Opinion of the European Data Protection Supervisor

- 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"

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 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], in particular its Article 41.

HAS ADOPTED THE FOLLOWING OPINION

I. Introduction

1. On 22 November 2010, the Commission adopted a Communication entitled "EU Internal Security Strategy in Action: Five steps towards a more secure Europe" (hereinafter the "Communication")[3]. The Communication was sent to the EDPS for consultation.

1 OJ 1995, L 281/31.
2 OJ 2001, L 8/1.
3 COM(2010) 673 final

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

2. The EDPS welcomes the fact that he was consulted by the Commission. Already before the adoption of the Communication, the EDPS provided informal comments on the draft text, some of which have been taken into account in the final version of the Communication.

Context of the Communication

3. The EU Internal Security Strategy (hereinafter the ISS), addressed in the Communication, was adopted on 23 February 2010 under the Spanish Presidency[4]. The strategy lays out a European security model, which integrates among others action on law enforcement and judicial cooperation, border management and civil protection, with due respect for shared European values, such as fundamental rights. Its main objectives are to:
   – present to the public the existing EU instruments that already help to guarantee the security and freedom of EU citizens and the added value that EU action provides in this area;
   – further develop common tools and policies using a more integrated approach which addresses the causes of insecurity and not just the effects;
   – strengthen law enforcement and judicial cooperation, border management, civil protection and disaster management.

4. The ISS aims to target the most urgent threats and challenges to EU security such as serious and organised crime, terrorism and cybercrime, the management of EU external borders and building resilience to natural and man-made disasters. The strategy provides for general guidelines, principles and directions on how the EU should react to these issues and it calls upon the Commission to propose timed actions to implement the strategy.

5. Furthermore, it is important to refer in this context to the recent Justice and Home Affairs Council Conclusions on the creation and implementation of an EU policy cycle for organised and serious international crime adopted on 8-9 November 2010[5] (hereinafter "November 2010 Conclusions"). This document follows the Council's Conclusion on the Architecture of Internal Security of 2006[6], and calls upon the Council and the Commission to define a comprehensive ISS based on the EU common values and principles as reaffirmed in the EU Charter on Fundamental Rights. [7]

6. Amongst the directions and goals that should drive the implementation of the ISS, the November 2010 Conclusions refer to the reflection on a

[4] Doc. 5842/2/10
[5] 3043rd Justice and Home Affairs Council meeting, 8-10 November 2010, Brussels
[6] Doc. 7039/2/06 JAI 86 CATS 34
[7] The EU policy cycle for serious international and organised crime addressed in the November 2010 Conclusions consists of four steps: 1) policy developments on the basis of a European Union Serious and Organised Crime Threat Assessment (EU SOCTA), 2) policy setting and decision-making through the identification by the Council of a limited number of priorities, 3) implementation and monitoring of annual Operational Action Plan (OAP) and 4) at the end of the policy cycle a thorough evaluation which will also serve as an input o the future policy cycle.

proactive and intelligence-led approach, stringent cooperation between the EU agencies, including further improving their information exchange and the aim of making citizens aware of the importance of the Union's work to protect them. Moreover, the Conclusions call the Commission to develop together with the experts of relevant agencies and Member States a Multi-Annual Strategic Plan (hereinafter MASP) for each priority, defining the most appropriate strategy to tackle the problem. It also calls on the Commission to develop through consultation with the Member States' and EU Agencies' experts an independent mechanism to evaluate the implementation of the MASP. The EDPS will come to these issues later on in this Opinion as they are closely linked or have significant impact on the protection of personal data, privacy and other related fundamental rights and freedoms.

Content and objective of the Communication

7. The Communication proposes five strategic objectives, all having links with privacy and data protection:

   - disrupting international crime networks,
   - preventing terrorism and addressing radicalisation and recruitment,
   - raising levels of security for citizens and businesses in cyberspace,
   - strengthening security through border management, and
   - increasing Europe's resilience to crisis and disasters.

8. The *ISS in Action* as proposed in the Communication, puts forward a shared agenda for Member States, the European Parliament, the Commission, the Council, agencies and others, including civil society and local authorities, and proposes how they all should work together over the next four years to achieve the goals of the ISS.

9. The Communication builds on the Lisbon Treaty and acknowledges the guidance provided by the Stockholm Programme (and its Action Plan) which highlight in Chapter 4.1 the need for a comprehensive ISS based on respect for fundamental rights, international protection and the rule of law. Moreover, in accordance with the Stockholm Programme, developing, monitoring and implementing the internal security strategy should become one of the priority tasks of the Internal Security Committee (COSI) set up under Article 71 TFEU. In order to ensure the effective enforcement of the ISS, it should also cover security aspects of an integrated border management and, where appropriate, judicial cooperation in criminal matters relevant to operational cooperation in the field of internal security. It is also important to mention in this context that the Stockholm Programme calls for an integrated approach to ISS which should also take into account the external security strategy developed by the EU as well as other EU policies, in particular those concerning the internal market.

Aim of the Opinion

10. The Communication refers to various policy areas which form part of or have impact on a broadly understood concept of *"internal security"* in the European Union.

11. The aim of this Opinion is not to analyze all policy areas and specific topics covered by the Communication, but to:

    - look at the very objectives of the ISS proposed in the Communication from a specific perspective of privacy and data protection, and - from that angle - stress the necessary links with other strategies currently discussed and adopted at the EU level;

    - specify a number of data protection notions and concepts which should be taken into consideration when designing, developing and implementing the ISS at EU level;

    - provide, where useful and appropriate, suggestions on how data protection concerns could best be taken into account when implementing the actions proposed in the Communication.

12. The EDPS will do so by highlighting in particular the links between the ISS and the Information Management Strategy and the work on the comprehensive data protection framework. Moreover, the EDPS will refer to such concepts as: Best Available Techniques and "Privacy by design", privacy and data protection impact assessment, and data subject's rights, which have direct impact on the design and implementation of the ISS. The Opinion will also comment on a number of chosen policy areas such integrated border management, including EUROSUR and the processing of personal data by FRONTEX, as well as other fields such as cyberspace and TFTP.

II. General comments

The need for a more comprehensive, inclusive and 'strategic' approach to EU strategies related to the ISS

13. Various EU strategies based on the Lisbon Treaty and the Stockholm programme and having a direct or indirect impact on data protection, are being currently discussed and proposed at EU level. The ISS is one of them and it is closely linked with other strategies (either addressed in recent Commission's Communications or envisaged for the near future) such as the EU Information Management Strategy and the European Information Exchange Model, the strategy on the implementation of the EU Charter of Fundamental Rights, the comprehensive data protection strategy and the EU Counter-terrorism policy. In this Opinion, the EDPS pays particular attention to the links with the Information Management Strategy and the comprehensive data protection framework based on Article 16 TFEU, which have most evident policy links with the ISS from a data protection perspective.

14. All these strategies constitute a complex "patchwork" of interrelated policy guidelines, programmes and action plans which call for a comprehensive and integrated approach at EU level.

15. In more general terms, this approach of "*linking the strategies*" if taken on board in the future actions would show that there is a vision at EU level when it comes to *EU strategies* and, that these strategies, and the recently adopted Communications which elaborate on them, are closely interlinked, which is the case, the Stockholm Programme being the common reference point for all of them. It would also result in positive synergies between different policies falling within the area of freedom, security and justice and would avoid any possible duplication of work and efforts in this area. Equally important, this approach would also lead to more effective and coherent application of data protection rules in the context of all interlinked strategies.

16. The EDPS highlights that one of the pillars of the ISS is an efficient information management in the European Union which should be grounded on the principles of necessity and proportionality in order to justify the need for exchange of information.

17. Moreover, as mentioned in the EDPS opinion on the Communication on Information Management[8], the EDPS underlines that all new legislative measures which would facilitate the storage and exchange of personal data should only be proposed if they are based on concrete evidence of their need[9]. This legal requirement should be transformed into a pro-active policy approach when implementing the ISS. The need of a comprehensive approach to the ISS inevitably also leads to the need for assessment of all instruments and tools existing already in the field of internal security before proposing new ones.

18. In this context, the EDPS also suggests more frequent use of clauses providing for periodical evaluation of existing instruments, such as

[8] Opinion of 30 September 2010 on the Communication from the Commission to the European Parliament and the Council - "Overview of information management in the area of freedom, security and justice.

[9] This is a legal requirement; see in particular ECJ Judgment in Joined Cases c-92/09 and C-93/09 of 2 November 2010. In more specific contexts, the EDPS has also advocated this approach in other opinions on legislative proposals related to the area of freedom, security and justice: e.g. Opinion of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information System (SIS II); Opinion of 20 December 2007 on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes; Opinion of 18 February 2009 on the Proposal for a Regulation concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...][establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third- country national or a stateless person]; Opinion of 18 February 2009 on the Proposal for a Regulation establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person; and Opinion of 7 October 2009 on the proposals regarding law enforcement access to EURODAC.

included in the Data Retention Directive which is currently being evaluated.[10]

Data protection as an objective of ISS

19. The Communication refers to the protection of personal data in the paragraph "*Security policies based on common values*" where it mentions that the tools and actions to be used to implement the ISS must be based on common values including the rule of law and respect of fundamental rights as laid down in the EU Charter of Fundamental Rights. In this context, it stipulates that "*Where efficient law enforcement in the EU is facilitated through information exchange, we must also protect the privacy of individuals and their fundamental right to protection of personal data*."

20. That is a welcome statement. However as such it cannot be considered as sufficiently addressing the issue of data protection in the ISS. The Communication neither elaborates on data protection[11] nor explains how respect for privacy and protection of personal data will be ensured in practice in the actions implementing the ISS.

21. According to the EDPS *ISS in Action* should have as one of its objectives a broadly understood *protection* which would ensure the *right* balance between on the one hand the protection of citizens against the existing threats and, on the other hand, the protection of their privacy and the right to the protection of personal data. In other words, security and privacy concerns must be equally taken serious in the development of the ISS which would be in line with the Stockholm Programme and the Council Conclusions.

22. In short, <u>providing security while fully respecting privacy and data protection</u> should be mentioned as a very objective of the EU Internal Security Strategy. This should be reflected in all actions taken by Member States and EU institutions to implement the strategy.

23. In this context the EDPS refers to the Communication (2010) 609 on a comprehensive approach on personal data protection in the European Union.[12] The EDPS will soon issue an opinion on this Communication, but emphasises here that efficient ISS can not be put in place without the support of a solid data protection scheme complementing it and providing for mutual trust and better effectiveness.

[10] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105/54.

[11] Data protection in only mentioned more specifically in the context of the issue of the processing of personal data by FRONTEX.

[12] Communication from the Commission to the European Parliament, the Council and the European and Social Committee and the Committee of Regions on a comprehensive approach on data protection in the European Union, COM (2010) 693

III. Notions and concepts applicable to the design and implementation of ISS

24. It is clear that some of the actions that derive from the ISS objectives may increase the risks for individuals' privacy and data protection. To counterbalance these risks, the EDPS would like to specifically draw attention to such concepts as "Privacy by design", privacy and data protection impact assessment, data subject rights and best available techniques (BATs). All of them should be taken into account in the implementation of the ISS and can usefully contribute to more privacy friendly and data protection oriented policies in this field.

Privacy by design

25. The EDPS has advocated on various occasions and in various opinions the concept of "built in" privacy ("*Privacy by design*" or "*Privacy by default*"). This concept is currently developed both for the private and public sector, and therefore must also play an important role in the context of EU internal security and the area of police and justice.[13]

26. The Communication does not mention this concept. The EDPS suggests that this concept is referred to in the targeted actions to be proposed and undertaken to implement the ISS, in particular in the context of Objective 4 "Strengthen security through border management" where there is clear mention of an enhanced use of new technologies for border checks and border surveillance.

Privacy and data protection impact assessment

27. The EDPS encourages the Commission to reflect - as part of the future work on the design and implementation of the ISS based on the Communication - on what should be meant by a real *'privacy and data protection impact assessment*' (PIA) in the area of freedom, security and justice, and in particular in the ISS.

28. The Communication refers to threat and risk assessments. This is welcomed. However it does not - in any point - refer to privacy and data protection impact assessments. The EDPS believes that the work on the implementation of the Communication on ISS provides a good opportunity to elaborate such privacy and data protection impact assessments in the context of internal security. The EDPS notes that neither the Communication nor the Commission's Impact Assessment Guidelines[14] specifies this aspect and develops it into a policy requirement.

[13] The EDPS in his opinion on the Commission's Communication on the Stockholm Programme recommended that there should be a legal obligation for builders and users of information systems to develop and use systems which are in accordance with the principle of "Privacy by design".
[14] SEC(2009)92, 15.1.2009

29. Therefore, the EDPS recommends that in the implementation of future instruments a more specific and rigorous impact assessment on privacy and data protection is conducted, either as a separate assessment or as part of the general fundamental rights' impact assessment carried out by the Commission. This impact assessment should not only state general principles or analyze policy options, as it is the case currently, but should also recommend specific and concrete safeguards.

30. Consequently, specific indicators and features should be developed to ensure that each proposal having impact on privacy and data protection in the field of EU Internal Security is subject to thorough consideration, including such aspects as proportionality, necessity and purpose limitation principle.

31. Additionally, it could be helpful in this context to refer to Article 4 of the RFID Recommendation[15] in which the Commission called upon the Member States to ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments. Furthermore, the Madrid Resolution, adopted in November 2009 by the International Conference of Privacy and Data Protection Commissioners, encouraged the implementation of PIAs prior to the implementation of new information systems and technologies for the processing of personal data or substantial modifications in existing processing.

Data subjects' rights

32. The EDPS notes that the Communication does not address specifically the issue of the data subjects' rights which constitute a vital element of data protection and should have impact on the design of ISS. It is essential to ensure that across all different systems and instruments dealing with EU internal security, the persons subject to them enjoy similar rights relating to how their personal data are processed.

33. Many of the systems referred to in the Communication establish specific rules on data subjects' rights (targeting also such categories of persons as victims, suspected criminals or migrants), but there is a lot of variation between the systems and instruments, without good justification.

34. Therefore, the EDPS invites the Commission to look more carefully into the issue of the alignment of data subjects' rights in the EU in the context of the ISS and Information Management Strategy in the near future.

35. Particular attention should be paid to redress mechanisms. The ISS should guarantee that whenever individuals' rights have not been fully respected, data controllers should provide for complaints procedures which are easily accessible, effective and affordable.

[15] C(2009) 3200 final, 12.05.2009

Best Available Techniques

36. The implementation of the ISS will inevitability build upon the use of an IT infrastructure that will support the actions envisaged in the Communication. Best Available Techniques (BATs) can be seen as enablers of the correct balance between the achievement of the objectives of the ISS and respect of the rights of individuals. In the present context, the EDPS would like to reiterate the recommendation made in previous opinions[16] regarding the need for the Commission to define and promote together with industry stakeholders concrete measures for the application of BATs. Such application means the most effective and advanced stage in the development of activities and their methods of operation, which indicate the practical suitability of particular techniques for providing the results envisioned in an efficient way and in compliance with the privacy and data protection EU framework. This approach is fully in line the "privacy by design" approach, mentioned before.

37. Where relevant and feasible, reference documents on BATs should be elaborated to provide guidance and greater legal certainty for the actual implementation of the measures framed by the ISS. This could also promote the harmonisation of such measures throughout the different Member States. Last but not least, the definition of privacy and security friendly BATs will facilitate the supervisory role of Data Protection Authorities by providing them with privacy and data protection compliant technical references adopted by data controllers.

38. The EDPS also notes the importance of a correct alignment of the ISS with the activities already carried out under the seventh Framework Programme for Research and Technological Development and the Security and Safeguarding Liberties Framework Program. A joint vision pursuing to provide BATs will enable the innovation in the knowledge and capabilities required to protect citizens while respecting fundamental rights.

39. Finally, the EDPS points to the role which European Network and Information Security Agency (ENISA) can play in the elaboration of guidelines and the assessment of the security capabilities required to ensure the integrity and availability of the IT systems, and also in the promotion of these BATs. With regard to this, the EDPS welcomes the inclusion of the Agency as key player in the improvement of capabilities for dealing with cyber attacks and fighting against cybercrime.[17]

Clarification of actors and their roles

40. In this context, more clarification is also needed when it comes to the actors which form part of or contribute to the ISS architecture. The

[16] EDPS Opinion on Intelligent Transport systems, of July 2009 and EDPS Opinion on the RFID Communication of December 2007, see also EDPS Annual Report 2006 p.48-49.

[17] The EDPS envisages adopting an opinion on the legal framework of ENISA, still in December 2010.

Communication refers to various actors and stakeholders such as citizens, judiciary, EU agencies, national authorities, police, and business. The specific roles and competences of these actors should be better addressed in the specific actions to be proposed in the implementation of the ISS.

IV. Specific comments on policy fields related to ISS

Integrated border management (IBM)

41. The Communication refers to the fact that with the Lisbon Treaty, the EU is better placed to exploit synergies between border management policies on persons and goods. In relation to movement of persons, it mentions that "*the EU can treat migration management and the fight against crime as twin objectives of the integrated border management strategy*". The document perceives border management as a potentially powerful means of disrupting serious and organised crime.[18]

42. The EDPS also notes that the Communication identifies three strategic strands: 1) an enhanced use of new technology for border checks (the SIS II, VIS, entry/exit system and registered traveller programme); 2) an enhanced use of new technology for border surveillance (European Border Surveillance System, EUROSUR) and 3) an enhanced coordination of Member States through FRONTEX.

43. The EDPS wishes to use the opportunity of this Opinion to recall his requests made in a number of previous opinions that a clear policy on border management - fully respecting data protection rules - is established at EU level. The EDPS believes that the current work on the ISS and Information Management are very good occasions to take more concrete steps towards a coherent policy approach to these areas.

44. The EDPS notes that the Communication does not only refer to the existing large scale-systems and those that might be put in operation in the near future (such as SIS, SIS II and VIS), but - in the same lines - also to the systems that might be proposed by the Commission in the future but the decision on which has not been taken yet (i.e. Registered Travellers Programme (RTP) and Entry/exit system). It should be recalled in this context that the objectives and legitimacy of the introduction of these systems still need to be clarified and demonstrated, also in light of the results of specific impact assessments carried out by the Commission. If this does not happen, the Communication can be read as anticipating the decision making process, and consequently not taking into account the fact that the final decision on whether the RTP and the entry/exit system should be introduced in the European Union has not yet been taken.

45. The EDPS therefore suggests that in the future work on the implementation of the ISS, such anticipations are avoided. As mentioned earlier, any decision on the introduction of new privacy intrusive large-

[18] Press release on the EU Internal Security Strategy in Action – five steps towards a more secure Europe Memo 10/598

scale systems should only take place after an adequate evaluation of all existing systems has taken place, with due regard to necessity and proportionality.

EUROSUR

46. The Communication mentions that the Commission will present a legislative proposal to set up EUROSUR in 2011 to contribute to internal security and the fight against crime. It is also mentioned that EUROSUR will make use of new technologies developed through EU funded research projects and activities, such as satellite imagery to detect and track targets at the maritime border, e.g. tracing fast vessels transporting drugs to the EU.

47. In this context, the EDPS notes that it is not clear whether and if so to which extent the legislative proposal on EUROSUR to be presented by the Commission in 2011 will also envisage the processing of personal data in the context of EUROSUR. The Commission has not taken a clear position on this in the Communication. This issue is even more relevant given that the Communication makes clear links between EUROSUR and FRONTEX at tactical, operational and strategic level (see comments below on FRONTEX) and asks for close cooperation between the two.

The processing of personal data by FRONTEX

48. The EDPS has issued an opinion on the revision of the FRONTEX Regulation on 17 May 2010[19] in which he called for real debate and in-depth reflection on the issue of data protection in the context of strengthening the existing tasks of FRONTEX and granting it new responsibilities.

49. The Communication refers to the need to enhance the contribution of FRONTEX at the external borders under Objective 4 *Strengthen security through border management.* In this context, the Communication mentions that based on experience and in the context of the EU overall approach to information management, the Commission considers that enabling FRONTEX to process and use this information, with a limited scope and in accordance with clearly defined personal data management rules, will make a significant contribution to dismantling criminal organisations. This is a new approach compared to the Commission proposal on the revision of the FRONTEX Regulation, currently subject to discussion in the European Parliament and the Council, which was silent about processing of personal data.

[19] EDPS Opinion of 17 May 2010 on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX).

50. Against this background, the EDPS welcomes the fact that the Communication provides for some indication as to the circumstances when such processing might prove necessary (e.g. risk analysis, better performance of joint operations or exchange of information with Europol). More specifically, the Communication explains that currently the information on criminals involved in trafficking networks - which FRONTEX comes across - cannot be further used for risk analysis or better targeting future joint operations. Moreover, relevant data on suspected criminals do not reach the competent national authorities or Europol for further investigations.

51. Nevertheless, the EDPS notes that the Communication does not refer to the ongoing discussion on the revision of the FRONTEX legal framework which, as mentioned earlier, tackles this issue in order to provide for legislative solutions. Moreover, the wording of the Communication emphasising the role of FRONTEX in the context of the objective to dismantle criminal organisations, can be read as broadening the mandate of FRONTEX. The EDPS suggests that this point is taken into account both in the revision of the FRONTEX Regulation and in the implementation of ISS.

52. The EDPS also draws attention to the need to ensure that there is no duplication of tasks between Europol and FRONTEX. In that context, the EDPS welcomes that the Communication mentions that duplication of tasks between FRONTEX and Europol should be avoided. However, this issue should also be more clearly addressed both in the revised FRONTEX Regulation and in the actions implementing the ISS which provide for close cooperation between FRONTEX and EUROPOL. This is of particular importance from the point of view of the principles of purpose limitation and data quality. This remark also applies to the future cooperation with such agencies as the European network and Information Security Agency (ENISA) or the European Asylum Support Office.

The use of biometrics

53. The Communication does not address specifically the current phenomenon of the increased use of biometric data in the area of freedom, security and justice, including the EU large-scale IT systems and other border management tools.

54. The EDPS therefore takes this opportunity to recall his suggestion[20] that this matter of high sensitivity from the perspective of data protection is taken seriously into account in the implementation of the ISS, in particular in the context of border management.

55. The EDPS also recommends that a clear and strict policy on the use of biometrics in the area of freedom, security and justice based on a serious evaluation and a case-by-case assessment of the need for the use of biometrics in the context of the ISS, with full respect for such

[20] See in particular EDPS Opinion on the Communication on the overview of information management in the AFSJ mentioned in footnote 8.

fundamental data protection principles as proportionality, necessity and purpose limitation, is developed.

TFTP

56. The Communication announces that the Commission will develop in 2011 a policy for the EU to extract and analyse financial messaging data held on its own territory. In this context, the EDPS refers to his Opinion of 22 June 2010 on processing and transfer of Financial Messaging Data from the EU to the US for purposes of the Terrorist Finance Tracking Programe (TFTP II)[21]. All critical remarks expressed in that Opinion are equally valid and applicable in the context of the envisaged work on a EU framework on financial messaging data. Therefore, they should be taken into account in the discussions on this issue. Particular attention should be paid to the proportionality of extracting and processing large amounts of data on people who are not suspects, and to the issue of effective oversight by independent authorities and by the judiciary.

Security for citizens and business in cyberspace

57. The EDPS welcomes the importance attached in the Communication to preventive actions at EU level and is of the view that the strengthening of security in IT networks is an essential factor contributing to a well-functioning information society. Also, the EDPS supports the specific activities improving capacities to deal with cyber attacks, building capacities in law enforcement and judiciary bodies, and creating partnerships with the industry to empower citizens and business. Also, ENISA's role as facilitator of many of the actions provided in this objective is welcome.

58. However, the *ISS in Action* does not elaborate on law enforcement actions envisaged in cyberspace, how these activities could put individual rights at risk and what the required safeguards should be. The EDPS calls for a more ambitious approach on appropriate guarantees; this approach should be set forth to protect the fundamental rights of all individuals, including those who may be affected by actions designed to counter any possible criminal activities in this area.

V. Conclusion and recommendations

59. The EDPS asks for linking various EU strategies and Communications in the process of the implementation of the ISS. This approach should be followed by a concrete action plan supported by a real assessment of needs, the outcome of which should be a comprehensive, integrated and well-structured EU policy on ISS.

[21] EDPS Opinion of 22 June 2010 on the Proposal for a Council Decision on the conclusions of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to United States for the purposes of Terrorist Finance Tracking Programme (TFTP II).

60. The EDPS also takes this opportunity to highlight the importance of the legal requirement of a real assessment of all existing instruments to be used in the context of the ISS and information exchange before proposing new ones. In this context, the inclusion of provisions requiring regular assessments of the efficiency of relevant instruments is highly recommended.

61. The EDPS suggests that in the preparation of the Multi-Annual Strategic Plan requested by the November 2010 Council Conclusions, account is taken of the ongoing work on the comprehensive data protection framework on the basis of Article 16 TFEU, in particular Communication (2009) 609.

62. The EDPS makes a number of suggestions on notions and concepts relevant from a data protection perspective which should be taken into account in the field of ISS, such as Privacy by design, Privacy and Data Protection Impact Assessment, Best Available Techniques.

63. The EDPS recommends that in the implementation of future instruments an impact assessment on privacy and data protection is conducted, either as a separate assessment or as part of the general fundamental rights' impact assessment carried out by the Commission.

64. He also invites the Commission to develop a more coherent and consistent policy on the prerequisites for use of biometrics in the field of ISS, and more alignment at EU level in terms of data subjects' rights.

65. The EDPS finally makes a number of comments on the processing of personal data in the context of border management and in particular by FRONTEX and possibly in the context of EUROSUR.

Done in Brussels, 17 December 2010

(**signed**)

Peter HUSTINX
European Data Protection Supervisor