Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council entitled 'Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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

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

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular Article 28 (2) thereof,[2]

Having regard to Council Framework Decision 2008/977/JHA of 27 November 2008[3] on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 7 December 2012, the Commission adopted a Communication entitled 'Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM) (hereinafter: 'the Communication').[4] On the same day the Commission adopted a report on the implementation of Council Decision

[1] OJ L281, 23.11.1995, p. 31.
[2] OJ L8, 12.1.2001, p. 1.
[3] OJ L350, 30.12.2008, p. 60.
[4] COM(2012)735 final.

2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (the 'Prüm Decision').[5] This report will not be separately commented in this opinion, but is mentioned here in order to better understand the context.

2. Before the adoption of the Communication, the EDPS was given the opportunity to provide informal comments. The EDPS welcomes that some of his comments have been taken into account in the Communication.

1.2. Background and objectives of the Communication

3. The Stockholm Programme[6] aims at meeting future challenges and further strengthening the area of freedom, security and justice with actions focusing on the interests and needs of citizens. It establishes the EU's priorities in the field of Justice and Home Affairs for the period of 2010-2014 and defines strategic guidelines for legislative and operational planning within the area of freedom, security and justice in accordance with Article 68 of the Treaty on the Functioning of the European Union ('TFEU')[7].

4. In particular, the Stockholm Programme acknowledges the need for coherence and consolidation in developing information management and exchange in the field of EU internal security and invites the Council and the Commission to implement the Information Management Strategy for EU internal security, including a strong data protection regime. In this context, the Stockholm Programme also invites the Commission to assess the need for a European Information Exchange Model (EIXM) based on evaluation of existing instruments in the field of EU information exchange. This assessment should help to determine whether these instruments function as originally intended and meet the goals of the Information Management Strategy[8].

5. Following-up the Stockholm Programme, the Commission published a Communication in July 2010[9] (hereafter the 'Communication of 2010') which provides a full overview of the EU-level measures in place, under implementation or consideration, that regulate the collection, storage or cross-border exchange of personal information for the purpose of law enforcement and migration management.

6. Answering the invitation of the Stockholm Programme and building on the Communication of 2010, the present Communication aims to take stock of how the cross-border information exchange in the EU works in practice and to recommend possible improvements.

---

[5] COM(2012)732 final

[6] The Stockholm Programme - An open and secure Europe serving and protecting citizens, Council Document 5731/10, 3.3.2010.

[7] Treaty on the Functioning of the European Union, OJ C 83/47, 30.03.2010.

[8] The Stockholm Programme - An open and secure Europe serving and protecting citizens, Council Document 5731/10, 3.3.2010, section 4.2.2

[9] Communication of 20 July 2010 from the Commission to the European Parliament and the Council entitled 'Overview of information management in the area of freedom, security and justice', COM(2010) 385 final.

2. COMMENTS

2.1. General comments

Need for better information exchange whilst respecting fundamental rights

7. As already pointed out in previous opinions[10], the EDPS acknowledges that a better exchange of information is an essential policy goal for the European Union in the area of freedom, security and justice. This emphasis on information exchange is even more logical in the absence of a European police force, a European criminal justice system and a totally harmonised European border control. Measures relating to information are therefore an essential contribution of the European Union allowing the national authorities of the Member States to address cross border crime in an effective way and to effectively protect the external borders.

8. However, these measures should not only contribute to guaranteeing the security of the citizen, but within our European society they also have to fully respect the citizen's fundamental rights including the right to the protection of personal data. This is all the more important as exchange of information in the area of police and judicial cooperation in criminal matters involves to a large extent personal data. The processing of personal data in this area poses specific risks for the individuals and therefore requires a high level of data protection.

9. The EDPS appreciates the general attention paid to data protection in the Communication. He welcomes that the Communication refers to the substantive principles of (i) safeguarding fundamental rights - in particular the right to privacy and protection of personal data - and (ii) the necessity requirement which implies that a restriction of the right to privacy may be justified only if it is lawful, pursues a legitimate aim and is necessary in a democratic society. The Communication also recalls that necessity tests and purpose limitation are essential.[11]

10. The EDPS also positively notes that the Communication emphasises the need to ensure high data quality, data security and data protection and stresses that "whatever combination or sequence is used for exchanging information, the rules on data protection, data security and data quality as well as the purpose for which the instruments may be used must be respected".[12]

The context of instruments already available

11. The Communication states at the outset that information exchange generally works well, adding that neither new EU-level law enforcement databases nor new EU information exchange instruments are needed, but existing instruments should be better implemented. The EDPS welcomes this conclusion. Considering that a

[10] See for instance EDPS Opinion of 10 July 2009 on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen, OJ C 276, 17.11.2009, p. 8 and EDPS Opinion of 7 October 2009 on the proposals regarding law enforcement access to EURODAC, OJ C 92, 10.04.2010, p. 1.
[11] See point 2.5 of the Communication.
[12] See point 2.3 of the Communication

multiplicity of systems for the cross-border exchange of information carries risks in terms of personal data protection and invasion of privacy, the EDPS has in various opinions advocated that before creating a new instrument, a thorough and more up-to-date evaluation should be carried out in order to see whether a full implementation of the existing instruments would not be sufficient.[13]

12. The Communication mainly focuses on Member State's use of four EU instruments: the Swedish initiative[14], the Prüm Decisions[15], Europol[16] and the Schengen Information System[17]. It does not address all existing and envisaged EU instruments for police and judicial cooperation in criminal matters and does not mention for instance the existing European Criminal Record Information System for EU nationals.[18] Furthermore although the Communication mentions other EU instruments in the area of freedom, security and justice (e.g. Customs information System, Visa Information System, EURODAC, EUROSUR) or initiatives (e.g. the proposals for an Entry-Exit System), it does not analyse them.

13. Finally, the EDPS draws the attention to the fact that also legal instruments in other areas than the area of freedom, security and justice should be taken into consideration, since they become more and more relevant (see the instruments meant in point 16).

Tendencies in investigative methods

14. New technologies have lead to an increasing amount of available information and a wide range of possible uses of this information. In an information society there is the logical tendency that law enforcement authorities increasingly make use of information available in open sources, and combine this information using

[13] See for instance EDPS Opinion of 5 September 2012 on law enforcement access to EURODAC, EDPS Opinion of 30 September 2010 on the Communication from the Commission to the European Parliament and the Council – 'Overview of information management in the area of freedom, security and justice', EDPS Opinion of 24 November 2010 on the Communication from the Commission to the European Parliament and the Council concerning the EU Counter-Terrorism Policy: main achievements and future challenges, EDPS Opinion of 20 December 2007 on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, and EDPS Opinion of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information System (SIS II).

[14] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89

[15] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L210, 06.08.2008, p. 1 and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 06.08.2008, p. 12.

[16] Council Decision 2009/371/JHA establishing the European Police Office, OJ L 121, 15.05.2009, p. 37.

[17] Council Decision 2007/533/JHAof 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ 205, 07.08.2007 p. 63.

[18] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States , OJ L 93, 07.04.2009,p. 23, and Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA , OJ L 93 , 07.04.2009 p. 33.

sophisticated IT tools. Technological phenomena like cloud computing, social networks, road toll collecting and geo-location devices as well as the linking and sharing of data from different databases or the use of analytical tools to predict human behaviours have profoundly changed the way in which data may be collected and further processed. Working methods of law enforcement authorities such as data mining and profiling are becoming more and more proactive and investigations take place on the basis of general developments, sometimes without concrete suspicions, but with the use of powerful IT-tools.

15. There is a general and growing tendency to grant law enforcement authorities access to available data which were, are or will be initially collected and processed for purposes that are not related to the combat of crimes and which concern individuals who in principle are not suspected of committing any crime. Wider access is more often given or envisaged for law enforcement authorities to several large-scale information and identification systems set up for example in the areas of immigration and borders control[19].

16. Traditionally, a clear separation has existed between law enforcement and private sector activities, where law enforcement tasks are performed by specifically dedicated authorities and private actors are only solicited on a case by case basis to communicate personal data to these authorities in the event of concrete suspicion. There is now a tendency to require that private actors cooperate with law enforcement authorities on a systematic basis. This tendency relates for instance to the traffic data of electronic communications[20] and the passenger data of individuals flying to (certain) third countries[21], and is also developing in the financial sector[22].

---

[19] See for instance Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218,13.08.2008, p. 129; the Amended proposal of the Commission for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version), COM (2012) 254 final, 30.05.2012 and the proposal of the Commission for a Regulation of the European Parliament and of the Council establishing an Entry/Exit system (EES) to register any entry and exit of third country nationals crossing the external borders of the Member States of the European Union, COM(2013) 95 final, 28.02.2013.

[20] Directive 2006/24/CE of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.04.2006, p.54.

[21] See Council Decision 2012/472/EU of 26 April 2012 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, OJ L 215, 11.08.2012, p.4.

[22] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing OJ L 309, 25.11.2005, p. 15 (currently under review). See also the Communication of 13.July 2011 from the Commission to the European parliament and the Council entitled 'A European terrorist finance tracking system: available options', COM(2011)429 final.

17. The availability of an increasing amount of information outside the law enforcement area as well as the use of new powerful IT tools by law enforcement authorities contribute - to a certain extent - to the current ongoing shift from a surveillance of individuals that are suspected of having committed or having taken part in a criminal offence or regarding whom there are reasonable grounds based on factual indications that they will commit criminal offences to a more general surveillance where all individuals may be considered *a priori* as potential law breakers, and for that reason subjected to surveillance.

Consequences

18. Because of these far reaching developments there is a need to rethink and possibly redefine the right balance between law enforcement purposes and safeguarding fundamental rights of the individuals. It is for instance worth noting that when information is gathered through surveillance methods outside of a concrete criminal case, also the context of fundamental rights protection changes. One could argue that when there is no case before a court, the principle of fair trial (Article 6 of the European Convention of Human Rights) cannot be applied and that therefore data protection and privacy considerations should gain importance.

19. This implies in the first place a reflection on the effectiveness of data protection principles in light of technological changes as well as the growing gathering and use of data for law enforcement purposes. This may lead to adjustments and/or additional safeguards.

20. In the second place, there is indeed nowadays, more than ever before, a clear need for an in-depth reflection on EU information exchange, in view of developments relating to IT large-scale systems and the growing use of data initially collected for purposes not related to the combat of crime. This reflection should also address the effectiveness for public security of the current trend to a widespread, systematic and proactive monitoring of non suspected individuals and its actual usefulness in the fight against crime.

21. The EDPS welcomes the Communication as a first step towards a full evaluation process and encourages the Commission to carry out the above further reflections, the outcome of which should lead to a comprehensive, integrated and well-structured EU policy on information and exchange management in this area.

The relation with the existing and the proposed data protection framework

22. The EDPS notes that it is crucial to ensure a consistent and comprehensive legal framework for data protection. A first important step has been taken through the adoption of Council Framework Decision 2008/977/JHA[23]. However, this legal instrument cannot be qualified as a comprehensive framework, in essence because its provisions do not have general application. They do not apply to domestic situations, when personal data originate from the Member State which uses

[23] 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. 60.

them[24]. Secondly, the other data protection instruments applicable in the area of freedom, security and justice should be further harmonised and consolidated.

23. The EDPS would like to stress that the ongoing discussions on the Commission's proposal of 25 January 2012 for a Directive applying to the processing of personal data for law enforcement purposes[25]should not prevent the Commission from - already now - making an inventory of data protection problems and risks, and of possible improvements within the current legal context. To the contrary, the discussions on the proposed directive could serve as an inspiration for further developing the European Information Exchange Model. Good examples in this context are the discussions on clear distinctions as to processing of data on suspects and non suspects. The EDPS recommends further analysing these notions in the context of the European Information Exchange Model.

24. The EDPS notes that the Communication refers to the Commission proposal for a Directive. In particular, the Communication mentions the need of reviewing existing instruments to align them with the proposed Directive. The EDPS fully subscribes to this intention and encourages the Commission to take further action in this direction.

2.2. Specific comments

Assessment of instruments

25. The Communication gives examples of success stories on exchange of information under the Swedish Initiative and the Prüm Decisions while stressing at the same time that implementation of the Prüm Decision is seriously lagging behind and that the Swedish initiative has not reached its full potential. As regards the SIS and SIRENE channels, the Communication mentions that it does not present recommendations because extensive changes are already underway, in particular the migration to SIS II.[26]

26. As mentioned in the Communication, the first outcomes of the exchange of information based on the Swedish initiative and Prüm Decisions are positive in the context of law enforcement. However, the EDPS wishes to point out that a comprehensive assessment of these instruments (including where appropriate failures and weaknesses of the systems such as the number of people wrongly arrested or inconvenienced following a false hit in the system) can only happen once they are fully implemented. He encourages the Commission to pursue the assessment of these instruments during and after their full implementation.

[24] See also EDPS opinion of 19 December 2005 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM (2005)475 final), OJ C 47, 25.02.2006, p. 27

[25] Proposal of 25 January 2012 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.

[26] See on this the announcement by the Commission on 9 April 2013: 'SIS II goes live' : http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130409_01_en.htm

Choice of channels

27. In its Communication, the Commission states that apart from legal requirements to use specific channels, Member States use different channels to different extents. Although nothing in the Communication seems to indicate that the use of different channels raises particular concerns, the Commission concludes that the time has come for a more coherent approach, which gives Europol a central role. In this respect, the Communication invites the Member States to use, for exchanges where the channel is not legally defined, the Europol channel using the SIENA tool as the default channel, unless there are specific reasons to use another.

28. The EDPS supports the need for a consistent and harmonised approach on the choice of channels. However, as regards the use of one of the channels as default channel, he recalls the principle of purpose limitation which is a key principle of data protection. As pointed out in the Communication, there is a diversity of instruments, channels and tools, each designed for particular purposes. The use of a channel designed for a specific purpose should not lead to the possible use or collection of the data transiting on this channel for other purposes. This poses the risk of what is often described as 'function creep', namely, a gradual widening of the use of a system or database beyond the purpose for which it was originally intended. Furthermore, the use of a channel has also a direct impact on the responsibilities in terms of data protection and security of the authority/agency managing the channel. The EDPS regrets that the Communication does not underline these consequences, and recommends that the guidance which the Council is invited to give takes these perspectives into account.

29. Finally, the EDPS draws attention to the fact that mechanisms that are designed for information exchange for a specific purpose are not necessarily appropriate to other purposes. The communication tool SIENA developed by Europol has been tailored for specific exchange of information between the competent authorities of Member States and third parties for police cooperation. Thus specific functionalities of SIENA have been developed and implemented based on the needs identified at the moment of the creation of such tool. These functionalities require amongst others the users to enter certain types and amount of information. The EDPS points out that SIENA's functionalities are not necessarily appropriate for the exchange of information in a different context and for different purposes. Therefore, in this specific case, he encourages the Commission to justify more clearly the choice of this channel, and to assess whether this choice is in compliance with the principle of privacy by design.

Managing the channels - SPOC

30. The Communication invites the Member States to create – or use, if already existing - a Single Point of Contact (SPOC) as a ‘one-stop shop’ for international cooperation covering all main channels, available 24/7, bringing together all law enforcement authorities with access to all relevant national databases. Given the existence of different units dealing with different parts of police cooperation on national level, the EDPS understands that the accessibility via one single point of contact will help the requesting country as it would not have to address the different authorities and contacts in the requested country.

31. The creation of SPOCs may present advantages since it facilitates the overview of the cross-border information flow and it allows a further recording of actors directly involved. However, the creation of SPOCs should take into account data protection implications. All databases have been created for defined purposes and are subject to specific rules. A database may only be accessed by duly authorised staff in the performance of their tasks and for the purposes for which the database has been created. Therefore, the composition and the modalities of SPOCs should be carefully analysed and defined in order to ensure that the rules applicable to each database are complied with.

32. In the absence of harmonised conditions for SPOCs there might be cases where entities represented in SPOCs will not be authorised to directly access the database but will facilitate the access and ensure that the requested information is communicated to the requested authority from another Member State. The EDPS notes that the Communication specifies that SPOCS should have direct access to national databases where legally permissible. The EDPS notes with satisfaction that the Communication recalls that information may only be actually exchanged and used where legally permitted, which includes compliance with data protection rules. However, he invites the Commission to start working on harmonised conditions for SPOCs, to ensure that the requirements are similar in all Member States and effectively protect individuals.

Ensuring data quality, data security and data protection

33. As to the interoperability between different national systems and administrative structures referred to in the Communication, the EDPS stresses the need to consider the protection of personal data as an inherent part of the establishment - or improvement - of the interoperability of relevant systems.

34. As already underlined in earlier comments and opinions[27], making access to or exchange of data technically feasible becomes, in many cases, a powerful drive for de facto acceding or exchanging these data. Although the introduction of interoperability will not lead to new databases, it will necessarily introduce a new use of existing databases by providing new possibilities of access to those databases.

35. In that respect, the EDPS would like to point at the basic data protection principle of purpose limitation, which requires that personal data may not be used for purposes which are incompatible with the purpose for which the data were originally collected, unless this would be specifically allowed under certain strict conditions.

[27] See EDPS Opinion of 26 February 2006 on Exchange of information under the principle of availability; EDPS Comments of 10 March 2006 on the Commission's Communication of 24 November 2005 on improved effectiveness of enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, and EDPS Opinion of 7 December 2009 on the Agency for large-scale IT systems.

Improving training and awareness

36. The Communication refers to the preparation by the Commission of a European Law Enforcement Training Scheme that will include training on cross-border exchange information. The EDPS notes the recent adoption of the Commission Communication establishing a European Law Enforcement Training Scheme[28] on which he will come back in his opinion on the proposal for a Regulation on Europol[29]. Taking into account that cross-border information exchange will in a number of cases involve personal data, the EDPS would like to draw attention to the need of including trainings on information security and data protection in the Scheme envisaged by the Commission as well as in the trainings Member States are invited to ensure.

3. CONCLUSIONS

37. The EDPS appreciates the general attention devoted to data protection in the Communication which emphasises the need to ensure high data quality, data security and data protection and recalls that whatever the combination or sequence used for exchanging information, the rules on data protection, data security and data quality as well as the purpose for which the instruments may be used must be respected.

38. The EDPS also:

- welcomes that the Communication concludes that neither new EU-level law enforcement databases nor new EU information exchange instruments are needed;

- emphasizes the need for a full evaluation process of the instruments and initiatives in the Justice and Home Affairs area, the outcome of which should lead to a comprehensive, integrated and well-structured EU policy on information and exchange management and encourages the Commission to pursue the assessment of other existing instruments;

- encourages the Commission to carry out reflections on (i) the effectiveness of data protection principles in light of technological changes, the developments relating to IT large-scale systems and the growing use of data initially collected for purposes not related to the combat of crime, as well as on (ii) the effectiveness for public security of the current tendency to a widespread, systematic and proactive monitoring of non suspected individuals and its real usefulness in the fights against crimes; the outcome of these reflections should lead to a comprehensive, integrated and well-structured EU policy on information and exchange management in this area;

[28] Communication of 27 March 2013 from the Commission to the European Parliament, the Council, the European and economic and Social Committee and the Committee of the Regions entitled 'Establishing a European Law Enforcement Training Scheme', COM(2013) 172 final.
[29] Proposal of 27 March 2013 for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final.

- underlines that the ongoing discussions on the proposal for a Directive should not prevent the Commission from making an inventory of data protection problems and risks, and of possible improvements within the current legal context, and recommends using theses discussions in particular on the distinction on processing of data of suspects and non suspects for further development of the European Information Exchange Model;

- fully subscribes to the need for reviewing existing instruments to align them with the proposed Directive and encourages the Commission to take further action;

- encourages the Commission to pursue the assessment of existing instruments along and after their full implementation;

- recommends that the guidance which the Council is invited to give as regards the choice of channel takes into account the consequences in terms of purpose limitation and responsibilities;

- encourages the Commission to justify more clearly the choice of the Europol channel using the SIENA tools as default channel and to assess whether this choice is in compliance with the principle of privacy by design;

- notes with satisfaction that the Communication recalls that information may only be actually exchanged and used where legally permitted, which includes compliance with data protection rules, and invites the Commission to start working on harmonised conditions for SPOCs, to ensure that the requirements are similar in all Member States and effectively protect individuals;

- recommends including trainings on information security and data protection in the Scheme envisaged by the Commission as well as in the trainings Member States are invited to ensure.

Done in Brussels, 29 April 2013

(**signed**)

Peter HUSTINX
European Data Protection Supervisor