Opinion of the European Data Protection Supervisor

on the Communication from the Commission to the European Parliament and the Council - "The EU Counter-Terrorism Policy: main achievements and future challenges"

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1],

Having regard to 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 its Article 41,

HAS ADOPTED THE FOLLOWING OPINION

I. Introduction

1. On 20 July 2010, the Commission adopted a Communication entitled "The EU Counter-Terrorism Policy: main achievements and future challenges"[3]. The Communication aims at providing "*the core elements of a political assessment of the current EU Counter Terrorism Strategy*", and constitutes also an element of the Internal Security Strategy[4]. It assesses past achievements and draws future challenges and policy lines for the EU Counter-Terrorism Policy.

2. Many of the initiatives mentioned in the Communication have been already subject of specific EDPS opinions or comments. However, this Communication presents a broad policy perspective and long-term orientations that justify a dedicated EDPS opinion.

1 OJ 1995, L 281/31.
2 OJ 2001, L 8/1.
3 COM (2010) 386 final
4 See page 2 of the Communication.

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

3. This opinion thus aims at contributing to more fundamental policy choices in an area where the use of personal information is at the same time crucial, massive and particularly sensitive.

4. The opinion does not comment on the most recent Communication of the Commission in this area 'The EU Internal Security Strategy in Action: Five steps towards a more secure Europe", adopted on 22 November 2010.[5] This Communication will be analyzed by the EDPS in a separate opinion which will also address again the need for clear links between the different documents.

5. In this opinion, the EDPS analyzes the different elements of the Communication, while providing advice and recommendations in order to ensure the fundamental right to the protection of personal data in the area of EU Counter-Terrorism Policy, especially when addressing future challenges and developing new policy orientations.

II. Analysis of the Communication and relevant data protection issues

6. By building on the structure of the 2005 EU Counter-Terrorism Strategy[6], the Communication first analyzes the four major strands of EU Counter-Terrorism Policy: prevent, protect, pursue and respond. A specific chapter then addresses some horizontal issues, namely the respect of fundamental rights, international cooperation and funding.

II.1. Prevent, Protect, Pursue, Respond and the need to embed data protection principles

7. "Prevent" encompasses a broad number of activities, ranging from preventing radicalisation and recruitment to dealing with the way terrorists use the internet. In this context the Communication reports among the main achievements the Council Framework Decision on combating terrorism, adopted in 2002[7] and amended in 2008[8].

8. "Protecting" people and infrastructure is also a very broad subject, including initiatives on border security, transport security, control of explosive precursors, protection of critical infrastructure and strengthening of the supply chain.

9. "Pursue" includes information gathering, police and judicial cooperation and combating terrorist activities and financing. Future challenges in this sector are the establishment of an EU PNR framework[9], the use of Article 75 TFEU to develop a framework for freezing of funds and financial assets, as well as mutual recognition in obtaining evidence in criminal matters.

---

5 COM (2010) 673 final

6 Doc. 14469/4/05 of 30 November 2005.

7 2002/475/JHA, OJ L 164, 22.6.2002, p.3.

8 2008/919/JHA, OJ L 330, 9.12.2008, p.21.

9 As also announced in the Commission Action Plan Implementing the Stockholm Programme COM(2010) 171 final of 20.04.2010.

10. "Respond" refers to the capacity of dealing with the aftermath of terrorist attack, and includes assistance to victims of terrorism.

11. All these areas present strong links with initiatives on which the EDPS has already taken position: the Stockholm Programme, restrictive measures and asset freezing, data retention, security scanners, weapons precursors, biometrics, the Prüm Decision, Passengers Name Records, the TFTP agreement, the Schengen Information System, the Visa Information System, integrated border management, the EU Information Management Strategy and the cross-border exchange of evidence.

12. The areas of "prevention" and "protection" are the most delicate ones from a data protection perspective, for various reasons.

13. Firstly, these areas are by definition based on prospective risk assessments, which in most cases trigger a broad and "preventive" processing of vast amounts of personal information on non-suspected citizens (such as, for example, internet screening, e-borders and security scanners).

14. Secondly, the Communication envisages increasing partnerships between law enforcement authorities and private companies (such as internet service providers, financial institutions and transportation companies) with a view to exchange relevant information and sometimes to "delegate" to them certain parts of law enforcement tasks. This entails an increased use of personal data, collected by private companies for commercial purposes, for the use by public authorities for law enforcement purposes.

15. Many of these initiatives were taken, often as a fast response to terrorist incidents, without a thorough consideration of possible duplications or overlapping with already existing measures. In some cases, even a few years after their entry into force, it is not yet established to which extent the invasion of citizens' privacy ensuing from these measures was in all cases really necessary.

16. Furthermore, "preventive" use of personal data is more likely to lead to discrimination. The preventive analysis of information would entail the collection and processing of personal data relating to broad categories of individuals (for example, all passengers, all internet users) irrespective of any specific suspicion about them. The analysis of these data - especially if coupled with data-mining techniques - may result in innocent people being flagged as suspects only because their profile (age, sex, religion, etc.) and/or patterns (for example, in travelling, in using internet, etc) match those of people connected with terrorism or suspected to be connected. Therefore, especially in this context, an unlawful or inaccurate use of (sometimes sensitive) personal information, coupled with broad coercive powers of law enforcement authorities, may lead to discrimination and stigmatization of specific persons and/or groups of people.

17. In this perspective, ensuring a high level of data protection is also a means contributing to fighting racism, xenophobia and discrimination, which, according to the Communication, "*can also contribute to preventing radicalisation and recruitment into terrorism*".

II.2. A consistent approach based on the principle of necessity

18. An important general remark concerns the need to ensure consistency and clear relations between all Communications and initiatives in the area of home affairs, and in particular within the area of Internal Security. For example, even though the EU counter-terrorism strategy is closely linked with the Information Management Strategy, the Strategy on the Charter of Fundamental Rights and the European Information Exchange Model, the relations between all these documents are not explicitly and comprehensively addressed. This became even more obvious with the adoption on 22 November 2010 of 'The EU Internal Security Strategy in Action: Five steps towards a more secure Europe[10]'.

19. The EDPS therefore recommends the EU institutions to ensure that policies and initiatives in the area of home affairs and internal security are designed and implemented in a way which will ensure a consistent approach and clear links between them, providing for appropriate and positive synergies, and avoiding duplication of work and efforts.

20. The EDPS recommends furthermore that the principle of necessity is explicitly considered in each proposal in this area. This should be done both by considering possible overlaps with already existing instruments and by limiting the collection and exchange of personal data to what is really necessary for the purposes pursued.

21. For example, in the case of the Terrorist Finance Tracking Program (TFTP II) Agreement with the US, the EDPS questioned to which extent the agreement was really necessary in order to obtain results that could be obtained by using less privacy-intrusive instruments, such as those already laid down by the existing EU and international framework[11]. In the same opinion, the EDPS questioned the necessity of sending personal data in bulk, rather than in a more targeted fashion.

22. The Communication mentions as one of the challenges "*to ensure that these instruments cover the real needs* [of law enforcement] *while ensuring full respect for the right to privacy and data protection rules*". The EDPS welcomes this explicit recognition and calls for EU institutions to carefully assess to which extent the instruments already in place as well as the envisaged ones cover the real needs of law enforcement, while avoiding overlaps of measures, or unnecessary restrictions to the private life. In this perspective, existing instruments should prove in periodic reviews that they constitute effective means of fighting terrorism.

23. The EDPS has advocated the need for assessment of all existing instruments on information exchange before proposing new ones in numerous opinions and comments, and with particular emphasis in the recent opinion on the "Overview of information management in the area of freedom, security and justice"[12]. Indeed, assessing the effectiveness of existing measures while considering the impact on privacy of new envisaged measures is crucial and should vest an important role in European Union's action in this area, in line with the approach put forward by the Stockholm Programme.

---

10 See para 4 of this opinion.

11 EDPS Opinion of 22 June 2010.

12 EDPS Opinion of 30 September 2010.

24. Overlaps and lack of effectiveness should lead to adjustments in policy choices or even to consolidating or dismissing existing data collection and processing systems.

25. The EDPS recommends that special attention be paid to those proposals resulting in general collections of personal data of all citizens, rather than only suspects. Specific consideration and justification should also be given to those cases where processing of personal data is foreseen for purposes other than those for which they were initially collected, such as for example in the case of access for law enforcement purposes of personal data stored in the Eurodac system.

.

26. The Communication also highlights that one of the future challenges will be to ensure an effective security research policy, which would contribute to a high level of security. The EDPS supports the Communication's statement that an effective security research should strengthen the links between different actors. In this perspective, it is crucial that data protection expertise is fed into the security research at a very early stage, so as to guide policy options and to ensure that privacy is embedded to the fullest possible extent in new security-oriented technologies, according to the principle of "privacy by design".

II.3. With regard to the use of restrictive (asset-freezing) measures

27. With regard to the use of restrictive (asset-freezing) measures towards specific countries and suspected terrorists, the case law of the Court of Justice has repeatedly and consistently confirmed that the respect of fundamental rights in the fight against terrorism is crucial, with a view to ensuring both respect of citizens' rights and lawfulness of the measures taken.

28. The EDPS has already contributed with opinions and comments in this area[13], on the one hand highlighting the improvements made in the procedures, but on the other hand requesting further improvements, especially with regard to the right of information and of access to personal data, the clear definition of restrictions to these rights, and the availability of effective judicial remedies and independent supervision.

29. The need for further improvements of the procedure and the safeguards available to listed individuals has been recently confirmed by the General Court in the so-called "Kadi II" case[14]. In particular, the Court highlighted the necessity that the listed person should be informed in details about the reasons for being listed. This comes very close to the rights, under data protection law, to have access to one's own personal data and to have them rectified, notably when they are incorrect or out of date. These rights, explicitly mentioned by Article 8 of the

[13] Opinion of 28 July 2009 on the proposal for a Council Regulation amending Regulation (EC) No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, OJ C 276, 17.11.2009, p. 1. Opinion of 16 December 2009 on various legislative proposals imposing certain specific restrictive measures in respect of Somalia, Zimbabwe, the Democratic Republic of Korea and Guinea, OJ C 73, 23.03.2010, p.1. See also the EDPS letter of 20 July 2010 on three legislative proposals concerning certain restrictive measures, namely with regard to Mr Milosevic and persons associated with him, in support of the mandate of the International Tribunal for the Former Yugoslavia, and in respect of Eritrea. All EDPS opinions and comments are available on the EDPS website www.edps.europa.eu.

[14] Judgment of 30 September in case T-85/09 *Kadi v. Commission*, see in particular paras.157, 177.

Charter of Fundamental Rights, constitute core elements of data protection, and may be subject to limitations only to the extent these limitations are necessary, foreseeable and laid down by law.

30. In this perspective, the EDPS agrees with the Communication that one of the future challenges in the area of counter-terrorism policy will be the use of Article 75 TFEU. This new legal basis, introduced by the Lisbon Treaty, specifically allows establishing asset-freezing measures against natural or legal persons. The EDPS recommends that this legal basis be used also to lay down a framework for asset freezing which is fully compliant with the respect of fundamental rights. The EDPS is available to further contribute to the development of relevant legislative instruments and procedures, and looks forward to being duly and timely consulted when the Commission - pursuant to its 2011 Work Programme - will develop a specific regulation in this area[15].

31. In a broader perspective, there is a need to establish a data protection framework applicable also to the Common Foreign and Security Policy. Indeed, Article 16 TFEU provides a legal basis for establishing data protection rules also in the area of Common Foreign and Security Policy. The different legal basis and procedure laid down by Article 39 TEU will apply only when personal data are processed in this area by the Member States. However, even if the Lisbon Treaty calls for these data protection rules and provides the tools to establish them, for the moment no initiative is foreseen in the recent Communication on "A comprehensive approach on personal data protection in the European Union"[16] Against this background, the EDPS urges the Commission to present a proposal for the establishment of a data protection framework in the Area of Common Foreign and Security Policy.

II.4. Respect for Fundamental Rights and International Cooperation

32. The chapter dedicated to the respect of fundamental rights, highlights that the EU should be exemplary in the respect of Charter of Fundamental Rights, which should be the compass for all EU policies. The EDPS welcomes this approach.

33. The EDPS also supports the statement that respect of fundamental rights is not only a legal requirement, but also a key condition for promoting mutual confidence between national authorities and trust among the public at large.

34. Against this background, the EDPS recommends a proactive approach and concrete actions in making this happen, also as a means to effectively implement the EU Charter of Fundamental Rights.[17]

35. Privacy Impact Assessments (PIAs) and early consultation of competent data protection authorities should be ensured for all initiatives having an impact on the protection of personal data, irrespective of their initiator and of the area in which they are proposed.

---

15 The Commission Work Programme 2011 (COM(2010)623 of 27.10.2010) mentions in its. Annex II (Indicative list of possible initiatives under consideration) a "Regulation establishing a procedure for the freezing of funds of persons suspected of terrorist activities inside the EU".

16 Commission Communication (2010)609 of 4 November 2010.

17 See Commission Communication (2010)573 of 19.102010 on a Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union.

36. In its chapter on international cooperation, the Communication also highlights the need to create "*the necessary legal and political framework conditions for enhanced cooperation with the EU's external partners in the field of combating terrorism*".

37. In this respect, the EDPS reminds of the need to ensure that adequate safeguards are put in place when personal data are exchanged with third countries and international organisations, in order to ensure that citizens' data protection rights are adequately respected also in the context of international cooperation.

38. This also includes promoting data protection in cooperation with third countries and international organizations, in order to ensure that EU standards are met. This is also in line with the Commission's intention to develop high legal and technical standards of data protection in third countries and at international level, and enhancing cooperation with third countries[18].

39. A clear opportunity for the European Union's action in this area is provided by the (asset-freezing) restrictive measures, where intense cooperation with third countries and United Nations should not reduce the high level of protection of fundamental rights provided by the EU legal system.

III. Conclusions

40. The EDPS welcomes the attention that the Communication pays to fundamental rights and data protection, and recommends further concrete improvements in the area of counter-terrorism policy.

41. The EDPS recommends supporting with concrete initiatives the respect of fundamental rights in this area, and in particular of the right to the protection of personal data which is a necessary ally to promote legal certainty, trust and cooperation in the fight against terrorism, as well as a necessary legal condition for the development of the envisaged systems.

42. The EDPS also supports the approach that systematic policy making in this area should be preferred to incident-driven policy-making, especially when incidents lead to the creation of new systems of data storage, collection and exchange without a proper assessment of existing alternatives.

43. In this perspective, the EDPS recommends the EU institutions to ensure that policies and initiatives in the area of home affairs and internal security are designed and implemented in a way which will ensure a consistent approach and clear links between them, providing for appropriate and positive synergies, and avoiding duplication of work and efforts.

44. Against this background, EDPS recommends the EU legislator to step up the role of data protection, by committing to specific actions (and deadlines), such as:

[18] See Communication (2010)609 on "A comprehensive approach on personal data protection in the European Union", pages 16-17.

- Assessing the effectiveness of existing measures while considering their impact on privacy is crucial and should vest an important role in European Union's action in this area;

- When envisaging new measures, considering possible overlapping with already existing instruments, taking into account their effectiveness, and limiting the collection and exchange of personal data to what is really necessary for the purposes pursued;

- Proposing the establishment of a data protection framework applicable also to the Common Foreign and Security Policy;

- Proposing a comprehensive and global approach to ensuring, in the area of (asset-freezing) restrictive measures, both the effectiveness of the law enforcement action and the respect for fundamental rights, on the basis of Article 75 TFEU;

- Putting data protection at the heart of the debate of the measures in this area, by ensuring for example that Privacy and Data Protection Impact Assessments are carried out and competent data protection authorities are timely consulted when relevant proposals in this area are put forward;

- Ensuring that data protection expertise is fed into the security research at a very early stage, so as to guide policy options and to ensure that privacy is embedded to the fullest possible extent in new security-oriented technologies;

- Ensuring adequate safeguards when personal data are processed in the context of international cooperation, while promoting the development and implementation of data protection principles by third countries and international organisations.

Done at Brussels, 24 November 2010

(**signed**)

Peter HUSTINX
European Data Protection Supervisor