I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the French Republic, the Italian Republic, the Republic of Hungary, the Republic of Poland, the Portuguese Republic, Romania, the Republic of Finland and the Kingdom of Sweden for a Directive of the European Parliament and of the Council on the European Protection Order, and on the initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters

(2010/C 355/01)

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 Article 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, and in particular its Article 41 [2],

Having regard to 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 [3],

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. Increasing efforts to improve judicial cooperation in criminal matters have been made in recent years. This subject, which now occupies a key position in the Stockholm programme [4], is characterised by the particular sensitivity of personal data involved and by the effects that the related data processing may have on data subjects.

2. For these reasons, the European Data Protection Supervisor (EDPS) has paid particular attention to this subject [5] and intends through this opinion to emphasise once more the need for protection of fundamental rights as a cornerstone of the Area of Freedom, Security and Justice (AFSJ) as laid out in the Stockholm programme.

3. This opinion reacts on two initiatives for a Directive of a number of Member States, as foreseen by Article 76 TFEU, namely:

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] OJ L 350, 30.12.2008, p. 60.
[4] European Council, the Stockholm programme — An Open and Secure Europe Serving and Protecting Citizens (2010/C 115/01), Chapter 3, 'Making people's lives easier: A Europe of law and justice' (OJ C 115, 4.5.2010, p. 1); see also EDPS Opinion 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).
[5] The EDPS has adopted in recent years a large number of opinions and comments about initiatives in the area of freedom, security and justice which all can be found on the website of the EDPS.

(a) The initiative of 12 Member States for a Directive of the European Parliament and of the Council on the European Protection Order (EPO initiative), presented in January 2010 ([6]), and

(b) The initiative of seven Member States for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters (EIO initiative), presented in April 2010 ([7]).

4. Advising on these initiatives falls within the remit of the task entrusted to the EDPS in Article 41 of Regulation (EC) No 45/2001 for advising EU institutions and bodies on all matters concerning the processing of personal data. This opinion, therefore, comments upon the initiatives as far as they relate to the processing of personal data. Since no request for advice has been sent to the EDPS, this opinion is issued on his own initiative ([8]).

5. The EDPS recalls that under Article 28(2) of Regulation (EC) No 45/2001 the Commission is obliged to consult the EDPS when it adopts a legislative proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. In case of an initiative of Member States this obligation does not apply *strictu sensu*. However, since the entry into force of the Lisbon Treaty the ordinary legislative procedure also applies to the area of police and judicial cooperation, with one specific exception foreseen in Article 76 TFEU, namely that a quarter of the Member States can take the initiative for EU measures. Under the Lisbon Treaty, these initiatives are aligned as much as possible with Commission proposals and procedural guarantees should be used where possible. It is for this reason that the present initiatives are accompanied by an impact assessment.

6. It is against this background that the EDPS not only regrets that he was not consulted when the initiatives were issued, but also recommends the Council to establish a procedure in which consultation of the EDPS will take place, in case an initiative introduced by Member States is related to the processing of personal data.

7. Although the two initiatives have different objectives — i.e. improving protection of victims and cross-border co-operation in criminal matters through the collection of evidence cross border — they have important similarities:

(a) they are both based on the principle of mutual recognition of judgments and judicial decisions ([9]);

(b) they are rooted in the Stockholm programme ([10]); and

(c) they provide for exchange of personal data between Member States (see points 10 and 13 and Section II.4).

For these reasons, the EDPS considers it appropriate to examine them jointly.

8. In this framework, it should be mentioned that also the European Commission has recently dealt with the issue of collecting evidence with a view to submitting it to the competent authorities in other Member States (which is the specific object of the EIO initiative). Indeed, a Green Paper ([11]) was published at the end of 2009 — whose consultation phase is now closed ([12]) — with the Commission's aim (inferred from the 'Action Plan Implementing the Stockholm programme' ([13])) of submitting a legislative proposal on obtaining a comprehensive regime on evidence in criminal matters based on the principle of mutual recognition and covering all types of evidence in 2011 ([14]).

([6]) OJ C 69, 18.3.2010, p. 5.
([7]) OJ C 165, 24.6.2010, p. 22.
([8]) Also, in the past, the EDPS adopted opinions on initiatives of Member States: see e.g. EDPS Opinion of 4 April 2007 on the initiative of 15 Member States with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ C 169, 21.7.2007, p. 2) and EDPS Opinion of 25 April 2008 on the initiative of 14 Member States with a view to adopting a Council Decision concerning the strengthening of Eurojust and amending Decision 2002/187/JHA (OJ C 310, 5.12.2008, p. 1).

([9]) This principle, introduced in the Vienna Action Plan (Action Plan of the Council and the Commission on How Best to Implement the Provisions of the Treaty of Amsterdam on an Area of Freedom, Security and Justice. Text adopted by the Justice and Home Affairs Council of 3 December 1998, (OJ C 19, 23.1.1999, p. 1, point 45(f))), has been clearly formulated in the Tampere European Council Conclusions of 15 and 16 October 1999, at the points 33, 35–37.
([10]) A third initiative (for a Directive of the European Parliament and of the Council of on the rights to interpretation and to translation in criminal proceedings, 22 January 2010, 2010/0801) has the same origin, but is not taken into account here, as it does not involve issues related to the protection of personal data. On the same topic see also proposal for a Directive of the European Parliament and of the Council on the right to interpretation and translation in criminal proceedings, 9.3.2010, COM(2010) 82 final.
([11]) Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility, COM(2009) 624 final, 11.11.2009.
([12]) The various and sometimes contrasting responses are being considered by the European Commission and can be read at: http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0004_en.htm
([13]) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Delivering an area of freedom, security and justice for Europe's citizens. Action Plan Implementing the Stockholm programme, Brussels, 20.4.2010, COM(2010) 171 final, p. 18.
([14]) It is not clear, for the time being, how a possible future instrument will interrelate with the EIO initiative.

II. JUDICIAL COOPERATION IN CRIMINAL MATTERS AND PERSONAL DATA PROCESSING IN THE FRAMEWORK OF EPO AND EIO INITIATIVES

II.1. Context of the initiatives

9. The aforementioned initiatives fit within the trend of the actions of the EU in the AFSJ in recent years. Since September 2001, there has been a significant escalation in the collection and sharing of information within the European Union (and with third countries), thanks also to developments in ICT and facilitated by a number of legal instruments of the EU. Also the EPO and EIO initiatives are aimed at improving the exchange of information relating to natural persons in the AFSJ.

II.2. EPO initiative

10. The EPO initiative — based on Article 82(1)(d) of the TFEU — focuses on the protection of the victims of criminal acts, particularly women, and aims to guarantee effective protection for them within the European Union. In order to achieve this goal, the EPO initiative permits the extension of protection measures listed in its Article 2(2) and adopted according to the law of one Member State (the issuing State) in another Member State to which the protected person moves (the executing State) without the need for the victim to start new proceedings or to reproduce any evidence in the executing State.

11. The protection measures imposed (at the request of the victim) on the person causing danger therefore aim to protect life, physical and psychological integrity, freedom, or sexual integrity of the victim within the EU regardless of national boundaries, and attempt to prevent new crimes against the same victim.

12. The EPO should be issued, at the request of the victim in the 'issuing (Member) State', by any judicial (or equivalent) authority. The process consists of the following steps:

(a) the 'issuing State' makes a request for an EPO;

(b) on receipt of the EPO, the 'executing State' adopts a decision under its national law in order to continue the protection of the person concerned.

13. For the achievement of this objective, administrative measures have to be put in place. These will in part cover the exchange of personal information between the 'issuing' and the 'executing' Member States relating to the person concerned (the 'victim') and the person causing danger. The exchange of personal data is foreseen in the following provisions:

(a) in Article 6 it is provided that the EPO itself contains many elements of personal information, as specified under (a), (e), (f), (g) and (h) and Annex I;

(b) the obligations of the competent authority of the executing State in Article 8(1) require the processing of personal data, in particular the obligation to notify any breach of the protection measure (Article 8(1)(d) and Annex II);

(c) the obligations of the competent authority of the executing and the issuing Member States in case of modification, expiry or revocation of the protection order and/or protection measures (Article 14).

14. The information mentioned in the preceding paragraph clearly falls within the scope of personal data, broadly defined in data protection legislation as 'any information relating to an identified or identifiable natural person' ([15]) and further explained by the Article 29 Working Party. The EPO initiative deals with information about an individual (the victim or the person causing danger) or information that is used or is likely to be used to evaluate, treat in a certain way or influence the status of an individual (in particular, the person causing danger) ([16]).

II.3. EIO initiative

15. The EIO initiative — based on Article 82(1)(a) of the TFEU — requires Member States to collect, store and transmit evidence, even if this is not yet available in the national jurisdiction. The initiative therefore goes beyond the principle of availability, presented in the Hague programme of 2004 as an innovative approach to the

([15]) See Article 2(a) of Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters as well as Article 2(a) of Directive 95/46/EC and Article 2(a) of Regulation (EC) No 45/2001.

([16]) See Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136, adopted on 20th June 2007, p. 10.

cross-border exchange of law enforcement information ([17]). It also goes beyond Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant that is only applicable to (given) evidence which already exists ([18]).

16. An EIO is to be issued for the purpose of having one or more specific investigative measure(s) carried out in the executing State with a view to gathering evidence (potentially not in existence when the order is released) and transferring it (Article 12). It applies to almost all investigative measures (see Recitals 6 and 7 of the initiative).

17. The objective of the EIO initiative is to create a single, efficient and flexible instrument for obtaining evidence located in another Member State in the framework of criminal proceedings, instead of the more complex current legal instrument used by judicial authorities (based on mutual legal assistance, on the one hand, and mutual recognition, on the other) ([19]).

18. Clearly, evidence collected by way of an EIO (see also Annex A to the initiative) may contain personal data, as in the case of information on bank accounts (Article 23), information on banking transactions (Articles 24) and monitoring of banking transactions (Article 25) or could cover the communication of personal data (as in the case of video or telephone conference, set out in Articles 21 and 22).

19. For these reasons the EIO initiative has a significant impact on the right to the protection of personal data. Also considering that the date for implementation of Framework Decision 2008/978/JHA has not yet expired (and it is therefore difficult to assess the effectiveness of the instrument and the need for additional legal measures) ([20]), the EDPS recalls the need of a periodical verification, in light of the data protection principles, of the effectiveness and of the proportionality of the legal measures adopted in the AFSJ ([21]). The EDPS therefore recommends adding an evaluation clause to the EIO initiative, requiring the Member States to report on a regular basis on the application of the instrument and the Commission to synthesise these reports and, where relevant, issue appropriate proposals for amendments.

II.4. **Processing of personal data envisaged in the EPO and EIO initiatives**

20. As explained above in points 13, 14 and 18, it is clear that under the proposed directives, personal data will be processed and exchanged by the competent authorities of the different Member States. Under those circumstances, the data subject is protected by the fundamental right to data protection, as recognised in Article 16 TFEU and Article 8 of the EU Charter of Fundamental Rights.

21. Despite this, in the 'Detailed statement' accompanying the EPO initiative the estimated 'Risk of encroaching upon fundamental rights' is identified as '0' (zero) ([22]), and in the impact analysis contained in the 'Detailed statement' accompanying the EIO initiative data protection issues are not taken into consideration ([23]).

22. The EDPS regrets these conclusions and emphasises the importance of data protection in the particular context in which personal data are processed, namely:

(a) the wide field of judicial cooperation in criminal matters;

(b) the data are quite often of a sensitive nature and usually obtained by police and judicial authorities as a result of an investigation;

(c) the possible content of the data, particularly in relation to the EIO initiative, which would extend to any kind of evidence; and

([17]) The principle enshrined in the Hague programme. Strengthening Freedom, Security and Justice in the European Union, point 2.1, means 'that, throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement of ongoing investigations in that State'. On this matter, see the EDPS Opinion on the proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final), OJ C 116, 17.5.2006, p. 8.

([18]) Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (OJ L 350, 30.12.2008, p. 72).

([19]) Two mutual recognition instruments applicable to obtaining evidence currently exist: Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ L 196, 2.8.2003, p. 45) and Framework Decision 2008/978/JHA, cited in footnote 18.

([20]) Article 23(1) of the Framework Decision 2008/978/JHA provides that 'Member States shall take the necessary measures to comply with the provisions of this Framework Decision by 19 January 2011'.

([21]) Also paragraph 1.2.3 of the Stockholm programme demands that new legislative initiatives should be tabled after verification of the principle of proportionality.

([22]) Detailed Statement allowing to appraise compliance with the principles of subsidiarity and proportionality in accordance with Article 5 of Protocol (No 2) to the Lisbon Treaty of 6 January 2010.

([23]) The Detailed Statement of 23 June 2010, Interinstitutional File: 2010/0817 (COD) refers explicitly only to the right of freedom and security and the right of good administration (see p. 25 and p. 41).

(d) the possible communication of evidence outside the EU, in accordance with Article 13 of Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters ([24]).

23. This context gives the data processing operations particular impact and may significantly affect the fundamental rights of the data subject, including the right to the protection of personal data.

24. Due to the above considerations, the EDPS wonders why the initiatives neither address the protection of personal data (apart from making reference to the duties of confidentiality imposed on the actors involved in an investigation by Article 18 of the EIO initiative), nor explicitly refer to Framework Decision 2008/977/JHA. Indeed, this Framework Decision would be applicable to the processing operations envisaged in the two initiatives (see Article 1(2)(a)).

25. For this reason, the EDPS welcomes that during the preparatory works in Council related to the EPO initiative, a reference to the Framework Decision 2008/977/JHA has been introduced ([25]) and is confident that the European Parliament will confirm this change to the original initiatives ([26]).

26. The EDPS regrets that a similar recital has not yet been introduced in the EIO initiative, which involves a much more intense exchange of personal data. The EDPS welcomes in this context that the European Commission, commenting on the EIO initiative, suggests that a reference (both in the recital and in the body of the proposal) to the applicability of the Framework Decision 2008/977/JHA should be introduced ([27]).

27. Therefore, and without prejudice to Section III below, both initiatives should include a specific provision clarifying that Framework Decision 2008/977/JHA applies to the data processing foreseen in the initiatives.

III. SPECIFIC RULES NEEDED IN ADDITION TO THE EXISTING LEGAL DATA PROTECTION FRAMEWORK FOR JUDICIAL COOPERATION IN CRIMINAL MATTERS

28. Both initiatives once again raise the fundamental issue of the incomplete and inconsistent application of data protection principles in the field of judicial cooperation in criminal matters ([28]).

29. The EDPS is aware of the importance of enhancing the effectiveness of judicial cooperation between Member States, also in the fields covered by the EPO and the EIO initiatives ([29]). The EDPS furthermore sees the advantages and the need to share information, but wishes to underline that the processing of such data must be in conformity — inter alia ([30]) — with the EU rules on data protection. This is even more evident in light of the Lisbon Treaty introducing Article 16 TFEU and giving binding force to Article 8 Charter of Fundamental Rights of the European Union.

30. Situations which involve the cross-border exchange of information within the EU deserve special attention since the processing of personal data in more than one jurisdiction increases the risks to the rights and interests of natural persons involved. The personal data will be processed in multiple jurisdictions where the legal requirements as well as the technical framework are not necessarily the same.

31. It furthermore leads to legal uncertainty for the data subjects: parties from other Member States may be involved, the national laws of various Member States might be applicable and might differ from the laws data subjects are used to, or apply in a legal system which is unfamiliar to the data subject. This requires greater efforts to ensure compliance with the requirements stemming from EU legislation on data protection ([31]).

([24]) Further: Framework Decision 2008/977/JHA.

([25]) See recital 27 of the latest draft of the EPO initiative (28 May 2010, Council doc. No 10384/2010): 'Personal data processed when implementing this Framework Decision should be protected in accordance with 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 and in accordance with the principles laid down in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which all Member States have ratified'.

([26]) In this sense, see the Amendment 21 included in the draft report on the initiative for a directive of the European Parliament and of the Council on the European Protection Order (00002/2010 — C7-0006/2010 — 2010/0802 (COD)), 20.5.2010, Committee on Civil Liberties, Justice and Home Affairs — Committee on Women's Rights and Gender Equality, Rapporteurs: Teresa Jiménez-Becerril Barrio, Carmen Romero López, at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/femm/pr/817/817530/817530en.pdf

([27]) See Commission comments on proposed European Investigation Order in criminal matters, 24.8.2010, JUST/B/1/AA-et D(2010) 6815, pp. 9 and 38, at http://ec.europa.eu/justice/news/intro/doc/comment_2010_08_24_en.pdf

([28]) See also Section V of the opinion.

([29]) See, inter alia, the endorsement of the need to improve access to justice, cooperation between European legal authorities and the effectiveness of the justice system itself in the EDPS Opinion on the European e-Justice Strategy (OJ C 128, 6.6.2009, p. 13, points 9 and 21).

([30]) In relation to the aspect related to the respect of the criminal procedural rules in Member States, notably in the area of the EIO proposal, reference can be made to the considerations and concerns contained in the responses sent to the European Commission during the public consultation on the Green Paper (see footnotes 11 and 12).

([31]) See also Council, the Hague programme: Strengthening Freedom, Security and Justice in the European Union (2005/C 53/01) (OJ C 53, 3.3.2005, p. 1, 7 et seq.).

32. In the EDPS' view, clarifying the applicability of Framework Decision 2008/977/JHA, as proposed in point 27, is only a first step.

33. The specific challenges for effective protection in the area of judicial cooperation in criminal matters, combined with a not fully satisfactory Framework Decision 2008/977/JHA (see points 52–56) may call for specific provisions on data protection, when specific legal instruments of the EU require the exchange of personal data.

IV. **CHALLENGES FOR EFFECTIVE DATA PROTECTION IN CRIMINAL COOPERATION: RECOMMENDATIONS ON EPO AND EIO INITIATIVES**

IV.1. **Introductory remarks**

34. Effective protection of personal data (as highlighted in point 29) is not only important for the data subjects but also contributes to the success of the judicial cooperation itself. In fact, the willingness to exchange these data with authorities of other Member States will increase if an authority is assured of the level of protection, accuracy and reliability of personal data in that other Member State ([32]). In short, setting a (high) common standard for data protection in this sensitive area will promote mutual confidence and trust between Member States and reinforce the judicial cooperation based on mutual recognition, improving data quality in the exchange of information.

35. In this specific context, the EDPS recommends including specific safeguards for data protection in the EPO and EIO initiatives, in addition to the general reference to Framework Decision 2008/977/JHA (as proposed in paragraph 27).

36. Some of these safeguards are of a more general nature and are meant to be included in both initiatives, in particular the safeguards aiming at improving the accuracy of the data, as well as the security and confidentiality. Other safeguards relate to specific provisions in either the EPO or the EIO initiative.

IV.2. **Safeguards of a more general nature**

Accuracy

37. In those situations foreseen by the initiatives where data are exchanged between Member States specific emphasis should be put on ensuring the accuracy of the information. The EDPS welcomes in this respect that the EPO initiative contains in Article 14 clear obligations on the competent authority of the issuing state to inform the competent authority of the executing state of any modification or of the expiry or the revocation of the protection order.

38. The EDPS also notes that the need for translation might affect the accuracy of the information, especially since the initiatives relate to specific legal instruments which may have a different meaning in different languages and different legal systems. In this context, the EDPS while welcoming the fact that the EPO initiative addresses the issue of translations (Article 16), also suggests including a similar provision in the EIO initiative.

Security, awareness and accountability

39. The growth of cross-border cooperation which could result from the adoption of the two initiatives requires a careful consideration of security aspects of cross-border transmission of personal data related to the execution of EPOs or EIOs ([33]). This is necessary, not only to meet the security standards in the processing of personal data required by Article 22 of Framework Decision 2008/977/JHA, but also to ensure the secrecy of investigations and the confidentiality of the concerned criminal proceedings which is regulated under Article 18 EIO initiative and, as a general rule for personal data resulting from cross-border exchange, under Article 21 of Framework Decision 2008/977/JHA.

40. The EDPS emphasises the need for secure telecommunication systems in the transmission procedures. He therefore welcomes the provision for use of the European Judicial Network ([34]) as a tool to ensure that EPO and EIO are correctly addressed to the competent national authorities, in this way preventing or minimising the risk that inappropriate authorities are involved in the exchange of personal data (see Article 7(2) and (3) of the EPO initiative and Article 6(3) and (4) of the EIO initiative).

41. Therefore, the initiatives should include provisions requiring the Member States to ensure that:

([32]) See EDPS Opinion on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (COM(2005) 475 final) (OJ C 47, 25.2.2006, p. 27, points 5–7).

([33]) More in general, see communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee, Towards a European e-Justice Strategy, Brussels, 30.5.2008, COM(2008) 329 final, p. 8: 'Judicial authorities should be able to exchange confidential data in complete confidence'.

([34]) Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (OJ L 348, 24.12.2008, p. 130).

(a) competent authorities have adequate resources for the application of the proposed directives;

(b) competent officials shall observe professional standards and be subject to appropriate internal procedures that ensure, in particular, the protection of individuals with regard to the processing of personal data, procedural fairness and the proper observance of the confidentiality and professional secrecy provisions (as provided for in Article 18 of the EIO initiative).

42. Furthermore, the EDPS recommends the introduction of provisions ensuring that substantive data protection principles are observed when processing personal data, and to have the necessary internal mechanisms in place to demonstrate compliance to external stakeholders. Such provisions would be instruments to make data controllers accountable (according to the 'accountability principle' which is discussed in the context of the current review of the data protection framework ([35])). It requires them to carry out the necessary measures to ensure compliance. These provisions should include:

(a) authentication systems that allow only authorised individuals to have access to both databases containing personal data or premises where evidence are located;

(b) tracking of accesses to personal data and operations performed on them;

(c) implementing audit control.

IV.3. **Safeguards in EIO initiative**

43. Considering the particularly intrusive characteristics of certain investigative measures, the EDPS calls for a thorough reflection on the admissibility of evidence gathered for purposes other than the prevention, investigation, detection or prosecution of crime or the enforcement of criminal sanctions and the exercise of the right of defence. In particular the use of evidence obtained under Article 11(1)(d) of the FD 2008/977/JHA should be carefully considered ([36]).

44. An exception to the application of the provision of Article 11(1)(d) should therefore be included in the EIO initiative, stating that evidence gathered under the EIO may not be used for other purposes than the prevention, investigation, detection or prosecution of crime or the enforcement of criminal sanctions and the exercise of the right of defence.

IV.4. **Safeguards in EPO initiative**

45. In relation to the EPO initiative, the EDPS recognises that the personal data exchanged between the competent authorities and listed in Annex I to the initiative (relating to both the victim and the person causing danger) are adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed.

46. However, it is not sufficiently clear from the initiative — especially in Article 8(1)(b) — which personal data relating to the victim will be communicated to the person causing danger by the competent authority of the executing State.

47. The EDPS believes it is appropriate to consider the circumstances and content of the protection measures issued by the judicial authority in the issuing Member State prior to informing the person causing the danger. The latter should therefore be given only those personal data of the victim (which in some cases may include contact data) strictly relevant for the full execution of the protection measure.

48. The EDPS is aware that providing contact information (e.g. telephone numbers, address of the victim as well as of other places usually frequented, like workplace or children's school) may actually endanger the physical and psychological well-being of the victim, as well as affect his/her right to privacy and to protection of personal data. On the other hand, an indication of the relevant addresses may in some cases be necessary in order to warn the person causing danger of the places where he/she is forbidden to go. This is to enable compliance with the order and to prevent any potential penalties for its violation. Moreover, depending on the circumstances, the identification of the location(s) where the person causing danger is prohibited may be required in order not to unnecessarily limit his freedom of movement.

49. In light of these considerations, the EDPS highlights the importance of this topic and recommends that the EPO initiative clearly states that, depending on the circumstances of the case, the person causing the danger should be given

([35]) See Article 29 Data Protection Working Party and Working Party on Police and Justice, The Future of Privacy, p. 20 et seq.

([36]) This provision admits the use of evidence also for 'any other purpose only with the prior consent of the transmitting Member State or with the consent of the data subject, given in accordance with national law'.

only those personal data of the victim (which in some cases may include the contact data) strictly relevant for the full execution of the protection measure ([37]).

50. Finally, the EDPS asks for the clarification of the expression 'electronic means' contained in Recital 10 of the EPO initiative. In particular, it should be explained if personal data are processed using 'electronic means' and, in this case, what guarantees are provided.

V. DATA PROTECTION RULES AND JUDICIAL COOPERATION IN CRIMINAL MATTERS: CONCERNS LINKED TO EPO AND EIO INITIATIVES

51. Framework Decision 2008/977/JHA applies to all exchange of personal data under the EPO and EIO initiatives.

52. Although the EDPS has recognised that the Framework Decision 2008/977/JHA — when implemented by the Member States — is an important step forward for data protection in police and judicial cooperation ([38]), the Framework Decision itself is not fully satisfactory ([39]). The main unresolved concern relates to its limited scope. The Framework Decision is restricted to exchanges of personal data in the area of police and justice between authorities and systems in different Member States and at EU level ([40]).

53. Even if this concern can not be resolved in the context of the EPO and EIO initiatives, the EDPS insists on highlighting that the lack of a (high) common standard of data protection in judicial cooperation could imply that a judicial authority at national or EU level, when dealing with a criminal file comprising information originating from other Member States (including, e.g. evidence collected on the basis of an EIO) would have to apply different data processing rules: autonomous national rules (which must comply with Council of Europe Convention 108) for data originating in the Member State itself and the rules implementing Framework Decision 2008/977/JHA for data originating from other Member States. Different 'pieces of information' thus could fall within different legal regimes.

54. The consequences of applying a 'double' data protection standard to each criminal file with cross-border elements are relevant in day to day practice (for instance, retention of the information laid down by applicable laws of each of the transmitting bodies; further processing restrictions requested by each of the transmitting bodies; in case of a request from a third country, each transmitting body would give its consent according to its own evaluation of adequacy and/or international commitments; and differences in the regulation of the right of access by the data subject). In addition, citizens' protection and rights could vary and be subject to different broad derogations depending on the Member State where processing takes place ([41]).

55. The EDPS therefore uses the occasion to reiterate his opinions regarding the need for a comprehensive data protection legal framework covering all areas of EU competence, including police and justice, to be applied to both personal data transmitted or made available by competent authorities of other Member States and to domestic processing in AFSJ ([42]).

56. Finally, the EDPS observes that the data protection rules should apply to all sectors and to the use of data for all purposes ([43]). Of course, duly justified and clearly drafted exceptions should be possible, particularly regarding personal data processed for law enforcement purposes ([44]). Gaps in the protection of personal data are contrary to the current (renewed) legal framework of the European Union. Article 3(2) of Directive 95/46/EC — excluding from the scope of application of the directive the police and justice area — does not fulfil the philosophy contained in

([37]) This seems to be the sense of the amendments 13 and 55 of the draft report on the initiative for a directive of the European Parliament and of the Council on the European Protection Order (00002/2010 — C7-0006/2010 — 2010/0802 (COD)), 20.5.2010, Committee on Civil Liberties, Justice and Home Affairs — Committee on Women's Rights and Gender Equality.

([38]) See EDPS Opinion on the communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee towards a European e-Justice Strategy (2009/C 128/02) (OJ C 128, 6.6.2009, p. 13, point 17).

([39]) See the three EDPS Opinions on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (COM(2005) 475 final) (OJ C 47, 25.2.2006, p. 27; OJ C 91, 26.4.2007, p. 9; OJ C 139, 23.6.2007, p. 1). See also EDPS Opinion 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, points 19, 29 and 30).

([40]) See Article 2 of the Framework Decision 2008/977/JHA.

([41]) See the third EDPS Opinion on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ C 139, 23.6.2007, p. 41), mentioned in footnote 39, point 46.

([42]) This EDPS position is clearly supported by the Article 29 Data Protection Working Party and Working Party on Police and Justice, The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168, adopted on 1 December 2009, pp. 4, 7 et seq. and 24 et seq.

([43]) See communication from the Commission to the European Parliament and the Council, An area of freedom, security and justice serving the citizen, Brussels, 10.6.2009, COM(2009) 262 final, p. 30: 'The Union must establish a comprehensive personal data protection scheme covering all areas of EU competence'.

([44]) Such an approach would also comply with the aim of Declaration 21 attached to the Lisbon Treaty on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation.

Article 16 TFEU. Moreover, these gaps are not sufficiently covered by Council of Europe Convention No 108 ([45]), by which all the Member States are bound.

VI. **CONCLUSIONS AND RECOMMENDATIONS**

57. The EDPS recommends with regard to both the EPO and the EIO initiatives:

— to include specific provisions stating that the instruments apply without prejudice to 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,

— to include provisions requiring the Member States to ensure that:

— competent authorities have the resources necessary for the application of the proposed directives,

— competent officials shall observe professional standards and be subject to appropriate internal procedures that ensure, in particular, the protection of individuals with regard to the processing of personal data, procedural fairness and the proper observance of the confidentiality and professional secrecy provisions,

— authentication systems allow only authorised individuals to have access to both databases containing personal data or premises where evidence are located,

— tracking of accesses and operations are performed,

— audit controls are implemented.

58. The EDPS recommends with regard to the EPO initiative:

— to clearly state that, depending on the circumstances of the case, the person causing the danger should be given only that personal data of the victim (which in some cases may include the contact data) strictly relevant for the full execution of the protection measure,

— to clarify the expression 'electronic means' contained in recital 10 of the EPO initiative.

59. The EDPS recommends with regard to the EIO initiative:

— to include a provision on translations, similar to Article 16 of the EIO initiative,

— to include a provision that prevents the use of evidence for purposes other than the prevention, investigation, detection or prosecution of crime or the enforcement of criminal sanctions and the exercise of the right of defence, as an exception to Article 11(1)(d) of Framework Decision 2008/977/JHA,

— to add an evaluation clause to the EIO initiative, requiring from the Member States to report on a regular basis on the application of the instrument and from the Commission to synthesise these reports and, where relevant, issue appropriate proposals for amendments.

60. Moreover, and more in general, the EDPS:

— recommends the Council to establish a procedure in which consultation of the EDPS will take place, in case an initiative introduced by Member States is related to the processing of personal data,

— reiterates the need for a comprehensive data protection legal framework covering all areas of EU competence, including police and justice, to be applied to both personal data transmitted or made available by competent authorities of other Member States and to domestic processing in AFSJ.

Done at Brussels, 5 October 2010.

Peter HUSTINX

European Data Protection Supervisor

([45]) Convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe, 28 January 1981, No 108.