

Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on migration

(2012/C 34/02)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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

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 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, and in particular Article 41 thereof ⁽²⁾,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 4 May 2011, the Commission issued a Communication on migration ⁽³⁾ ('the Communication'). In accordance with Article 41 of Regulation (EC) No 45/2001, the EDPS presents this Opinion on his own motion.
2. The EDPS has not been consulted before the adoption of the Communication. This is regrettable, as comments provided at an earlier stage could have helped to address some of the issues outlined in this Opinion.

Objectives and scope of the Communication

3. The Communication aims to set recent and future policy proposals in a framework that takes account of all relevant aspects of migration and to avoid 'a short-term approach limited to border control without taking account of long-term issues' ⁽⁴⁾. It is written mostly as a response to current events in North Africa, especially the conflict in Libya.
4. In order to do this, the Communication addresses humanitarian aid, border management, visas, asylum, the economic need for immigration and integration. It refers to a number of legislative proposals, some of which are new, while others have already been tabled. Many of these proposals deal with border management, which forms an important part of the Communication. Some of these would entail large-scale processing of personal data.
5. The Communication is only the first in a number of communications and proposals to be issued in the near future, each elaborating on particular aspects referred to in the present Communication. In this context, the European Council Conclusions of 23 and 24 June 2011 ⁽⁵⁾ mention that 'efforts will also be strengthened by pushing forward rapidly with work on "smart borders", to ensure that new technologies are harnessed to meet the challenges of border control. In particular, an entry/exit system

⁽¹⁾ OJ L 281, 23.11.1995, p. 31.

⁽²⁾ OJ L 8, 12.1.2001, p. 1.

⁽³⁾ COM(2011) 248 final.

⁽⁴⁾ Communication, p. 3.

⁽⁵⁾ European Council Conclusions of 23 and 24 June 2011, Conclusion, EUCO 23/11.

and a registered travellers' programme should be introduced. The European Council also welcomes the agreement reached on the agency for the operational management of large-scale IT systems in the area of freedom, security and justice'.

Aim of the Opinion of the EDPS

6. While matters of data protection do not form the heart of the Communication, it nevertheless mentions several initiatives and proposals in the area of border management, such as the entry-exit system and the registered traveller programme, which will have a significant impact on the fundamental right to data protection. In this context, the Communication highlights that border control makes a major contribution in the fight against crime and refers to the Internal Security Strategy presented by the Commission in 2010 ⁽⁶⁾.
7. Many of the proposals and initiatives mentioned will be elaborated in more detail in the future; the present Communication therefore provides an opportunity to comment on these initiatives at an early stage. For those initiatives that have already been tabled, such as the proposal for a regulation amending the Frontex Regulation ⁽⁷⁾, this presents an opportunity to reiterate some of the most essential comments made on earlier occasions pending the final adoption by the Council and the European Parliament.
8. The aim of this Opinion is not to analyse all policy areas covered and proposals mentioned in the Communication, but to:
 - address several data protection principles and notions such as purpose limitation, necessity, proportionality, and 'privacy by design', which should be taken into account when putting the approach outlined in the Communication into practice,
 - discuss the specific measures proposed in the Communication from a data protection perspective and provide advice already at this stage on how to ensure proper respect for fundamental rights, in particular the right to the protection of personal data.
9. To this end, the Opinion is divided in two main parts. The first part comments on the general approach taken in the Communication and contains horizontal considerations on the Communication, such as the need for evaluation and the implications of fundamental rights for the design of IT systems. The second part contains targeted comments on specific proposals and initiatives ⁽⁸⁾.

II. GENERAL COMMENTS

The Communication's approach

10. The EDPS welcomes the Communication's aim to avoid 'a short-term approach limited to border control without taking account of long-term issues' ⁽⁹⁾. A comprehensive and effective approach to migration cannot only consist of border control, but also has to integrate other aspects.

⁽⁶⁾ Commission's Communication on the EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM(2010) 673.

⁽⁷⁾ Proposal for a regulation 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), COM(2010) 61.

⁽⁸⁾ This Opinion will especially draw on and complement the EDPS Opinion of 17 December 2010 on the Communication 'Internal Security Strategy in Action' ('EDPS Opinion of 17 December 2010') (OJ C 101, 1.4.2011, p. 6); the EDPS Opinion of 15 December 2010 on the amended proposal for a regulation of the European Parliament and of the Council on the establishment of 'Eurodac' ('EDPS Opinion of 15 December 2010') (OJ C 101, 1.4.2011, p. 14); the EDPS Opinion of 30 September 2010 on the Communication 'Overview of information management in the area of freedom, security and justice' ('EDPS Opinion of 30 September 2010') (OJ C 355, 29.12.2010, p. 16); and the EDPS preliminary comments of 3 March 2008 on the border package ('EDPS preliminary comments of 3 March 2008'), available on the EDPS website.

⁽⁹⁾ Communication, p. 3.

11. Such a comprehensive approach must respect the fundamental rights of migrants and refugees, including their right to data protection. This is even more important as these groups often find themselves in vulnerable positions.
12. In this context, the Communication mentions that the Union's dual aim must be to maintain high levels of security while also making border crossings simpler for 'those who should be admitted, in full respect of their fundamental rights' ⁽¹⁰⁾. This formulation could give the impression that the fundamental rights of persons who — for various reasons — should not be admitted need not be respected. According to the EDPS, it is obvious that their rights do not necessarily include the right to settle in EU territory, in which case appropriate reactions, such as return operations, would need to be taken, however always respecting fundamental rights.
13. It is noted that in terms of border management, the Communication advocates an approach strongly based on the use of technology. Among others, it is in favour of increased surveillance at the border (see the envisaged European border surveillance system Eurosur) ⁽¹¹⁾. It also envisages exploring the possible establishment of new large-scale IT systems for processing information about travellers (an entry-exit system and a registered traveller programme) ⁽¹²⁾. Finally, it advocates the expansion of existing systems to new users (i.e. for Eurodac) ⁽¹³⁾. This focus on technology reflects a general tendency in recent years.

Evaluation of existing instruments before proposing new ones and the necessity test

14. The EDPS has on many occasions emphasised that existing instruments should be evaluated before proposing new ones ⁽¹⁴⁾. In this context, recalling the case-law of the European Court of Human Rights ⁽¹⁵⁾ and the European Court of Justice ⁽¹⁶⁾, the EDPS points out that interferences with the right to private life must meet the standard of being 'necessary in a democratic society' and comply with the principle of proportionality. The notion of necessity implies a stricter burden of proof than just being 'useful' ⁽¹⁷⁾. This implies that any relevant proposals have to be accompanied by clear proof of their necessity and proportionality.
15. Such proof should be provided by a privacy impact assessment ⁽¹⁸⁾ based on sufficient evidence ⁽¹⁹⁾. A selective use of statistics and estimates is not sufficient. The EDPS is aware that gathering reliable information on phenomena such as irregular migration is difficult; however, these impact assessments

⁽¹⁰⁾ Communication, p. 7.

⁽¹¹⁾ Communication, pp. 7-8. See also paragraphs 42-44 of this Opinion.

⁽¹²⁾ Communication, p. 10.

⁽¹³⁾ Communication, p. 14.

⁽¹⁴⁾ See EDPS Opinion of 30 September 2010, cited above; see also EDPS preliminary comments on the border package, cited above. In this regard, the EDPS welcomes the work carried out by the information project mapping team in the context of the work on the European Information Exchange Model. However, the scope of this exercise should be extended and the future work in this area needs to take a broader perspective.

⁽¹⁵⁾ See for example European Court of Human Rights, *S. and Marper v. United Kingdom*, Nos 30562/04 and 30566/04, selected for publication in Reports of Judgments and Decisions.

⁽¹⁶⁾ For instance Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke and Hartmut Eifert v. Land Hessen* [2010], not yet published in European Court Report ('Schecke').

⁽¹⁷⁾ Numerous judgments since European Court of Human Rights *Handyside v. United Kingdom*, No 5493/72, Series A Number 24, §48.

⁽¹⁸⁾ These could either take the form of a separate privacy and data protection impact assessment or be integrated into the general impact assessment. The current guidance on impact assessments (European Commission Impact Assessment Guidelines, SEC(2009) 92) does not foresee a separate impact assessment for the impact on fundamental rights, such as data protection; these aspects are to be integrated in the general impact assessment. In the meantime, following the Commission's Communication on the strategy for the effective implementation of the Charter of Fundamental Rights by the European Union (COM(2010) 573), additional guidance has been prepared in the form of a Commission staff working paper on operational guidance on taking account of Fundamental Rights in Commission Impact Assessments (SEC(2011) 567).

⁽¹⁹⁾ See on this also EDPS Opinion of 25 March 2011 on the proposal for a directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime ('EDPS Opinion of 25 March 2011'), not yet published in the OJ, especially point 25.

would also have to consider alternative solutions to the problems faced in order to minimise the impact on fundamental rights⁽²⁰⁾. The mere fact that technological solutions are feasible does not mean that they are necessary and proportionate.

16. If an assessment leads to the conclusion that new large-scale IT systems are needed, the concept of 'privacy by design' should be taken into account when designing them. Controllers should be able to demonstrate that appropriate measures have been taken to ensure that privacy requirements have been met in the design of their systems. Doing so may limit the negative impact of new measures on privacy (or enhance the positive impact). This approach has been endorsed by the Commission⁽²¹⁾. Implementing 'privacy by design' in the context of systems such as the entry-exit system mentioned in the Communication, would result in restricting the collection of personal data to the minimum necessary, limiting retention periods and making processing privacy friendly and transparent to data subjects.
17. Additionally, the principle of purpose limitation must be adhered to. 'Function creep' has to be prevented. For instance, the Communication foresees the reintroduction of the initiative to give law-enforcement agencies access to Eurodac⁽²²⁾, which seems to confirm a tendency to grant access of law enforcement to the EU large-scale systems and raises the issue of the extension of the original purpose of the system. Granting additional authorities access to databases is an issue that may have a serious impact: a database regarded as proportionate when used for one specific purpose can become disproportionate when the use is expanded to other purposes afterwards⁽²³⁾.
18. Consequently, the EDPS calls for any (current and new) proposals involving restrictions to the fundamental right to data protection to be accompanied by clear proof of their necessity⁽²⁴⁾. Furthermore, when large-scale IT systems are deemed necessary, they should be designed with due account to the principle of 'privacy by design'. Additionally, implemented measures should be regularly evaluated to establish whether they are still necessary.

III. SPECIFIC COMMENTS

Eurodac

19. The Communication refers to law enforcement access to Eurodac, saying that Eurodac, apart from continuing to support the efficiency of the Dublin Regulation, should also be 'meeting other needs of law enforcement authorities'⁽²⁵⁾.
20. The December 2008 proposal for a reform of the Eurodac Regulation⁽²⁶⁾ did not contain provisions for law enforcement access. These were included in a proposal put forward by the Commission in

⁽²⁰⁾ On the need to consider alternative solutions see also the ECJ in *Schecke*, cited above.

⁽²¹⁾ Commission's Communication on a comprehensive approach on personal data protection in the European Union, COM(2010) 609, p. 12. See also the EDPS Opinion of 14 January 2011 on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — 'A comprehensive approach on personal data protection in the European Union' (OJ C 181, 22.6.2011, p. 1), paragraphs 108-115.

⁽²²⁾ Communication, p. 14.

⁽²³⁾ See EDPS preliminary comments on the border package, cited above, p. 3.

⁽²⁴⁾ See also the EDPS Opinion of 31 May 2011 on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), not yet published in the OJ, as well as the EDPS Opinion of 25 March 2011.

⁽²⁵⁾ Communication, p. 14.

⁽²⁶⁾ 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), COM(2008) 825.

September 2009⁽²⁷⁾. In October 2010, the Commission adopted an amended proposal⁽²⁸⁾ which no longer included provisions for law enforcement access, similar to the original proposal.

21. In his Opinion of 15 December 2010 on Eurodac, the EDPS welcomed the omission of law enforcement access⁽²⁹⁾, recalling that such a use for a different purpose must be based on substantial evidence of a link between asylum applicants and terrorism and/or serious crime. Additionally, the precarious situation of asylum seekers has to be taken into account when analysing the necessity and proportionality of such access.
22. The reform of the Eurodac Regulation is part of the establishment of a European asylum system, which according to the Stockholm Programme should be put in place by 2012⁽³⁰⁾. One of the reasons given by the Commission for the omission of law enforcement access in the October 2010 proposal was that not including this controversial measure could facilitate a timely adoption of the asylum package⁽³¹⁾. This is also linked to the establishment of the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice⁽³²⁾.
23. Against this background and in light of previous comments, the EDPS takes the position that until now sufficient clear and reliable evidence of the necessity of the reintroduction of the law enforcement access to Eurodac was not produced. Only after a new impact assessment, taking into account privacy concerns, such reintroduction could possibly be contemplated. Moreover, including access for law enforcement authorities would require significant changes to the Eurodac database in order to accommodate such access in a secure manner. The technical and financial implications of this would also need to be addressed in a new impact assessment⁽³³⁾.
24. Furthermore, the reintroduction of the proposal might have a significant impact on the timing of the asylum package as a whole. The Commission does not mention a date when a possible new proposal should be put forward; neither does it mention whether such a proposal would be accompanied by a new impact assessment.

⁽²⁷⁾ Amended proposal for a regulation of the European Parliament and of the Council 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), COM(2009) 342. The EDPS issued an opinion on this proposal, see EDPS Opinion of 7 October 2009 on the amended proposal for a regulation of the European Parliament and of the Council 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), and on the proposal for a Council decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes ('EDPS Opinion of 7 October 2009') (OJ C 92, 10.4.2010, p. 1).

⁽²⁸⁾ Amended proposal for a regulation on 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), COM(2010) 555 ('COM(2010) 555'). The EDPS issued an opinion on this proposal, see EDPS Opinion of 15 December 2010, cited above, especially paragraphs 18-22, 28-33, 51-57.

⁽²⁹⁾ EDPS Opinion of 15 December 2010, especially paragraphs 12-17.

⁽³⁰⁾ European Council: The Stockholm Programme — An open and secure Europe serving and protecting citizens, p. 5 (OJ C 115, 4.5.2010, p. 1).

⁽³¹⁾ COM(2010) 555, cited above, p. 3.

⁽³²⁾ Ibid.

⁽³³⁾ The October 2010 proposal was not accompanied by an impact assessment. Instead, the Commission referred to the impact assessment conducted for the 2009 proposal, see Commission staff working document — Accompanying document to the amended proposal for a regulation of the European Parliament and of the Council 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) and to the proposal for a Council decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes — Impact assessment, SEC(2009) 936. See also COM(2010) 555, cited above, p. 3.

Entry-exit system

25. The Communication also announces a Communication on smart borders to be issued in September 2011. This Communication is supposed to elaborate on initiatives for an entry-exit system and a registered traveller programme. The Commission acknowledges that these projects would require 'substantial investment' in order to ensure 'high level standards for the protection of personal data' ⁽³⁴⁾.
26. As regards the entry-exit system, the Commission justifies this initiative by claiming that 'over-stay' is 'the main source of irregular immigration in the EU' ⁽³⁵⁾. Apart from that, the Communication does not provide explanation as to the purpose of this system.
27. Reducing the number of 'overstayers' can certainly have positive effects. The EDPS understands that an entry-exit system could deter third country nationals from overstaying if they know that they are likely to be identified automatically once their visa expires. However, several questions remain.
28. So far, there is no consistent policy relating to the phenomenon of overstaying in the Member States. The concept of 'overstaying' in general is not well defined; arriving at a common definition of the term would be a necessary first step towards a clear understanding of the issue ⁽³⁶⁾.
29. Additionally, any numbers available so far are estimates ⁽³⁷⁾. The dimension of the problem would need to be clarified as a precondition for a reasoned assessment on necessity.
30. Alerts under Article 96 of the Schengen Implementing Convention are an existing measure for preventing specific persons from entering the Schengen territory. These alerts can be used to stop known 'overstayers' from re-entering ⁽³⁸⁾. In a recent Communication, the Commission called on Member States to use this possibility to the fullest extent possible ⁽³⁹⁾. This implies that the measure is currently not used to its full extent.
31. The entry-exit system would probably also rely on biometrics. While the EDPS acknowledges the possible benefits of the use of biometrics, he is also compelled to point out their weaknesses. Any use of biometrics must be accompanied by stringent safeguards and should take into account the risk of mistake ⁽⁴⁰⁾. In this context, the EDPS encourages the establishment of a set of minimum criteria related to the use of biometrics such as reliability of biometrics, targeted impact assessment on biometrics, accuracy and a fallback procedure ⁽⁴¹⁾. Additionally, a certain portion of the population involved does

⁽³⁴⁾ Communication, p. 10.

⁽³⁵⁾ Communication, p. 10.

⁽³⁶⁾ It would also need to be clarified which exceptions — for example for medical or humanitarian reasons — would apply.

⁽³⁷⁾ See EDPS Opinion of 30 September 2010, cited above, paragraphs 52-56.

⁽³⁸⁾ See EDPS preliminary comments of 3 March 2008, cited above, p. 4.

⁽³⁹⁾ Commission's Communication: Annual report on asylum, COM(2011) 291, p. 9.

⁽⁴⁰⁾ See e.g. EDPS Opinion of 16 October 2006 on the modified proposal for a Council regulation amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals (OJ C 320, 28.12.2006, p. 21); see also Article 29 Data Protection Working Party Opinion No 3/2007 on the proposal for a regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics, including provisions on the organisation of the reception and processing of visa applications (COM(2006) 269 final), WP134 of 1 March 2007.

⁽⁴¹⁾ See e.g. EDPS Opinion of 19 October 2005 on the proposal for a Council decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II), the proposal for a regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (...) (OJ C 91, 19.4.2006, p. 38); and 'Towards more comprehensive data protection in Europe including biometrics — a European perspective', 12th Conference — Biometrics Institute Australia, Sydney, 26 May 2011:

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2011/11-05-26_Biometrics_Institute_EN.pdf

not have fingerprints that could be read by such a system⁽⁴²⁾. If the entry-exit system is to include biometrics, it would have to provide for fall-back procedures for these travellers⁽⁴³⁾.

32. The EDPS would also like to draw attention to the experiences with regard to US-VISIT (United States Visitor and Immigrant Status Indicator Technology), a similar system in the USA. Under US-VISIT, most third country nationals are obliged to provide biometrics upon entering US territory. The 'exit' part of this system is still under development. In 2009, two pilot tests on collecting biometrics for this part of the system were conducted⁽⁴⁴⁾. The Department of Homeland Security acknowledged that the results of these tests were 'overstated due to system limitations related to instances where ADIS records did not reflect up-to-date traveller status due to recent changes or extensions of status'⁽⁴⁵⁾. The tests also screened passengers against several watch lists; however, 'none of the [...] hits would have prevented departure'⁽⁴⁶⁾. In total, the Department of Homeland Security has spent about 1,3 billion USD for developing the entry component of US-VISIT⁽⁴⁷⁾. This raises the question of whether an entry-exit system is a cost-efficient measure to reduce 'overstaying'.
33. In short, neither the purpose of such a system nor the way it would be constructed and implemented is sufficiently clear. As regards the need for action, there is no clear definition of the central term of 'overstaying'; consequently, there are no reliable statistics on the size of the problem. As regards the action to be taken, the existing instruments in place to prevent known 'overstayers' from re-entering are probably not used to the extent they should be; additionally, the biometric component of the entry-exit system raises questions. As regards the feasibility and cost of this system, experiences from the USA suggest that an entry-exit system will be expensive to implement. These points cast doubts on the necessity and cost-effectiveness of an entry-exit system.

Registered traveller programme

34. The Communication also mentions the introduction of a registered traveller programme. It is not entirely clear what the added value of this system would be, as compared for instance to using multiple-entry visa with a long period of validity. The target groups would be the same (frequent travellers). The fact that there is still 'reluctance'⁽⁴⁸⁾ to issue such visas cannot on its own serve as a reason to propose new measures instead, when the ones currently in place — if fully used — would allow the same objectives to be met. In light of the above, the EDPS is not fully convinced that the system is really necessary.
35. Moreover, the Communication refers to the concept of 'bona fide' travellers (page 11), mostly relating to the registered travellers programme. Implicitly, this wording might be read as creating a class of 'mala fide' travellers. Only those travellers taking extra steps, enrolling in the registered travellers

⁽⁴²⁾ This can for example be due to illnesses, disabilities, wounds and burns. It also seems to be the case that the fingerprints of persons working in agriculture and construction may, in a non-trivial number of cases, be damaged to the point that they become unreadable. See also EDPS Opinion of 15 December 2010, cited above, paragraph 19.

⁽⁴³⁾ For similar comments in the context of Eurodac see EDPS Opinion of 15 December 2010, paragraphs 18-25.

⁽⁴⁴⁾ In one of the airports selected for testing, USD 393 410 in labour costs and expenses were incurred for 35 days of test operations, which lead to 90 cases of suspected 'overstay'. In a second test conducted at the same time, there were 44 suspected hits, at the cost of USD 77 501. These numbers do not include development costs. For an assessment of these tests see: United States Government Accountability Office: US-VISIT Pilot Evaluations Offer Limited Understanding of Air Exit Options, August 2010, GAO-10-860, available at: <http://www.gao.gov/new.items/d10860.pdf> ('US GAO: US-VISIT Pilot Evaluations').

⁽⁴⁵⁾ Reproduced in US GAO: US-VISIT Pilot Evaluations, p. 72.

⁽⁴⁶⁾ US GAO: US-VISIT Pilot Evaluations, p. 72.

⁽⁴⁷⁾ See EDPS preliminary comments of 3 March 2008, cited above, p. 4.

⁽⁴⁸⁾ Communication, p. 11.

programme and supplying additional personal information, would be regarded as 'bona fide'. The starting assumption would no longer be that travellers in general are to be considered as entering the Union in good faith, unless specific evidence causes suspicion, but that it would be up to travellers to exculpate themselves by supplying additional information about themselves, even in the absence of any evidence. This implies that by declaring only some travellers 'bona fide', those who are not willing to provide additional information de facto become labelled 'mala fide', although such a refusal to supply additional information can have legitimate reasons, e.g. not travelling frequently⁽⁴⁹⁾.

Frontex and interagency cooperation

36. The Communication calls for 'close interagency cooperation' between Europol, Frontex and national customs and police authorities, which is deemed 'essential', especially between border control and customs authorities⁽⁵⁰⁾. This cooperation will be supported by proposals on best practices to be put forward during 2012. The Commission also announces a legislative proposal to be put forward during 2011 allowing Member States' agencies carrying out border surveillance to 'share operational information and to cooperate with each other and with Frontex'⁽⁵¹⁾. Finally, the proposal to update Frontex's legal framework in order to 'be more effective in terms of its operational capacity' is currently negotiated in Council and European Parliament⁽⁵²⁾.
37. With a view to ensuring consistency and creating an added value from a data protection perspective, the respective provisions in the legal bases for concluding possible cooperation agreements and exchanging personal data between Frontex and the agencies it shall cooperate with should be coherent and consistent to ensure full cooperation between the bodies in respect of data protection rules.
38. The EDPS reiterates furthermore the points raised in his Opinion on the proposal for a reform of the Frontex Regulation⁽⁵³⁾, specifically the need for a clear legal basis for the processing of personal data. If Frontex is given a mandate to exchange personal data, this should include strong and clear provisions on data subject rights, as well as other safeguards. Any provision allowing Frontex to process and/or exchange personal data should be precise and clearly delineated.

Eurosur

39. The Commission also announces a legislative proposal for defining the scope, purpose, and technical and operational framework for the European border surveillance system (Eurosur) for December 2011⁽⁵⁴⁾. This proposal is supposed to ensure 'greater use of modern technology at land as well as sea borders'⁽⁵⁵⁾ as well as the exchange of operational information on incidents⁽⁵⁶⁾. This is also related to Frontex, as the Commission plans to put forward another proposal allowing Member States' authorities carrying out border surveillance to share operational information with each other and Frontex⁽⁵⁷⁾.

⁽⁴⁹⁾ See also EDPS preliminary comments of 3 March 2008, cited above.

⁽⁵⁰⁾ Communication, p. 10.

⁽⁵¹⁾ Communication, p. 8.

⁽⁵²⁾ Communication, p. 8.

⁽⁵³⁾ 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), not yet published in the OJ; see also EDPS Opinion of 17 December 2010, cited above, paragraphs 48-51.

⁽⁵⁴⁾ Communication, p. 18.

⁽⁵⁵⁾ Communication, p. 7.

⁽⁵⁶⁾ Communication, p. 8.

⁽⁵⁷⁾ Communication, p. 8.

40. It is not clear whether and to which extent this would include processing personal data ⁽⁵⁸⁾. The EDPS encourages the Commission to clarify these matters in the proposals to come.

European system of border guards

41. The Communication mentions that the feasibility of a European system of border guards should be considered. It is not clear from the text what this system could look like. According to the text, it would not 'necessarily' ⁽⁵⁹⁾ have to be a central administration, which still leaves open the possibility that there could be one. If there is not to be a central administration, the Commission suggests that — among others — 'shared capacities' and 'practical cooperation' will have to be improved ⁽⁶⁰⁾.
42. It is not clear whether this is meant to aim at better implementation of existing measures or if it hints at new, as yet unannounced proposals. Given that 'practical cooperation' would likely include the exchange of personal data, which would necessarily have to have a legal basis, this should be specified in future proposals, if the project is to be pursued.

IV. CONCLUSION AND RECOMMENDATIONS

43. In line with the established case-law of the European Court of Justice and the European Court of Human Rights, the EDPS recalls the requirement of necessity and proportionality for all (current and new) proposals that infringe the fundamental rights to privacy and data protection. For each proposal, necessity would have to be demonstrated by a privacy impact assessment.
44. The principle of 'privacy by design' and the purpose limitation principle must be observed when proposing and designing new large-scale IT systems.
45. The EDPS urges that any use of biometrics should be accompanied by stringent safeguards and fall-back procedures for those who cannot enrol. In more general terms, minimum conditions for the use of biometric data should be established.
46. Furthermore, the EDPS urges the Commission to clarify the scope and content of its proposals mentioned in this Opinion. This applies to the announced legislative proposals related to the entry-exit system, the registered traveller programme, Eurosur, Frontex and interagency cooperation, as well as to the Communication on smart borders and the study into a European system of border guards.
47. He also calls on the Commission not to re-introduce the proposal on law enforcement access to Eurodac, unless a new impact assessment would clearly demonstrate the necessity of the proposal including technical and financial implications for the system.
48. The EDPS will closely follow these developments and issue additional comments where appropriate. He is available for further consultations, in the spirit of good cooperation.

Done at Brussels, 7 July 2011.

Peter HUSTINX
European Data Protection Supervisor

⁽⁵⁸⁾ See also the EDPS Opinion of 17 December 2010, cited above, paragraphs 46-47, in which already addressed this issue. This Opinion also addresses the so far unresolved question of the nature of the envisaged links between Frontex and Eurosur.

⁽⁵⁹⁾ Communication, p. 7.

⁽⁶⁰⁾ Communication, p. 7.