Opinion of the European Data Protection Supervisor

on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU"

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[2], and in particular Article 41 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

I.1. Consultation of the EDPS

1. On 27 November 2013, the Commission adopted the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows"[3] (hereinafter: "the Communication on rebuilding trust"). This Communication is accompanied by a Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection (hereinafter: "the Report" and "the Working Group").

2. On the same date, the Commission adopted a Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour

[1] OJ L 281, 23.11.1995, p. 31 (hereinafter: "Directive 95/46/EC").
[2] OJ L 8, 12.1.2001, p. 1 (hereinafter: "Regulation 45/2001).
[3] COM(2013) 846 final.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

from the Perspective of EU Citizens and Companies Established in the EU"[4] (hereinafter: "the Communication on Safe Harbour").

3. The EDPS welcomes that he was given the possibility to provide informal comments to the Commission before the adoption of the above-mentioned documents. These documents were adopted by the Commission in the aftermath of the revelations about the surveillance programmes carried out by US intelligence services. Considering the impact of these surveillance programmes on individuals' rights to privacy and to the protection of their personal data in the EU, he has decided to adopt this Opinion on his own initiative.

I.2. Objective and scope of the Commission documents

a) The Communication on rebuilding trust and the Report

4. The Communication proposes a way forward following the revelations on large-scale US intelligence collection programmes (hereinafter: "the programmes" or "the revealed programmes") and their impact on trust between the EU and the US. It does not refer to revelations on the conduct of similar activities and/or collaboration with the US by EU Member States or by other third countries.

5. The Report collates the findings of the EU Co-chairs of the ad-hoc EU-US Working Group on Data Protection that was created further to the COREPER meeting of 18 July 2013 to establish the facts about the programmes and their impact on fundamental rights in the EU and personal data of EU citizens. It analyses the US legal framework[5], how the collection and further processing of data takes place[6] and the existing oversight and redress mechanisms.

6. The Report mentions a "second track" that was also established during the COREPER meeting of 18 July 2013. It states that, under that "second track" EU institutions may raise with the US authorities questions relating to the alleged surveillance of EU institutions and diplomatic missions, whilst Member States may discuss with the US authorities, in a bilateral format, matters relating to their national security.

7. The Report also states that this division set some limitations to the discussion in the Working Group and the information provided therein. The EDPS has not been provided with any information on the "second track" or on the creation of a parallel working group in this regard. The Commission is therefore requested to inform the EDPS about the findings of the "second track", in particular as regards the alleged surveillance of EU institutions and diplomatic missions.

b) The Communication on Safe Harbour

[4] COM(2013) 847 final.

[5] In particular the Constitution, as interpreted by the Supreme Court; Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA) (as amended by the 2008 FISA Amendments Act, 50 U.S.C. § 1881a); and Section 215 of the USA PATRIOT Act 2001 (which also amended FISA, 50 U.S.C. 1861) and Executive Order 12333.

[6] On the basis of the information provided by the US in the Working Group and declassified documents, including opinions of the Foreign Intelligence Surveillance Court (hereinafter: "FISC") and publicly available documents such as the Attorney General's Guidelines for Domestic FBI Operations.

8. The Communication on Safe Harbour analyses the functioning of the Safe Harbour, identifies shortcomings and proposes possible improvements. It acknowledges the increasing amount of data transferred between the EU and the US and the growing number of companies adhering to the Safe Harbour principles. After recalling the structure and the functioning of the Safe Harbour, the Commission insists on the need to improve the enforcement of the principles on adhering companies and their subcontractors. According to the Communication, this would require that the Safe Harbour principles are incorporated in adhering companies' privacy policies more effectively and are made available to the public. The FTC should enforce their compliance more proactively. Besides, data protection authorities should participate in raising awareness of Safe Harbour in the EU and in particular on the existence of the EU data protection panel. The Commission also gives solutions to improve alternative dispute resolution mechanisms.

9. Regarding access to data transferred in the framework of the Safe Harbour scheme and further processed by US authorities, the Commission insists that it should be limited to what is strictly necessary and proportionate. It also requires that the use of limitations to privacy policies to meet national security, public interest or law enforcement requirements be carefully monitored so that it does not undermine the protection afforded. It also encourages adhering companies to be transparent on these limitations and their effect on the confidentiality of communications to raise citizens' awareness.

I.3. Scope and aim of the present Opinion

10. The present Opinion focuses on the Communication on rebuilding trust, and within that context also on the Communication on Safe Harbour. In consequence, it does not comment directly on revelations regarding EU Member States, be it in collaboration with the US or on their own; or on surveillance activities by third countries other than the US.

11. The Opinion starts by commenting on the general approach of the Communication on rebuilding trust. Part II briefly analyses the applicability of the relevant legal framework and its consequences, including comments on the Communication on Safe Harbour. Since the Article 29 Working Party[7] is currently examining the applicable EU and international legal framework, the present Opinion does not go in detail in this part. Part III addresses the Commission's recommendations on the future steps to be taken.

I.4. Comments on the approach of the Communication on rebuilding trust

12. The Communication focuses on the fact that trust between the EU and the US as strategic partners has been negatively affected by the revelations on the programmes and needs to be restored. The EDPS welcomes this acknowledgement.

[7] The Article 29 Data Protection Working Party, set up under Directive 95/46/EC, has an advisory status and acts independently. It is composed of representatives of EU national Data Protection Authorities, the EDPS and the Commission.

13. However, the programmes, whose existence is in some cases clearly confirmed by the Report[8] affect not only trust, but also legal rights as laid down in EU and Council of Europe primary and secondary law, in particular the rights of privacy and data protection. They also show the large scale of foreign intelligence collection that is actually taking place under the US legal framework[9], as interpreted by the US Supreme Court[10]. The report also confirms the lack of safeguards, protections, rights, oversight and redress possibilities available for EU citizens under the US framework[11].

14. As repeatedly underlined by the Commission, citizens' and businesses' trust in Internet communications depends on the availability of effective technical protection tools for privacy, and more specifically the confidentiality of communications. This need has also been recognized in the US Review Group on Intelligence and Communications Technologies[12] which made several recommendations to restore the trust in encryption tools and commercial software, as well as in the functioning of rapid mechanisms to fix software vulnerabilities. The weakening of trust in these systems has been considered one of the most damaging effects of the recent discussions about signal intelligence operations by some of the most recognized security experts[13]. In view of the importance of effective cybersecurity for Europe, a response to this technical and political challenge should be developed at EU level, based on an initiative by the Commission.

15. In section 3 of the Communication, the Commission addresses the future steps that need to be taken to restore trust in data transfers between the EU and the US. The EDPS welcomes this section, which focuses on the improvement of the existing legal framework and proposes new instruments. However, the Commission does not address how applicable national, EU and Council of Europe instruments have been affected by the programmes. The EDPS considers that the impact on existing legal instruments should have received more attention in the Communication.

II. COMMENTS ON THE APPLICABLE LEGAL FRAMEWORK

II.1. EU and Council of Europe data protection legal frameworks

16. The rights to privacy and data protection are enshrined in primary law in Article 8 of the Council of Europe Convention on Human Rights and Fundamental Freedoms (hereinafter: "the ECHR"), Articles 7 and 8 of the EU Charter of Human Rights

[8] See p. 5, 10 and 26 of the Report, which, on the basis of declassified opinions of the Foreign Intelligence Surveillance Court, confirms that "US intelligence agencies have recourse to methods of collection under Section 702 that have a wide reach, such as the PRISM collection of data from internet service providers or through the "upstream collection" of data that transits through the US".

[9] The US confirmed that there are other legal bases for intelligence collection where the data of non-US persons may be acquired, but did not provide details on the legal authorities and procedures applicable. Not all the relevant legal bases were disclosed to the WG (see p.13 of the Report).

[10] See p.4-12 of the Report .

[11] See p.26-27 of the Report.

[12] "Liberty and Security in a Changing World", Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, in particular recommendations 25, 29 and 30. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[13] B Schneier, C Soghoian in report of 6 September 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; B. Preneel: ISSE 2013 closing keynote: "The Cryptographic Year in Review" http://homes.esat.kuleuven.be/~preneel/preneel_isse13.pdf

(hereinafter: "the Charter") and Article 16 of the Treaty on the Functioning of the EU (hereinafter: "the TFEU"). Article 17 of the International Covenant on Civil and Political Rights (hereinafter: "the ICCPR"), which has been ratified by the US also provides for the right not to be subject to arbitrary or unlawful interference with one's privacy. Council of Europe Convention 108 for the protection of individuals with regard to automated processing of personal data provides more details on the right to data protection.

17. Under secondary law, Directive 95/46/EC, Council Framework Decision 2008/977[14], Regulation (EC) 45/2001 and Directive 2002/58/EC[15], as interpreted by the EU Court of Justice, regulate the exercise of such rights. Together with Article 8(2) of the ECHR and Article 52(1) of the Charter, they specify the criteria and conditions to limit their exercise.

18. The above provisions of EU law do not apply to the national security of EU Member States since, according to Article 4(2) of the Treaty of the European Union (hereinafter: "TUE"), this is an "essential state function" of the Member States, which remains their "sole responsibility" and is thus regulated at national level.

II.1.1. Scope of national security exceptions

a) National security limiting the scope of application of EU instruments

19. The Communication states that "whilst the EU can take action in areas of EU competence, in particular to safeguard the application of EU law, national security remains the sole responsibility of each Member State"[16]. The EDPS welcomes this assertion of the EU's competence to safeguard the application of EU law. The EDPS also points out that the national security of third countries is not an essential function or sole responsibility of EU Member States and thus not covered by this exemption.

20. In any case, the exclusion of Member States' national security from the scope of application of EU law does not mean that national security remains an unregulated area, in particular as regards the protection of fundamental rights: the Council of Europe instruments mentioned above[17] and national laws are in most situations fully applicable to this field[18].

21. In particular, even where EU law does not apply, the European Convention of Human Rights and Convention 108 apply to many of the processing operations in question as their general application to most of their parties[19] does not exclude

[14] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. OJ L 350, 30.12.2008, p.6.
[15] 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, 31.07.2002, p.37.
[16] See p.4 of the Communication.
[17] Only a minority of the parties to Convention 108 have deposited declarations in accordance with Article 3(2)(a) stating that Convention 108 will not apply to "automated personal data files" relating to "State Security" or "State Secrets".
[18] See e.g., the decision of the Bundesverfassungsgericht decision in the Rasterfahndung case (BVerfG 1 BvR 518/02 of 4.4.2006).
[19] See footnote 17.

national security as a whole[20]. These instruments also create a positive obligation for their parties to secure privacy and data protection rights to everyone within their jurisdiction[21] and to adopt domestic law giving effect to data protection principles[22].

b) National security limiting rights granted by EU and Council of Europe instruments

22. Where the above mentioned EU and Council of Europe instruments apply, the rights to privacy and data protection can be restricted if necessary to safeguard national security or State security[23], among other reasons. However, such restrictions have to be interpreted in a restrictive way[24] and any limitation to the rights these instruments grant can only be allowed if it is laid down by a foreseeable and accessible[25] law[26] and only if it is necessary in a democratic society[27].

23. The exceptions provided by the aforementioned instruments for national security purposes can therefore not justify massive limitations to fundamental rights as the ones provided by the programmes, for purposes which can go beyond national security, mostly relate to interests of a third country[28], and are not strictly necessary to safeguard national security[29].

II.1.2. Enforceability of the EU and Council of Europe legal framework

a) Enforceability on controllers

24. National laws implementing Directive 95/46/EC are applicable to processing operations in the context of the activities of an establishment of controllers in the EU[30]. They are also applicable where a non EU controller is established in a place where a Member State's national law applies by virtue of international law or if the controller is using equipment in the EU[31]. EU Data Protection Authorities have thus competence in these cases to directly enforce their national data protection laws against organisations that have provided access to or disclosed personal data to third country governments in breach of national data protection laws.

---

[20] As in EU instruments, where Council of Europe instruments are applicable they provide for restrictions to certain rights, e.g., for national security purposes. However, such limitations must be interpreted in a restrictive way (see e.g., ECtHR, Klass and others v. Germany, judgment of 6 September 1978, Series A no.28).
[21] See Articles 1 and 8 of the ECHR.
[22] See Article 4(1) of Convention 108.
[23] See e.g., Article 8(2) of the ECHR, Article 9(2)(a) and Article 13(1)(a) of Directive 95/46/EC.
[24] ECtHR, Klass and others, above cited, at paragraph 42.
[25] ECtHR, Rotaru v. Romania, judgment of 4 May 2000, application no. 28341/95, paragraph 48.
[26] See Article 52(1) of the Charter.
[27] *Idem.*
[28] According to FISA, "foreign intelligence" as defined by FISA could include information concerning political activities of individuals or groups and activities of government agencies, provided that they could be of interest to the US for its foreign policy. The EU side of the WG asked for further specification of the scope of "foreign intelligence" but the US declined explaining that such clarifications would reveal specific operational aspects of the programmes. See p.5-7 of the Report.
[29] Under Section 702 FISA, data of non US persons is considered "foreign intelligence" as soon as they *relate* to the purposes pursued. Data of US persons, on the contrary, have to be *necessary* for the specified purposes in order to be considered "foreign intelligence". See p.26 of the Report.
[30] See Article 4(1)(a) of Directive 95/46/EC.
[31] See Article 4(1)(b-c) of Directive 95/46/EC and its interpretation by the Article 29 Working Party in the Opinion 8/2010 on applicable law (WP 179), available on http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm...

25. Since Regulation 45/2001 is also applicable, the EDPS has initiated a discussion with EU institutions and bodies on risks to confidentiality of communications and security of processing and the adoption of appropriate and effective technical security measures.

b) Enforceability on Parties to the ECHR

26. Articles 1 and 8 of the ECHR create a positive obligation for Parties to the Convention to protect privacy and data protection rights. As a consequence of the programmes, this obligation has not been fulfilled. Convention 108, which applies to processing operations in the States party to that Convention by the public and by the private sector, has in that context not been respected either.

27. EU Member States, as well as any Party to the ECHR, can be brought to the European Court of Human Rights (hereinafter: "ECtHR") for not complying with their obligation to "secure to everyone within their jurisdiction the rights and freedoms provided in the Convention"[32], in particular the right to privacy[33]. On 4 September 2013, a complaint was lodged against the United Kingdom by Big Brother Watch and others[34].

II.2. Instruments regulating transfers

a) Instruments regulating transfers from the EU to the US within the private sector

28. Exchanges of personal data between EU and US private companies and organisations are facilitated by several instruments adopted on the basis of Articles 25 and 26 of Directive 95/46/EC: Commission Decision 2000/520/EC (hereinafter: "the Safe Harbour Decision"); Commission Decisions 2001/497/EC, 2004/915/EC and 2010/87/EU (hereinafter: "the Standard Contractual Clauses") and a series of Article 29 Working Party documents on Binding Corporate Rules (hereinafter: "BCR").

29. Some of these instruments (Safe Harbour and Standard Contractual Clauses) allow for a derogation of the principles they provide where necessary in a democratic society, e.g. for national security purposes. In some cases (Safe Harbour, Standard Contractual Clauses and Binding Corporate Rules) they include a requirement to inform the EU transferor or the relevant EU Data Protection Authority where national laws in the recipient's country conflict with the principles these instruments provide for.

30. However, the programmes go beyond what is necessary, at least as regards data of non US persons[35]. In any case, such instruments were not designed to protect against massive onward transfers to or access by the government of the recipient organisation. The EDPS therefore recommends that they should be improved, in

[32] See Art.1 ECHR.
[33] See Art.8 ECHR.
[34] Big Brother Watch and Others v. the United Kingdom, application no. 58170/13, available on http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-140713, last accessed on 17.02.2014.
[35] See footnote 29.

particular the Safe Harbour, which has been discussed both in the Communication on rebuilding trust and more extensively in the Communication on Safe Harbour.

b) Implementation of Safe Harbour

31. The EDPS welcomes the analysis and the recommendations made by the Commission on the implementation of the Safe Harbour. The Communication on Safe Harbour states that the Commission has identified weaknesses such as a lack of transparency and of enforcement. It further notes that some self-certified Safe Harbour companies do not, in practice, comply with its principles, which has, among other consequences, a negative impact on EU citizens' fundamental rights.

32. The Communication on Safe Harbour also addresses the issue of 'access to data transferred in the framework of the Safe Harbour Scheme'. The Communication on rebuilding trust raises the question of whether the large-scale collection and further processing of personal data under the programmes fulfils the Safe Harbour requirements of necessity and proportionality. The Commission finds that Safe Harbour acts as "a conduit for the transfer of the personal data of EU citizens from the EU to the US by companies required to surrender data to US intelligence agencies".

33. In this respect, the EDPS also welcomes the reaffirmation by the Commission that: "in order for limitations and restrictions on the enjoyments on fundamental rights to be valid they must be narrowly construed; they must be set forth in a publicly accessible law and they must be necessary and proportionate in a democratic society"[36]. Any limitation to data protection rules for national security should meet these conditions. This "necessity" requirement is already set out in the Safe Harbor Decision[37] which states that: "Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements".

34. However, the EDPS regrets that the Commission concludes that "large scale access by US authorities to data processed by Safe Harbour self-certified companies" only "risks undermining the confidentiality of electronic communications", without specifying that such access goes beyond the limits referred to in the Safe Harbour principles. The EDPS considers that both the large scale of the programmes and the fact that under US law the "necessity" requirement only applies to data of US persons[38] show that the programs do not fulfil the condition of necessity as regards non US persons[39].

c) Instruments regulating transfers from the EU to the US for law enforcement purposes

35. In addition to the above mentioned instruments, several agreements regulate the exchange of personal data between the EU and the US for law enforcement purposes, including the prevention and combating of terrorism:

[36] See p.17, first para. of the Communication on Safe Harbour.
[37] See annex I, Safe Harbor Privacy Principles, paragraph 4.
[38] See footnote 29.
[39] See also the decision of the EU Court of Justice in the Huber case, C-524/06.

- the Mutual Legal Assistance Agreement (hereinafter: "the MLAA")[40],
- the Agreement on the use and transfer of Passenger Name Records (hereinafter: "the PNR Agreement")[41],
- the Agreement on the processing and transfer of Financial Messaging Data for the purpose of the Terrorist Finance Tracking Program (hereinafter: "the TFTP Agreement")[42], and
- the Agreement between Europol and the US[43].

36. Access by US authorities to data processed under EU jurisdiction should exclusively take place under these agreements.

37. The revelations on the programmes include allegations that the PNR agreement and the TFTP agreement may have been breached. According to the Commission, there is no evidence proving such allegations[44]. However, recent developments would require a more prudent judgment, especially as far as TFTP is concerned, in view of the concerns raised by the Europol Joint Supervisory Board[45] and the joint investigation by the Dutch and Belgian Data Protection Authorities[46].

38. As regards exchanges of information for law enforcement purposes, the Communication asserts that the PNR Agreement and the TFTP Agreement provide "a high level of protection of personal data". As explained on a number of occasions[47],

[40] Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 291, 7.11.2009, p. 40.

[41] Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security (Council Decision Council Decision 2012/472/EU of 26 April 2012, OJ L 215, 11.8.2012, p. 4).

[42] 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 the United States for the purposes of the Terrorist Finance Tracking Program (Council Decision of 13 July 2010, OJ L 195, 27.7.2010, p. 3).

[43]Agreement Between the United States of America and the European Police Office of 6 December 2001 and Supplemental Agreement between the Europol Police Office and the United States of America on the exchange of personal data and related information of 20 December 2002..

[44] The Communication states that neither the joint review of the implementation of the PNR Agreement nor the formal consultations opened by the Commission on the TFTP Agreement "revealed any elements proving a breach of these agreements", and that the US have provided written assurance that no direct data collection has taken place contrary to the provisions of the TFTP Agreement.

[45] Report of the JSB of 18 March 2013 on the implementation of the TFTP agreement.

[46] Joint press release of Belgian and Dutch Data Protection Authorities of 14 November 2013.

[47] See the EDPS Opinion of 30 September 2013 on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data; Opinion of 9 December 2011 on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security; Opinion of 15 July 2011 on the Proposal for a Council Decision on the conclusion of an Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service; Opinion of 19 October 2010 on the global approach to transfers of Passenger Name Record (PNR) data to third countries; Opinion of 15 June 2005 on the Proposal for a Council Decision on the conclusion of an agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information (API) / Passenger Name Record (PNR) data; all available on www.edps.europa.eu.

the level of protection provided by these agreements is questionable and such a statement can therefore not be made without reservations[48].

39. While the allegations that the PNR and the TFTP agreements may have been breached are not confirmed, there is no evidence either of any investigation being conducted in this regard. The EDPS may react separately to the US PNR joint review report, the TFTS Communication and the TFTP joint review report.

III. SPECIFIC COMMENTS ON THE FUTURE STEPS TO TAKE

III.1. A swift adoption of the EU data protection reform

40. The EDPS shares the views of the Commission on the importance of the proposals for a new data protection framework (hereinafter: "the proposals")[49] in this context. The Communication mentions in particular five elements of the proposals: the extension of the territorial scope of application, the clarification of the conditions for transfers, the harmonisation and reinforcement of the enforcement powers of EU Data Protection Authorities, the inclusion of clear rules on the obligations and liabilities of processors, and the establishment of "comprehensive rules" for the protection of personal data in the law enforcement area.[50]

41. In this respect, the EDPS would highlight two further elements that are being discussed by the co-legislators: (i) addressing the processing for law enforcement purposes of personal data initially collected for commercial purposes, and (ii) addressing international conflicts of law.

42. The first of these further elements relates to the fact that, despite the possibilities offered by the new legal basis provided by Article 16 TFEU, the data protection package does not consist of a single comprehensive proposal but of two proposals with different material scope. This is likely to create legal uncertainty for situations where personal data initially subject to the proposed Data Protection Regulation are subsequently processed for purposes and by authorities subject to the proposed Data Protection Directive. This problem was already highlighted by the Commission in the Impact Assessment[51] but not solved by the proposals. The EDPS recommends that the co-legislators correct this omission and regulate these situations.

43. As regards international conflicts of law, it should be made clear that all processing activities which fall within the scope of the data protection package should comply with it, unless a binding international agreement granting adequate data protection safeguards has provided otherwise, or unless a judicial or a data protection authority has granted an exemption.

---

[48] See also Article 29 Working Party Opinions on PNR agreements between the EU and third countries, available on http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

[49] Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012)11) final and Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012)10 final).

[50] See p.5-6 of the Communication on rebuilding trust.

[51] See Annex III, p. 4 of the Impact Assessment accompanying the proposals (SEC(2012) 72 final).

44. The EDPS supports the conclusive remark of the Communication insisting on the fact that recent events constitute a "wake-up call" for the EU and its Member States "to advance swiftly and with ambition on the data protection reform".

III.2. Strengthening the Safe Harbour

45. In the Communication on rebuilding trust the Commission proposes strengthening the Safe Harbour. The EDPS welcomes this proposal but he would have favoured the use of more affirmative language. As stated above, the EDPS also underlines the need to draw the appropriate legal conclusions regarding the insufficient respect for the Safe Harbour principles.

46. In particular, the strengthening of the scheme should be the *outcome* of the review of its functioning, rather than the other way around. Even if the Communication on rebuilding trust brings forward several justifications for maintaining the scheme, the final choice should depend on the way the recommendations made in the Report are effectively implemented. In case of failure, the suspension or revocation of the scheme might still be envisaged.

47. Different scenarios could be envisaged, including possible actions depending on the outcome of the review. Such scenarios should provide for an in-depth analysis of the possible application of Article 3 and/or Article 4 of the Safe Harbour Decision, and explain in which cases and under what conditions suspension could be an option, and where Article 4 would be the basis for better defining the Safe Harbour principles, and in particular the exact scope of the exception for national security as opposed to other interests which fall outside the exception.

48. In this respect, the EDPS considers that the Communication on rebuilding trust would have benefitted from more ambition when defining the next steps to be taken. The text does not provide for any precise deadline except for the identification of "remedies" by summer 2014, to be implemented "as soon as possible"[52]. It is not clear to what these remedies refer. Both the Report and the Communication identify steps to be taken to improve the functioning of the scheme, and the EDPS recommends that the Commission indicates more precisely how such steps could be implemented in practice. In addition, the substance and schedule of the "broader review process" should be better defined.

49. As regards the possible ways to improve the Safe Harbour, the EDPS shares with the Commission the opinion that any reform should address the structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception.

50. In particular, the EDPS welcomes the statements that (a) the monitoring and supervision by US authorities of compliance with the Safe Harbour principles should be more effective and systematic, (b) the transparency of certified organisations' privacy policies should be improved, (c) the availability and affordability of dispute

[52] See p.7.

resolution mechanisms for EU citizens should be ensured, and (d) the national security exception should only be used where strictly necessary and proportionate.

51. Independently of the policy option chosen, currently self-certified Safe Harbour organisations should comply with all the scheme's principles, including transparency. At the same time, US intelligence agencies should not address requests to Safe Harbour members beyond what is strictly necessary and proportional for national security purposes.

52. The EDPS also finds it necessary to :
    a. review the FAQ of the Safe Harbour principles in order to clarify their application and explain their practical implications for companies who choose to adhere to them. This will also be the occasion to clarify the modalities of application to processors, in particular in the case of onward transfer and increase the degree of liability of European data controllers for checking that companies located in the US which claim to comply with the Safe Harbour principles effectively do so;
    b. involve European data protection authorities in an extensive communication campaign on the Safe Harbour once the FAQ have been reviewed;
    c. encourage the FTC to conduct more on-site inspections and increase the level of sanctions for non-compliance;
    d. insist on the fact that the Safe Harbour principles have not been designed for large-scale access of US intelligence authorities to data transferred under them.

III.3. Strengthening data protection safeguards in law enforcement cooperation

53. According to the Communication on rebuilding trust[53], the Council decision authorising the Commission to negotiate a general EU-US agreement for the exchange of data for law enforcement purposes (hereinafter: "the umbrella agreement"), which is not public, aims at ensuring "a high level of protection in line with the EU data protection acquis".

54. The EDPS welcomes this objective, as such an agreement could potentially establish a clearer framework for the exchanges of data that are or will be taking place, and provide stronger data protection safeguards. However, as the EDPS has previously warned, "such a framework could legitimise massive data transfers in a field - law enforcement - where the impact on individuals is particularly serious and where strict and reliable safeguards and guarantees are all the more needed"[54].

55. As the EDPS has also previously stated[55], in order to ensure consistency the EU should first agree on the reform of its internal data protection instruments, and on the basis of this framework it should negotiate agreements with third countries. Subsequently, a general EU-US agreement on the exchange of personal data for law

[53] See p.8.
[54] See the EDPS Opinion of 11 November 2008 on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection, available on www.edps.europa.eu.
[55] See, e.g., the EDPS Opinion on the Communication from the Commission on the global approach for transfers of Passenger Name Record (PNR) data to third countries, cited above.

enforcement purposes should be the basis to negotiate sector-specific agreements (e.g. PNR and TFTP), rather than the other way round.

56. Taking into account the current context, the EDPS recommends ensuring that the future data protection framework applies to existing agreements on the exchange of personal data for law enforcement purposes, both at general and sectoral level. In particular, as stated in his opinion on the data protection reform, the EDPS recommends restricting in time the non-applicability of the data protection package, which should only refer to existing international agreements. Furthermore, the proposed Regulation and the proposed Directive should include a transitional clause providing for the review of international agreements within a set time in order to align them with the package. Such clauses should be included in the substantive provisions of both proposals and not only in their Preamble[56].

57. As stated above, the EDPS also questions the statement repeated in the Communication on rebuilding trust that the PNR and TFTP Agreements set strict conditions for transfer of data and safeguards for EU citizens.

58. The Communication on rebuilding trust states that "the negotiations provide an opportunity to clarify that personal data held by private companies and located in the EU will not be directly accessed by or transferred to US law enforcement authorities outside of formal channels of co-operation". The EDPS welcomes this assurance. However, the text further states that "access by other means should be excluded unless it takes place in clearly defined, exceptional and judicially reviewable situations". The EDPS recommends that the Communication should specify that any exception should only be allowed if it is strictly necessary, proportional and in line with the established case law of the European Court of Human Rights and the Court of Justice.

59. As regards the scope of the concept of national security, which may differ across the Atlantic, the EDPS welcomes the statement that derogations based on national security needs should be narrowly defined and that safeguards and limitations should be agreed in this respect.

60. As regards the safeguards mentioned in the Communication and those missing, such as judicial redress, the EDPS supports the aim of the Commission of obtaining commitments on enforceable rights including judicial redress mechanisms for EU citizens not resident in the US.

III.4. Addressing European concerns in the on-going US reform process

61. The Communication on rebuilding trust[57] cites possible improvements in the US legal framework, especially with a view to extend safeguards available to US citizens and residents to EU citizens not resident in the US. It also argues for more transparency and better oversight. Such changes should of course be welcomed and encouraged where they are likely to provide more and better protection to EU

[56] See the EDPS Opinion of 7 March 2012 on the data protection reform package, available on www.edps.europa.eu.
[57] See p.9.

citizens and the fundamental rights at stake, in particular as regards redress possibilities.

62. In this regard, the report of the Privacy and Civil Liberties Oversight Board of 23 January 2014, the speech of president Obama of 17 January 2014 and the Presidential Directives of the same date are good signals. However, further changes as just called for would not only increase trust and reduce the extent to which Europeans are affected by the programmes, as stated in the Communication, but would also reduce the situations where organisations may be caught in a conflict of jurisdictions.

63. The Communication states that such changes "would reduce the processing of personal data of Europeans that are not relevant for national security purposes". As stated above, the EDPS notes that this standard is inadequate and that personal data of Europeans should only be processed for national security purposes if this is strictly necessary and proportionate.

64. The EU should also encourage and support efforts by the US Administration and the US Congress to enact a general privacy act, providing for strong safeguards and adequate oversight, particularly in areas where any substantial protection of privacy rights is currently lacking.

65. Like the Commission, the EDPS would welcome the strengthening of the US domestic legal framework, including the passage of the "Consumer Privacy Bill of Rights" announced in February 2012 by President Obama[58]. The EDPS encourages the EU institutions to actively support the enactment of a comprehensive data protection framework in the US that would facilitate trans-border data flows while providing a high level of protection.

66. Being relevant stakeholders, the US government and the US private sector have contributed to the debate on the reform of the EU data protection framework. In order to increase understanding and trust, and taking into account the importance of transfers between the EU and the US, EU institutions should also actively provide their views on the legislative debates on privacy in the US.

III.5. Negotiations on the TTIP

67. The Commission refers to the negotiations between the EU and the US on a Transatlantic Trade and Investment Partnership (hereinafter: "TTIP") and states that data protection standards will not be negotiated within the TTIP, "which will fully respect the data protection rules".

68. The EDPS calls on the Commission to ensure that this commitment is respected and that issues that might be negotiated under the TTIP, such as "trans-border data flows"[59], standards and certificates for the cloud[60] or data security requirements[61] do

[58] See "Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", White House, February 2012, available at: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[59] See the comments of the Commission in p.4 of the report on the Civil Society Dialogue - Update on the TTIP of 16.07.2013, available on http://trade.ec.europa.eu/doclib/docs/2013/july/tradoc_151656.pdf, last accessed on 31.03.2014.

not have a negative impact on the protection of personal data. In particular, on the basis of Article XIV of the GATS, the text of the agreement should include a provision stating that it will apply without prejudice to the applicable data protection legislation.

69. At the same time, the Commission should consider setting a common goal of gradual development towards greater interoperability of legal frameworks for privacy and data protection, to which goal the US might contribute in ways mentioned in points 63 and 64.

III.6. Promoting privacy standards internationally

70. The EDPS supports the intention of the Commission[62] of internationally promoting EU rules on collection, processing and transfer of data. In particular, the EDPS supports the adoption of an international instrument requiring the respect of data protection standards by intelligence activities. This could be adopted at UN level on the basis of Article 17 of the International Covenant on Civil and Political Rights[63].

71. As regards the current discussions with regard to the Council of Europe Cybercrime Convention, the EDPS stresses that access of law enforcement authorities of third countries to data under EU jurisdiction should comply with EU data protection requirements[64].

72. The EDPS supports the view of the Commission that, in order to promote privacy standards internationally, the US should preferably accede to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), which is open to countries which are not member of the Council of Europe.

73. The EDPS considers that these efforts should be complemented with the improvement of cooperation among data protection authorities and privacy enforcement authorities around the world[65]. The development of international enforcement cooperation mechanisms should facilitate the enforcement of national, regional and international privacy and data protection laws in cross-border situations.

III.7. The need to subject intelligence activities to appropriate safeguards

---

[60] See the comments of the Commission in p.2 of the report on the TTIP Stakeholders Event of 12.06.2013, http://ec.europa.eu/digital-agenda/en/news/ttip-ict-stakeholders-event-report last accessed on 31.03.2014.

[61] See the Commission press release of 20.12.2013 on the third round of negotiations, available on http://trade.ec.europa.eu/doclib/press/index.cfm?id=1007, last accessed on 31.03.2014.

[62] See p.9 of the Communication on rebuilding trust.

[63] See the Resolution on Anchoring Data Protection and the Protection of Privacy in International Law, adopted by the International Conference of Data Protection and Privacy Commissioners (Warsow, 23-26 September 2013).

[64] See letter of the WP29 to the Cybercrime Committee of the Council of Europe of 5 December 2013, available on http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf.

[65] See the Resolution on International Enforcement Coordination, adopted by the International Conference of Data Protection and Privacy Commissioners (Warsow, 23-26 September 2013).

74. Intelligence services and related entities are operating in a loose framework within which the requirements for necessity and proportionality are more important than ever, but at the same time not always sufficiently addressed with legal safeguards and arrangements for adequate accountability and oversight. The ever growing use of telecommunications networks by users worldwide and the deployment of ever more powerful technical means for massive data collection and storage have considerably increased the capacities of intelligence agencies to gather data. The establishment of strong safeguards at all relevant levels is crucial to restrain this increased power and ensure that surveillance is necessary and interference in the right to the protection for private life is proportionate.

75. In the EDPS' view, one of the safeguards for ensuring that surveillance activities do not go further than what is necessary and proportionate consists in strengthening the supervision of those intelligence activities. Supervision should take place in different forms at different stages:

- At the moment of implementing a surveillance activity which involves a new processing operation, the need for an authorisation of the activity by a judge or another independent authority would reduce the risk of abuse by ensuring that necessity and proportionality are determined at the moment that decisions are taken that affect the private life of citizens. The authorisation should contain an assessment of the necessity and proportionality of the measure, provide for appropriate safeguards where necessary, and be limited in time.

- The whole processing operation should be subject to the appropriate and effective oversight by Parliaments or other competent independent bodies. The mandate of oversight bodies should be broadened to ensure they can inspect all aspects of the data processing carried out by all intelligence agencies.

- The exchange of data between intelligence agencies of different countries should also be subject to independent oversight.

76. Oversight bodies should be entrusted with the task of supervising the application of data protection principles to intelligence activities; they should also be given the appropriate powers to do so. The supervision of the application of data protection principles should include the following elements:

- The establishment of strong data quality checks: risk of errors can emerge when mixing private and public databases (cf. PNR) and data mining raises an accuracy problem that must be addressed.

- Regular examinations of personal data exchanges should be conducted to control the destination of the data, the purpose of the exchange, the quality of the recipients of the data, and the proportionality of the exchange in view of its interference on fundamental rights.

- Oversight bodies should cooperate with each other. This requires assisting the existing network of oversight bodies to meet and exchange information with each other on common problems and solutions found to this problem.

III.8. Ensuring effective IT security

77. The community of Internet engineers has recognized the dangers of mass surveillance and pledged to design and implement infrastructures that should be more resilient to interception[66]. European researchers have provided the foundations for many of the most important cryptographic mechanisms. In addition to encryption, developers of software, in particular on the Internet, should be aware of privacy risks of their products and use concrete design methods to avoid or at least reduce them.

78. The EU should analyse its strengths and weaknesses in this domain and review its research, development and education initiatives to ensure the availability of effective and trustworthy security tools for everyone and training developers able to design privacy-protecting systems. The EDPS fosters exchanges on this subject with relevant stakeholders[67].

IV. CONCLUDING REMARKS

79. The EDPS welcomes the measures considered by the Commission, but highlights that the revealed surveillance activities of US intelligence agencies not only affect trust in EU-US data flows. They also have an impact on the existing and enforceable rights of EU citizens to respect for privacy and to the protection of their personal data. These rights are enshrined in both EU and Council of Europe primary and secondary law. Therefore, the EDPS regrets that the Communication on rebuilding trust has not given more attention to the impact on existing legal instruments.

80. The EDPS would favour on several points that the Commission be more ambitious when defining the next steps to be taken and finds that:

- A correct application and enforcement of the current European data protection legal framework is not only required by law, but would also be an essential contribution to restoring trust. This also applies to the instruments regulating international transfers between the EU and the US, including the existing Safe Harbour principles.

- The Commission should recall that exceptions or restrictions to fundamental rights allowed for national security purposes are only justified and permissible if they are strictly necessary, proportionate and in line with the jurisprudence of the ECtHR and the Court of Justice.

- The EDPS entirely agrees that consolidation and improvement of the EU data protection framework requires a swift adoption of the data protection reform proposals with adequate substance so as to provide for stronger, more effective and more consistent protection of personal data and privacy within the full scope of EU law. This should also provide for adequate protection of data in the case of their further use for law enforcement purposes and international conflicts of jurisdictions.

[66] Vancouver IETF, https://www.ietf.org/media/2013-11-07-internet-privacy-and-security.html;
[67] https://www.w3.org/2014/strint/papers/64.pdf

- The Safe Harbour principles should be reviewed and strengthened along the lines indicated by the Commission. The EDPS recommends setting up stricter deadlines within which these actions must be taken, including adequate follow up in case of any remaining deficiencies.

- Data protection safeguards applying to EU-US law enforcement cooperation have to be reinforced. Current negotiations on an "umbrella agreement" should not legitimise massive data transfers of data but comply with the existing data protection framework and with the outcome of its current review process. In particular, effective redress mechanisms should be accessible to all data subjects, regardless of their nationality. This should in due course also apply to existing international agreements, where necessary on the basis of appropriate transition clauses.

- The Commission should support efforts by the US Administration and US Congress to enact a general privacy act, providing for strong safeguards and adequate oversight, in particular in areas where any substantial protection of privacy is currently lacking.

- The negotiations currently taking place to adopt a TTIP should not have an adverse impact on the protection of personal data of citizens. At the same time, the Commission should consider setting a common goal of gradual development towards greater interoperability of legal frameworks for privacy and data protection, to which goal the US might contribute as just mentioned above.

- The international promotion of privacy standards should include:
  i. promoting full consistency of new international instruments with the European data protection framework;
  ii. promoting the adhesion of third countries, and in particular the US, to Council of Europe Convention 108;
  iii. supporting the adoption of an international instrument requiring the respect of data protection standards by intelligence activities. This could be adopted at UN level on the basis of Article 17 of the ICCPR.

- Surveillance activities should at all times be obliged to respect the rule of law and the principles of necessity and proportionality in a democratic society. Legal frameworks at all relevant levels should therefore be clarified and where necessary supplemented. These frameworks should include appropriate and sufficiently strong oversight mechanisms.

- EU institutions and all relevant entities in the Member States are, as data controllers, also directly responsible for ensuring effective IT security. This involves carrying out a data security risk assessment at the appropriate level. It also requires encouraging research on encryption mechanisms and raising data controllers and citizens' awareness on privacy risks of the products sold or used, and requiring that developers use concrete design methods to avoid or, at least, reduce these risks. The EU should lead education initiatives on security of data processed on the Internet.

Done in Brussels, 20 February 2014

(**signed**)

Peter HUSTINX
European Data Protection Supervisor