High common level of network and information security across the Union. NIS Directive

2013/0027(COD) - 14/06/2013 - Document attached to the procedure

Opinion of the European Data Protection Supervisor on (i) 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 (ii) on the Commission proposal for a directive concerning measures to ensure a high common level of network and information security across the Union.

The EDPS welcomes the comprehensive Cyber Security Strategy and 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.

However, 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 formulates the following recommendations:

The Cyber Security Strategy:

- 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; he also notes that many actions consist in the setting up of coordination mechanisms;

- as guardians of the privacy and data protection rights of individuals, data protection authorities (DPAs) should 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).

Proposed directive on network and information security (NIS):

- provide more clarity and certainty 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;

- explicitly provide that the directive 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;

- specify that the processing of personal data would be justified under insofar as it is necessary to meet the objectives of public interest pursued by the proposed directive;

- lay down the circumstances when a notification is required 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);

- ensure 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;

- specify the time limit for the retention of personal data;

- 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;

- clarify 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;

- add 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;

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