EUROPEAN DATA PROTECTION SUPERVISOR

Executive Summary of the 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 full text of this Opinion can be found in English, French and German on the EDPS website (www.edps.europa.eu))

(2014/C 116/04)

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' ([1]) (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 from the Perspective of EU Citizens and Companies Established in the EU' ([2]) (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 ([3]), how the collection and further processing of data takes place ([4]) and the existing oversight and redress mechanisms.

([1]) COM(2013) 846 final.

([2]) COM(2013) 847 final.

([3]) 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.

([4]) 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.

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

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 ([1]) 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.

([1]) 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 ([1]) 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 ([2]), as interpreted by the US Supreme Court ([3]). The report also confirms the lack of safeguards, protections, rights, oversight and redress possibilities available for EU citizens under the US framework ([4]).

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 ([5]) 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 ([6]). 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.

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.

([1]) 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'.

([2]) 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).

([3]) See p. 4-12 of the Report.

([4]) See p. 26-27 of the Report.

([5]) '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

([6]) 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

— 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.

— 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 at Brussels, 20 February 2014.

Peter HUSTINX

European Data Protection Supervisor