Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)

(2011/C 101/04)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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

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 the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 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],

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

Description of the Proposal

1. On 30 September 2010, the Commission adopted a proposal for a Regulation of the European Parliament and of the Council concerning ENISA, the European Network and Information Security Agency [3].

2. ENISA was established in March 2004 for an initial period of five years by Regulation (EC) No 460/2004 [4]. In 2008, Regulation (EC) No 1007/2008 [5] extended the mandate until March 2012.

3. As follows from Article 1(1) of Regulation (EC) No 460/2004, the Agency was established for the purpose of ensuring a high and effective level of network and information security within the Union and for contributing to the smooth functioning of the internal market.

4. The Commission proposal intends to modernise the Agency, to strengthen its competences, and to establish a new mandate for a five year period that will enable the continuity of the Agency beyond March 2012 [6].

5. The proposed Regulation finds its legal basis in Article 114 of the TFEU [7], which confers competence on the Union to adopt measures with the aim of establishing or ensuring the functioning of the internal market. Article 114 TFEU is the successor of Article 95 of the former EC Treaty on which the previous regulations on ENISA were based [8].

6. The Explanatory Memorandum which accompanies the proposal refers to the fact that preventing and combating crime has become a shared competence following the entry into force of the Lisbon Treaty. This has created an opportunity for ENISA to play a role as a platform on Network Information Security (NIS) aspects of the fight against cybercrime and to exchange views and best practices with cyber defence, law enforcement and data protection authorities.

7. Out of several options the Commission chose to propose an expansion of the tasks of ENISA and to add law enforcement and data protection authorities as fully fledged members of its permanent stakeholders' group. The new list of tasks does not include operational ones, but updates and reformulates the current tasks.

EDPS consultation

8. On 1 October 2010, the proposal was sent to the EDPS for consultation in accordance with Article 28(2) of Regulation (EC) No 45/2001. The EDPS welcomes that he was consulted on this matter and recommends that a reference to this consultation is made in the recitals of the proposal, as is usually done in legislative texts on which the EDPS has been consulted in accordance with Regulation (EC) No 45/2001.

9. Prior to the adoption of the proposal, the EDPS has been informally consulted and provided several informal comments. However, none of these remarks were taken into account in the final version of the proposal.

General assessment

10. The EDPS underlines that security of data processing is a crucial element of data protection [9]. In this respect, he welcomes the proposal's objective to strengthen the

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM(2010) 521 final.
[4] OJ L 77, 13.3.2004, p. 1.
[5] OJ L 293, 31.10.2008, p. 1.
[6] In order to prevent a legal vacuum, should the legislative procedure in the European Parliament and in the Council last beyond the expiry of the current mandate, the Commission, on 30 September 2010, adopted a second proposal for amendment of Regulation (EC) No 460/2004 which intends only to extend the deadline of the current mandate with 18 months. See COM(2010) 520 final.
[7] Cf. supra.
[8] On 2 May 2006, the Court of Justice dismissed an action for annulment of the previous Regulation (EC) No 460/2004 that challenged its legal basis (Case C-217/04).
[9] 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.

competences of the Agency so that it can fulfil more effectively its current tasks and responsibilities and at the same time, expand its field of activity. The EDPS furthermore welcomes the inclusion of data protection authorities and law enforcement bodies as fully fledged stakeholders. He considers the extension of ENISA's mandate a way to encourage at European level professional and streamlined management of security measures for information systems.

11. The overall assessment of the proposal is positive. However, on several points the proposed Regulation is unclear or incomplete which raises concerns from a data protection perspective. These issues will be explained and discussed in the next chapter of this opinion.

II. COMMENTS AND RECOMMENDATIONS

The expanded tasks that will be carried out by ENISA are not sufficiently clear

12. The expanded tasks of the Agency which relate to the involvement of law enforcement bodies and data protection authorities are formulated in a very general way in Article 3 of the proposal. The Explanatory Memorandum is more explicit in that respect. It refers to ENISA as interfacing with cybercrime law enforcement bodies and carrying out of non-operational tasks in the fight against cybercrime. However, these tasks have not been included or have only been mentioned in very general terms in Article 3.

13. In order to avoid any legal uncertainty, the proposed Regulation should be clear and unambiguous about the tasks of ENISA. As stated, security of data processing is a crucial element of data protection. ENISA will play an increasingly important role in that area. It should be clear to citizens, institutions and bodies what kind of activities ENISA could be engaged in. Such dimension is even more important should the expanded tasks of ENISA include the processing of personal data (see pts. 17-20 below).

14. Article 3(1)(k) of the proposal states that the Agency carries out any other task conferred on the Agency by another Union legislative act. The EDPS has concerns about this open ended clause since it creates a potential loophole that may affect the coherence of the legal instrument and could lead to 'function creep' of the Agency.

15. One of the tasks referred to in Article 3(1)(k) of the proposal is contained in Directive 2002/58/EC [1]. It provides that the Commission is required to consult the Agency on any technical implementing measures applicable to notifications in the context of data breaches. The EDPS recommends that this activity of the Agency is described in greater detail while delimiting it to the security area. Given the potential impact ENISA might have on the policy development in this area, this activity should have a clearer and more prominent position within the proposed Regulation.

16. The EDPS furthermore recommends the inclusion of a reference to Directive 1999/5/EC [2] in Recital 21 given the particular task of ENISA referred in Article 3(1)(c) of the current proposal to assist the Member States and the European institutions and bodies in their efforts to collect, analyse and disseminate network and information security data. This should fuel ENISA promotional exercises in favour of NIS (Network Information Security) best practices and techniques, as it will better illustrate possible constructive interactions between the Agency and the standardisation bodies.

It should be clarified whether personal data will be processed by the Agency

17. The proposal does not specify whether the tasks attributed to the Agency might include the processing of personal data. Therefore, the proposal does not contain a specific legal basis for the processing of personal data, in the meaning of Article 5 of Regulation (EC) No 45/2001.

18. However, some of the tasks attributed to the Agency might involve (at least to a certain extent) the processing of personal data. It is, for instance, not excluded that the analysis of security incidents and data breaches or the execution of non-operational functions in the fight against cybercrime might involve the collection and analysis of personal data.

19. Recital 9 of the proposal refers to the provisions contained in Directive 2002/21/EC [3] which establish that where appropriate, the Agency is notified by the national regulatory authorities in the event of security breaches. The EDPS recommends that the proposal is more detailed about which notifications are meant to be sent to ENISA and about how ENISA should respond to these. Equally, the proposal should address the personal data processing implications that might arise from the analysis of these notifications (if any).

[1] 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 (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

[2] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, OJ L 91, 7.4.1999, p. 10 and in particular its Article 3(3)c.

[3] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive, OJ L 108, 24.4.2002, p. 33).

20. The EDPS invites the legislator to clarify whether, and if so which ENISA activities listed in Article 3 will include the processing of personal data.

Internal security rules for ENISA should be specified

21. Although ENISA plays an important role in the discussion on network and information security in Europe, the proposal is almost silent on the establishment of security measures for the Agency itself (either or not related to the processing of personal data).

22. The EDPS is of the opinion that the Agency will be in an even better position to promote good practices in relation to security of data processing if such security measures are strongly applied internally by the agency itself. This will foster that the Agency is recognised not only as centre of expertise but also as a point of reference in the practical implementation of Best Available Techniques (BATs) in the field of security. Striving for excellence in security practices implementation should therefore be embedded within the Regulation governing the working procedures of the Agency. The EDPS therefore suggests adding a provision in this sense to the proposal, for instance by requiring that the Agency applies Best Available Techniques which means the most effective and advanced security procedures and their methods of operation.

23. This approach will allow the Agency to advise on the practical suitability of particular techniques for providing the required security safeguards. Furthermore, the implementation of these BATs should prioritise those ones that allow ensuring the security while at the same time minimising as much as possible the impact on privacy. Techniques which are better in line with the 'privacy by design' concept should be selected.

24. Even with a less ambitious approach, the EDPS recommends, at a minimum, that the Regulation contains the following requirements: (i) the creation of an internal security policy following a comprehensive risk assessment and taking into account international standards and best practices in Member States, (ii) the appointment of a security officer in charge of implementing the policy with the adequate resources and authority, (iii) the approval of this policy after a close examination of the residual risk and the controls proposed by the Management Board, and (iv) a periodic review of the policy with a clear statement of the periodicity timeframe chosen and the objectives of the review.

Cooperation channels with data protection authorities (including the EDPS) and the Article 29 Working Party should be better defined

25. As already stated, the EDPS welcomes the extension of the Agency's mandate and believes that data protection authorities can greatly benefit from the existence of the Agency (and the Agency from the expertise of these authorities). Given the natural and logical convergence between security and data protection, the Agency and data protection authorities are indeed called to collaborate closely.

26. Recitals 24 and 25 contain a reference to the proposed EU Directive on cybercrime and mention that the Agency should liaise with law enforcement bodies and also data protection authorities with respect to the information security aspects of the fight against cybercrime [1].

27. The proposal should also provide concrete channels and collaboration mechanisms that will (i) ensure the *consistency* of the activities of the Agency with those of the data protection authorities and (ii) enable *close cooperation* between the Agency and the data protection authorities.

28. With regards to *consistency*, recital 27 explicitly refers to the fact that Agency tasks should not enter into conflict with Member States' data protection authorities. The EDPS welcomes this reference, but notes that no reference is made to the EDPS and the Article 29 Working Party. The EDPS recommends the legislator to also include a similar non-interference provision in the proposal with regard to these two entities. This will create a clearer working environment for all the parties and should frame the collaboration channels and mechanisms that will enable the Agency to assist the different data protection authorities and the Article 29 Working Party.

29. Accordingly, with regard to *close cooperation*, the EDPS welcomes the inclusion of a representation of data protection authorities in the Permanent Stakeholders' group that will advise the Agency in the performance of its activities. He recommends that it is explicitly mentioned that such representation from national data protection authorities should be appointed by the Agency on the basis of a proposal from the Article 29 Working Party. Also, it would be appreciated if a reference were included that provides for the attendance of the EDPS, as such, to those meetings where issues, which are relevant for the cooperation with the EDPS, are meant to be discussed. Moreover, the EDPS recommends that the Agency (advised by the Permanent Stakeholders' group and with the approval of the Management Board) establishes ad hoc working groups for the different topics where data protection and security overlap to frame this close cooperation effort.

[1] Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, COM(2010) 517 final.

30. Finally, in order to avoid any possible misunderstanding, the EDPS recommends using 'data protection authorities' instead of 'privacy protection authorities' and clarify who those authorities are by including a reference to Article 28 of Directive 95/46/EC and the EDPS as provided in Chapter V of Regulation (EC) No 45/2001.

It is unclear which beneficiaries can request assistance from ENISA

31. The EDPS notes an inconsistency in the proposed Regulation with regard to who can request assistance from ENISA. From recitals 7, 15, 16, 18 and 36 of the proposal, it follows that ENISA has the capacity to assist Member States bodies and the Union as a whole. However, Article 2(1) only refers to the Commission and the Member States, whereas Article 14 restricts the capacity to make requests for assistance to: (i) the European Parliament, (ii) the Council, (iii) the Commission and (iv) any competent body appointed by a Member State leaving out some of the institutions, bodies, agencies and offices of the Union.

32. Article 3 of the proposal is more specific and envisages different types of assistance depending on the type of beneficiaries: (i) collection and analysis information security data (in the case of Member States and the European institutions and bodies), (ii) analysis of the state of network and information security in Europe (in the case of Member States and the European institutions), (iii) promotion of the use of risk management and security good practices (across the Union and the Member States), (iv) develop network and information security detection (in the European institutions and bodies) and (v) collaboration in the dialogue and cooperation with third countries (in the case of the Union).

33. The EDPS invites the legislator to remedy this inconsistency and align the aforementioned provisions. In this respect, the EDPS recommends that Article 14 is amended in a way that it indeed includes all institutions, bodies, offices and agencies of the Union and that it is clear as to the type of assistance that can be required by the different entities within the Union (in case this differentiation is envisaged by the legislator). In the same direction, it is recommended that certain public and private entities could request assistance from the Agency if the support demanded shows a clear potential from an European perspective, and it is aligned with the objectives of the Agency.

Management Board functions

34. The Explanatory Memorandum provides for enhanced competences of the Management Board as regards its supervisory role. The EDPS welcomes this increased role and recommends that several aspects concerning data protection are included among the functions of the Management Board. Additionally, the EDPS recommends that the Regulation specifies unambiguously who is entitled to: (i) establish measures for the application of Regulation (EC) No 45/2001 by the Agency, including those concerning the appointment of a Data Protection Officer, (ii) approve the security policy and the subsequent periodic revisions, and (iii) set the cooperation protocol with data protection authorities and law enforcement bodies.

Applicability of Regulation (EC) No 45/2001

35. Although this is already required by Regulation (EC) No 45/2001, the EDPS suggests to include in Article 27 the appointment of the Data Protection Officer since this is of particular importance and should be accompanied by the prompt establishment of the implementing rules regarding the scope of powers and tasks to be entrusted to the Data Protection Officer in accordance with Article 24(8) of Regulation (EC) No 45/2001. More concretely, Article 27 could read as follows:

1. The information processed by the Agency in accordance with this Regulation shall be subject 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. The Management Board shall establish measures for the application of Regulation (EC) No 45/2001 by the Agency, including those concerning the Data Protection Officer of the Agency.

36. In case a specific legal basis for the processing of personal data is required, as discussed in pts. 17-20 above, it should also provide for specification as to the necessary and appropriate safeguards, limitations and conditions under which such a processing would take place.

III. **CONCLUSIONS**

37. The overall assessment of the proposal is positive and the EDPS welcomes the extension of the Agency's mandate and the expansion of its tasks by the inclusion of data protection authorities and law enforcement bodies as fully fledged stakeholders. The EDPS considers that the continuity of the Agency will encourage at European level professional and streamlined management of security measures for information systems.

38. The EDPS recommends that in order to avoid any legal uncertainty, the proposal should be clarified with regard to the expansion of the Agency's tasks and in particular those that relate to the involvement of law enforcement bodies and data protection authorities. Also, the EDPS draws the attention to the potential loophole created by the inclusion of a provision in the proposal that allows the addition of new tasks to the Agency by any other Union legislative Act without any additional restriction.

39. The EDPS invites the legislator to clarify whether, and if so which of ENISA's activities will include the processing of personal data.

40. The EDPS recommends including provisions on the establishment of a security policy for the Agency itself, in order to reinforce the role of the Agency as enabler of excellence in security practices, and as promoter of privacy by design by integrating the use of best available techniques in security with the respect to personal data protection rights.

41. The cooperation channels with data protection authorities, including the EDPS and the Article 29 Working Party, should be better defined with the aim of ensuring consistency and close cooperation.

42. The EDPS invites the legislator to solve some inconsistencies with regard to the restrictions expressed on Article 14 concerning the capacity to request the assistance of the Agency. In particular, the EDPS recommends that these restrictions are waived and all institutions, bodies, agencies and offices of the Union are empowered to request assistance from the Agency.

43. Finally, the EDPS recommends that the extended capacities of the Management Board include some concrete aspects that could enhance the assurance that good practices are followed within the Agency with regard to security and data protection. Among others, it is proposed to include the appointment of a data protection officer and the approval of the measures aimed at the correct application of Regulation (EC) No 45/2001.

Done at Brussels, 20 December 2010.

Giovanni BUTTARELLI

Assistant European Data Protection Supervisor