORMATION SECURITY (NIS) IN THE EU

The Commission has launched an initiative aimed at better defining a Network and Information Security (NIS) strategy. It aims at stepping up the fight against cybercrime, as well as addressing the external dimension of cyber-security. The Commission considers the fight against cybercrime to be a cornerstone in building security and safety in the digital space and generating the required level of trust. The purpose of the strategy is also to minimise the risks of technical failures, especially on critical infrastructures.

I. Relevance of data protection in the context of Network and Information Security

The EDPS has in many occasions underlined that the security of data processing operations, in particular those carried out through the use of information and communication technologies, is a crucial element of data protection.[1] The correct application of the data protection principles set forth in Directive 95/46/EC and Directive 2002/58/EC (ePrivacy Directive), including security requirements, is a core condition for the success of the deployment of networks and information systems. When the security in the digital space is enhanced, the level of data protection in this area should be equally improved.

In this sense, the strategy adopted in order to improve NIS should take full account of data protection principles, in particular as breaches of security on the Internet may also compromise data of individuals. Some of these data might include sensitive personal data -for instance, health data-,[2] which require additional safeguards in terms of data protection (in accordance with Article 8 of Directive 95/46/EC). The ePrivacy Directive and the proposed Data Protection Regulation[3] both contain a personal data breach provision, obliging the concerned organisations to notify a breach of security which compromises personal data to the data protection authority as well as to the individuals affected where they are likely to be negatively affected. A data breach is

[1] For instance, EDPS Opinion on the Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA), 20.12.2010.

[2] See EDPS Opinion on the proposal for a directive of the European Parliament and of the Council on the application of patients’ rights in cross-border healthcare ,2.12.2008; and EDPS Opinion on the proposal for a Regulation of the European Parliament and of the Council amending, as regards pharmacovigilance of medicinal products for human use, Regulation (EC) No 726/2004 laying down Community procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency, and on the proposal for a Directive of the European Parliament and of the Council amending, as regards pharmacovigilance, Directive 2001/83/EC on the Community code relating to medicinal products for human use, 22.04.2009.

[3] COM(2012) 11 final, 25.01.2012.

broadly defined as any breach leading to the destruction, loss, disclosure etc of personal data transmitted, stored or otherwise processed in connection with the service. The EDPS thus notes that the compliance with data protection law should be regarded as an integral part of the objective of cyber-security.

The EPDS regrets that the public consultation does not mention data protection as an element to be considered. Therefore, the EDPS wishes to contribute to this public consultation by providing comments on the areas of the public consultation that have relevance to or an impact on the rights to data protection and to privacy.

II. General issues

A priority of the Internal Security Strategy[4] is to improve the capability of dealing with cyber attacks. A key element of the Strategy is to improve the level of NIS across the Union. NIS is defined by the Commission as the "*ability of a network or an information system to resist […] accidental events or malicious actions that compromise its availability, authenticity, integrity and confidentiality […]*"[5].

The EDPS regrets that, notwithstanding the existence of widely recognised technical standards, there is no EU provision clearly setting out the scope of what types of incidents or threats are being tackled in the context of NIS. The public consultation refers to 'cyber security' and to 'cyber threats' without, however, providing a clear definition of what these terms would entail.

The EDPS is of the view that a clear distinction should be made between accidental events, which are incidents that have occurred on a network or an information system, and malicious actions, which could have a connection with cybercrime. In this respect, the EDPS notes the absence of a legal definition for cybercrime in EU legislation. Although the Council of Europe assessed this concept in 2001,[6] not all EU Member States have ratified the Convention[7]. There is therefore a need to provide for a clear definition of the types of incidents or threats that any future policy action aims at addressing in the context of NIS. It should furthermore be clarified that the actions foreseen in the context of NIS do not include content-related cybercrime offences.

III. Specific comments

The EDPS would like to stress some aspects related to data protection that should be taken into account while examining the questions included in the public consultation at stake.

Information exchange between the public and private sector (question 15)

[4] COM(2010) 673 final, 22.11.2010.

[5] http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf.

[6] ETS 185, Convention on Cybercrime, 23.11.2001.

[7] In particular Czech Republic, Greece, Luxembourg and Sweden have not yet ratified the Cybercrime Convention.

The exchange of information between the public and the private sectors has been the object of analysis in different EDPS Opinions[8].

At EU level, the European Cybercrime Centre (EC3) and the European Network and Information Security Agency (ENISA) are in charge of collecting and analysing data on security incidents and emerging risks in Europe. However, ENISA and the EC3 have different roles depending on the nature of the security issue whether it is an incident or a threat. The EC3 is being established in order to share expertise by providing "operational support" to cybercrime investigations, as well as in developing training and awareness-raising for law enforcement and judiciary. On the other hand, ENISA aims at helping the European Commission, the Member States and the business community to address, respond and especially prevent Network and Information Security incidents.

The EDPS believes that these two organisations should have a central role in the information exchange concerning NIS, in view of their respective roles. However, as mentioned in previous opinions, the EDPS points out that the specific tasks of the EC3 should be clarified[9]. As a more general comment, the EDPS also underlined in previous opinions that both organisations should implement a solid data protection scheme in their procedures for dealing with these information exchanges, as they may often involve data collected for initial commercial purposes as well as international data transfers [10].

In many cases, depending on the type of infringement committed online, law enforcement bodies will be involved and exchanges of information may be sought from private parties. The EDPS recalls that the processing by law enforcement bodies of data initially collected by private companies for commercial purposes - for instance in the telecommunications, transport and financial sectors - must not be contrary to the purpose limitation principle. It is a cornerstone of data protection law that personal data shall be collected for specified purposes and not used in a way incompatible with those purposes[11].

Reporting cyber security incidents (question 17)

The EDPS recommends that the reporting about cyber security incidents is done in accordance with the current and future EU data protection legislation.

The EDPS considers that competent authorities in charge of NIS, including national/governmental Computer Emergency Response Teams (CERTs), should be in charge of dealing with reports of cyber security incidents.

Furthermore, as the reporting of cyber security incidents is closely linked to the data breach notification obligation, data protection authorities should also be involved where relevant. This is currently regulated by the ePrivacy Directive, which was

[8] 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, 29.06.2012, and EDPS Opinion on ENISA, *op.cit.*

[9] See EDPS Opinion on EC3, *op.cit*.

[10] EDPS Opinion on EC3, *op.cit.*, p.11; EDPS Opinion on ENISA, *op.cit.*, p. 7.

[11] EDPS Opinion on the Communication from the Commission to the European Parliament and the Council on an area of freedom, security and justice serving the citizen, 10.07.2009.

amended in 2009[12] with the inclusion of an obligation to notify personal data breaches. Moreover, Article 31 of the proposal for a Data Protection Regulation introduces a general obligation for the controller to notify personal data breaches to the supervisory authority, while it also obliges in some cases the data controller to communicate such personal data breach to the data subject.

The EDPS has supported the adoption of a personal data breach notification scheme pursuant to which competent authorities and individuals will be notified when their personal data have been compromised, since the existence of a security breach notification in the electronic communication sector has proved to be a factor that drives security investment at organisations that process personal data. In this regard, the EDPS encourages companies to improve data security and enhance their accountability regarding the personal data for which they are responsible[13].

Raising awareness about cyber-security (question 23)

The EDPS considers the purpose of raising awareness about cyber-security risks amongst businesses, consumers and governments of a great importance.

Data collected and processed by ENISA and EC3 in the context of NIS should improve their knowledge on cyber security incidents and threats. Within the frame of their respective roles, these organisations should play a role in raising awareness about NIS towards governments, businesses and the public at large.

The mandatory notification of data breaches to individuals will also help them become aware of the risks they face when their personal data are compromised and help them to take measures to mitigate such risks.

The EDPS supports awareness raising campaigns regarding online security, which should also include references to data protection risks and to prevention tools (such as data protection by default settings, appropriate security parameters, etc). The EDPS also wishes to draw the attention to the fact that awareness raising actions should also be developed in respect of children, who are a growing category of users of online services. In such case, information should be provided in a simple and clear manner to inform them about the seriousness of cyber security incidents and other Internet threats and possible consequences[14].

Implementing ways to ensure security (question 26)

Setting up technical and organisational measures to safeguard personal data on the Internet implies ensuring confidentiality, integrity (including non-repudiation) and availability of that data according to data protection law:

- Confidentiality of personal data will ensure that the information is disclosed on a need-to-know basis to the intended recipients according to the purpose of the

[12] OJ L337, 18.12.2007, p.11-36.

[13] Second Opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 09.01.2009.

[14] EDPS Opinion on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - "European Strategy for a Better Internet for Children", 17.07.2012.

processing operations and that any possible transfers will target only intended addressees.

- Personal data integrity will prevent unauthorised modifications thus contributing to data quality principles.
- Non-repudiation of personal data processing - i.e. the property of not being able to claim not to have performed an action (e.g. a processing operation or a digital transaction) - will, among others, enable accountability of controllers and processors.
- Availability of personal data will enable transparency, ease the free flow of that data while ensuring the access so that the data subject can be able to exercise their rights without hindrances.

Further to classical security requirements, other data protection specific safeguards need to be put in place in the cyberspace. Specific concepts have been developed in the last years which are also reflected in the proposal for a General Data Protection Regulation.

The independent supervisory authorities for the protection of individuals with respect to the processing of personal data, e.g. national DPAs, are responsible for monitoring the enforcement of the data controllers' obligations regarding personal data processing, including obligations regarding security of personal data. In this respect, they make an important contribution to raising NIS.

The EDPS has advocated on various occasions and in various opinions the concept of “built in” privacy or “Privacy by design”.[15] Privacy by design refers to the integration of data protection and privacy from the very inception of new products, services and procedures that entail the processing of personal data. Privacy by design also requires ensuring that data processing systems are designed to process as little personal data as possible. As regards the techniques which are better in line with the "privacy by design" concept, the EDPS has recommended in previous opinions that organisations who are data controllers, but also system developers, implement Privacy Enhancing Technologies (PETs) and Best Available Techniques (BATs)[16]:

- The use of PETs[17] can help design information and communication systems and services in a way that minimises the collection and use of personal data and facilitate compliance with data protection rules. Some examples of PETs could be the automatic anonymisation of data after a certain lapse of time, enhancing encryption tools or installing cookie-cutters.[18]

[15] See EDPS Opinion on ENISA, *op.cit,*, p. 5; EDPS Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 18.03.2010; 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", 17.12.2010.

[16] EDPS Opinion on ENISA, *op.cit.*, and 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" , 17.12.2010, p. 9.

[17] EDPS Opinion on the Commission Recommendation on preparations for the roll-out of smart metering systems, 08.06.2012; EDPS Opinion 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), 27.09.2012.

[18] COM(2007) 228 final, 02.05.2007, p. 3-4.

- As for the practical implementation of BATs in the field of security, it refers to the most effective and advanced stage in the development of processes, facilities and their methods of operation for minimising the impact on privacy and strengthening personal data protection.

Therefore, in line with the "privacy by design" concept, the EDPS considers that there should be a mandatory application of privacy-enhancing technologies and other 'best available techniques' in all network and information systems deployed on the Internet. This is also in line with the proposed Data Protection Regulation, which makes data protection by design and data protection by default mandatory.

Done at Brussels, on 10 October 2012