EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on

the Proposal 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

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

I. INTRODUCTION

I.1. Context of the opinion

1. On 27 March 2013, the Commission adopted the proposal 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 ("the Proposal"). The Proposal was sent by the Commission to the EDPS for consultation on the same day and received on 4 April 2013.

[1] OJ 1995, L 281/31.
[2] OJ L8, 12.1.2001, p. 1.
[3] OJ L350, 30.12.2008, p. 60.

2. Before the adoption of the Proposal, the EDPS was given the opportunity to provide informal comments. The EDPS welcomes the fact that many of these comments have been taken into account.

3. The EDPS welcomes the fact that he has been consulted by the Commission and that a reference to the consultation is included in the preambles of the Proposal.

4. The EDPS was also consulted on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions establishing a European law Enforcement Training Scheme, adopted in parallel with the Proposal[4]. However, he will refrain from issuing a separate reaction on this communication, since he has only very limited comments which are included in part IV of this opinion.

I.2. Aim of the Proposal

5. The Proposal is based on Articles 88 and Article 87 (2) (b) of the Treaty on the Functioning of the European Union (TFEU) and has the following aims[5]:
   - align Europol with the requirements of the Lisbon Treaty, by adopting a legal framework under the ordinary legislative procedure;
   - meet the goals of the Stockholm Programme by making Europol a hub for information exchange between the law enforcement authorities of the Member States and establishing European training schemes and exchange programmes for all relevant law enforcement professionals;
   - grant Europol new responsibilities, by taking over the tasks of CEPOL and giving a legal basis for the EU cybercrime centre;
   - ensure a robust data protection regime, in particular by strengthening the supervision structure;
   - improve the governance of Europol by seeking increased efficiency and aligning it with the principles laid down in the Common approach on EU decentralised agencies.

   The EDPS emphasises that the Proposal is of great importance from the perspective of processing of personal data. The processing of information, including personal data, is a principal reason for the existence of Europol. In the current state of EU development, operational police work remains a competence of the Member States. However, this task has an increasingly cross border nature, and the EU level provides support by providing, exchanging and examining information.

I.3. Aim of the Opinion

6. This Opinion will focus on the most relevant changes of the legal framework for Europol from the perspective of data protection. It will first analyse the legal context, its development and the consequences for Europol. It will then elaborate on the main changes, which are:
   - The new information structure for Europol, which implies a merger of the different databases, and its consequences for the principle of purpose limitation.

[4] COM(2013) 172 final.
[5] Explanatory Memorandum, part 3.

- The strengthening of data protection supervision.
- Transfer and exchange of personal data and other information, with a focus of the exchange of personal data with third countries.

7. Subsequently, the Opinion will discuss a number of specific provisions of the Proposal, with an emphasis on Chapter VII thereof (Articles 34-48) on data protection safeguards.

II. ANALYSIS OF THE LEGAL CONTEXT

8. The European Police Office ('Europol') started as an intergovernmental body regulated by a Convention[6] concluded between Member States, which entered into force on 1 October 1998. In 2009, the Europol Convention was replaced by a Council Decision adopted on 6 April 2009[7]. This provided that Europol would be financed from the Community budget and would be subject to the EC Financial Regulation and Staff Regulations, thus aligning Europol with other EU bodies and agencies. This new legal framework came into force on 1 January 2010 when Europol became an EU Agency.

Lisbon Treaty and Europol

9. The Lisbon Treaty - which entered into force on 1 December 2009 - abolished the 'pillar structure' of EU legislation and brought the establishment of Europol under Article 88 TFEU. Consequently, Europol's legal basis has moved from the consultation procedure, subject to unanimity in the Council following consultation of the European Parliament, to the ordinary legislative procedure, with qualified majority voting in the Council and full co-legislative powers of the European Parliament. Furthermore, the Lisbon Treaty has transformed the area of police and judicial cooperation in criminal matters (the former third pillar) into the main area of EU law, which - for example - will lead to the full jurisdiction of the Court of Justice of the European Union.

10. In this respect, the Protocol on transitional provisions annexed to the Lisbon Treaty[8] imposes a five-year transition period before the existing third pillar instruments, including the Europol Council Decision, will be treated in the same way as the Community instruments. Article 10 of the Protocol provides for the legal effects of all acts adopted before the entry into force of the Lisbon Treaty to be preserved until these acts are repealed, annulled or amended. In addition, the extended competence of the Court of Justice and the possibility for the Commission to launch infringement procedures will not apply to these acts, until either they are amended or five years from the entry into force of the Treaty have elapsed.

11. The EDPS welcomes the Proposal. It aligns Europol with the requirements of Article 88 (2) TFEU. The stronger role for the European Parliament as co-legislator, the extension of the qualified majority principle in the Council as well as the full

[6] Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (the 'Europol Convention'), OJ C 316, 27.11.1995, p.1.
[7] Council Decision of 6 April 2009 establishing the European Police Office (Europol) (the 'Europol Council Decision'), OJ L 121, 15.05.2009, p. 37.
[8] Protocol (No 36) on transitional provisions, OJ C115, 09.05.2008, p. 322.

jurisdiction of the Court of Justice will have a positive impact on the quality and the consistency of the legal framework, including the crucial aspects relating to the protection of personal data. The general data protection rules, as well as specific tailored rules that may be necessary for particular exchanges of data will benefit from the full involvement of all the EU institutions concerned.

Lisbon Treaty and data protection

12. The entry into force of the Lisbon Treaty marked a new era for data protection. Article 6 of the Treaty on European Union (TEU), as amended, confers binding legal effect on the EU Charter of Fundamental Rights[9]. Article 8 of the Charter enshrines the right of every individual to the protection of personal data and sets forth its main elements. This fundamental right is also laid down in Article 16(1) TFEU. Moreover, Article 16(2) TFEU provides a specific legal basis for a strong EU wide data protection law in all areas of EU policy, including the field of police and judicial cooperation in criminal matters.

13. In this respect, the Commission adopted a package for reforming the EU legal framework for data protection on 25 January 2012. The package includes a Communication[10] and two legislative proposals ('the DP proposals): a general Regulation on data protection[11] ('the proposed DP Regulation') and a specific Directive for the area of police and justice[12] (the 'proposed DP Directive').

14. The EDPS has warmly welcomed the DP proposals, in particular the proposed DP Regulation which constitutes a huge step forward in providing more effective and more consistent data protection in EU. However, the EDPS has warned that the Data Protection proposals are still far from a comprehensive set of data protection rules on national and EU level in all areas of EU policy[13].

15. The need for a comprehensive approach to the revised EU data protection framework had been announced by the Commission in its Communication of November 2010 entitled 'A comprehensive approach on personal data protection in the European Union'[14]. This was welcomed and endorsed by the European Parliament and the Council. In its Resolution of 6 July 2011, the European Parliament expressed its full engagement with a comprehensive approach[15]. Also the

[9] Charter of Fundamental Rights of the European Union, OJ C 83, 30.03.2010, p. 389.
[10] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, entitled 'Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century', COM(2012)9 final.
[11] Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012)11 final.
[12] Proposal for a Directive on the protection of individuals with regard to the processing of personal data for the purposes of prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012)10.
[13] See EDPS opinion of 7 March 2012 on the data protection reform package, OJ C192, 30.06.2012, p.7, section 1.2. The full text of this opinion can be found on the EDPS website: http://www.edps. europa.eu.
[14] Communication of 4 November 2010 of the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee for the Regions entitled 'A comprehensive approach on personal data protection in the European Union', COM(2010) 609 final.
[15] See European Parliament Resolution of 6 July 2011, 2011/2025(INI).

Council, in its conclusions of 24 and 25 February 2011, referred to a new legal framework based on the comprehensive approach[16].

16. The EDPS Opinion of 14 January 2011 stressed the importance of a comprehensive legal instrument for data protection, including police and judicial cooperation in criminal matters. Comprehensiveness was underlined as a *conditio sine qua non* for effective data protection in the future[17]. The EDPS highlighted that there is no fundamental difference between police and judicial authorities and other authorities of the Member States endowed with tasks of law enforcement, such as authorities for taxation, customs, anti-fraud and immigration. These latter authorities are subject to Directive 95/46/EC. He also recalled that most Member States have given wide scope to their national legislation implementing Directive 95/46/EC and Council of Europe Convention 108[18], also applying them to their police and judicial authorities.

17. The EDPS also expressed a clear preference for including data processing by the EU institutions, bodies, offices and agencies in this general legal instrument. A single text would avoid the risk of discrepancies between provisions between different instruments and would be the most suitable vehicle for data exchange between the EU level and the public and private entities in the Member States.

18. However, the Commission has taken a different approach. First, it has chosen to regulate data protection in the law enforcement area in a self-standing instrument (the proposed DP Directive) which is not fully aligned to the level of protection of the proposed DP Regulation[19]. Second, the data protection rules for EU institutions, bodies and agencies as laid down in Regulation (EC) No 45/2001 have been left untouched, as well as specific measures in the area of police and judicial cooperation in criminal matters, and have been postponed to a later stage.

Consequences for Europol

19. At EU level, following the entry into force of the Lisbon Treaty, Regulation (EC) No 45/2001 applies to the processing of personal data by all Union institutions, bodies, offices and agencies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Union law, except where Union law has clearly and specifically provided otherwise.

20. It has been argued that under the current legal framework the existence of specific rules for data protection would have as a consequence that Regulation (EC) No 45/2001 would not apply to Europol, in any event not to its core activities. There is no need to question, in the context of this Opinion, this argument.

---

[16] See the Council conclusions of the 3071st Justice and Home Affairs Council meeting of 24 and 25 February 2011.

[17] See EDPS Opinion of 14 January 2011 on the Communication from the Commission on 'A comprehensive approach on personal data protection in the European Union', OJ C 181/01, 22.06.2011, p.1, point 3.2.5.

[18] Convention for the Protection of Individuals with regard to Automatic Processing of Personal data, Strasbourg, 28.01.1981

[19] In his Opinion of 7 March 2012 (No. 20) the EDPS even stated that the level of protection provided by the proposed DP Directive is by far inferior to the proposed DP Regulation (see also Nos. 309-310).

21. However, despite the fact that the current specific regime for Europol would only seem to refer to Europol's core activities, there is some debate as to the status of administrative personal data and staff data at Europol. The EDPS therefore welcomes the proposal to clarify that Regulation (EC) No 45/2001 should be fully applicable to those data[20].

22. The processing of personal data by Europol for its core activities (*i.e.* to support and strengthen Members States' action in combating serious crimes) is treated differently. The Commission has opted in the Proposal for an autonomous data protection regime, based on the assumption that Regulation (EC) No 45/2001 is inapplicable to Europol. The EDPS regrets that the Commission has not chosen to apply Regulation (EC) No 45/2001 to Europol, and limit the Proposal to additional special rules and derogations, which duly take account of the specificities of the law enforcement sector.

23. However, the EDPS notes that Recital 32 of the proposal explicitly mentions that data protection rules at Europol should be strengthened and draw on the principles underpinning Regulation (EC) No 45/2001. As a consequence, the Proposal includes most of the substantive elements of Regulation (EC) No 45/2001.

24. Recital 32 also specifies that the data protection rules at Europol should be aligned with other relevant data protection instruments applicable in the area of police cooperation in the Union, in particular Convention 108 and Recommendation No R(87)15 of the Council of Europe[21] and Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[22]. The EDPS recalls that neither Convention 108, nor the Council Framework Decision apply to Europol, but he of course supports the intention to ensure that the protection afforded by those instruments in the Member States is respected by Europol.

The data protection reform

25. As said before, comprehensiveness is one of the main drivers and purposes for the data protection reform. Earlier, the EDPS had called for a single comprehensive instrument including police and justice. Such an instrument may allow for additional special rules which duly take account of the specificities of the police and justice sector, in line with Declaration 21 attached to the Lisbon Treaty. A proliferation of different regimes applying to, for instance, Europol, Eurojust, SIS and Prüm should be avoided.

26. The EDPS therefore recommends specifying in the recitals of the Proposal that the new data protection framework of the EU institutions and bodies should be applicable to Europol as soon as it is adopted. In addition, the application of the data protection regime for EU institutions and bodies to Europol should be clarified

[20] Regulation 45/2001 already applies to all activities of CEPOL.
[21] Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector, 17.09.1987.
[22] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJ L 350, 30.08.2008, p. 60.

within the instrument replacing Regulation (EC) No 45/2001, as first announced in 2010, in the context of the review of the data protection package[23].

27. Recital 32 of the Proposal mentions that the data protection rules of Europol should be autonomous and aligned with other relevant data protection instruments applicable in the area of police cooperation in the Union including the Framework Decision 2008/977/JHA, and specifies that this Decision will be replaced by the relevant Directive in force at the moment of adoption. The EDPS draws the attention to the fact that the Europol Council Decision provides for a robust data protection regime and considers that this level should not be lowered independently of the discussions on the proposed DP Directive. This should be specified in the recital.

28. Finally, at the latest from the moment of the application of the new general framework, the main new elements of the data protection reform (*i.e.* accountability principle, data protection impact assessment, privacy by design and by default and notification of personal data breach) , should also be applied to Europol. This should also be mentioned in the recitals. As will be developed further below, these elements are currently absent from, or not sufficiently taken into account in, the Proposal.

III. ANALYSIS OF THE PROPOSAL

GENERAL COMMENTS

29. The role of Europol is to provide support to national law enforcement authorities and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States[24]. The assistance offered by Europol to national law enforcement authorities involves facilitating exchanges of information, providing criminal analyses, as well as helping and coordinating cross border operations. To achieve these tasks, Europol's core activities consist of gathering, analysing and disseminating information including, to a large extent, personal data.

30. A strong framework of data protection is not only important for data subjects but also contributes to the success of police and judicial cooperation itself. It forms the basis for the trust of the Member States which provide the police and judicial information. The personal data concerned are quite often of a sensitive nature and have been obtained by police and judicial authorities as a result of an investigation of persons. One of the problems raised in the Impact assessment is that Member States do not provide Europol with sufficient information. This tendency not to share information is driven, amongst others, by the police culture which encourages law enforcement officers to be cautious about such things. A strong data protection regime should contribute to enhance trust between Member States, as a condition for a successful exchange of information. Clear purposes with related specific and strict rules would result in an easier acceptance of personal data exchanges. Finally, ensuring respect for the data protection principles would further ensure that Europol

[23] Communication from the Commission entitled "A comprehensive approach on personal data protection in the European Union", COM(2010)609 final, pp. 18-19.
[24] Article 4 of Europol Council Decision.

operates under the rule of law, generating trust in its behaviour and thereby fostering a wider sense of trust in EU institutions

31. The Commission has repeatedly highlighted the importance of strengthening data protection in the context of law enforcement and crime prevention, where the exchange and use of personal information has significantly increased[25]. In addition the Stockholm Programme, approved by the European Council, refers to a strong data protection regime as the main prerequisite for the EU Information Management Strategy in this area[26].

32. It is all the more important therefore that the Proposal ensures a high level of data protection, at least as high as that resulting from the current framework.

a) New Europol information structure

33. The present Europol Council Decision contains detailed provisions on data protection, which are further complemented by a set of implementing rules such as the Council Acts related to the rules applicable to Analysis Work Files[27], rules governing Europol's relations with partners[28], rules on confidentiality[29] and conditions related to the processing of data for the purpose of determining relevance to Europol tasks[30].

34. Under the Europol Council Decision, Europol processes information, including personal data, in two main systems, the Europol Information System ('EIS') and the Analysis Work files ('AWF')[31]. These systems are technically and legally separated, with specific rules on their purposes and access rights. As a result, Europol is not allowed to link and make analysis of pieces of data spread over the different databases found in these systems. In addition, there are no possibilities for Europol to deviate from the specific pre-defined architecture.

35. The Proposal aims to provide for more flexibility, to allow Europol to set up gradually an architecture that would adapt to upcoming business needs requiring the establishment of innovative data processing solutions. To this end, the Proposal

[25] See Communication of 20.07.2010 from the Commission to the European Parliament and the Council - "Overview of information management in the area of freedom, security and justice", COM(2010) 385 final.
[26] The Stockholm Programme - An open and secure Europe serving and protecting citizens (2010/C 115/01), OJ C 115, p. 1.
[27] Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files, OJ L 325, 11.12.2009, p. 14.
[28] Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information, OJ L 325, 11.12.2009, p.6. See also Council Decision 2009/935/JHA of 30 November 2009 determining the list of third States and organisations with which Europol shall conclude agreements, OJ L 325, 11.12.2009, p. 12.
[29] Council Decision 2009/968/JHA of 30 November 2009 adopting the rules on the confidentiality of Europol information, OJ L 332, 17.12.2009, p. 17.
[30] Decision of the Management Board of Europol of 4 June 2009 on the conditions related to the processing of data on the basis of Article 10(4) of Europol Council Decision, OJ L 348, 29.12.2009, p.1.
[31] Article 10 of Europol Council Decision.

removes the general rules governing different systems and focuses on purposes for which the data have been provided rather than pre-defined systems[32].

36. Under Article 24 of the Proposal, Europol is allowed to process information for the following purposes: (a) cross-checking aimed at identifying connections between information, (b) analysis of strategic or thematic nature and (c) operational analyses in specific cases. Neither the Proposal nor any accompanying document further specifies these purposes.

The current information architecture

37. To enable the changes to be understood, the EDPS will briefly describe below the main elements of the present system, and its functioning in practice. This description will show that the Europol Council Decision already offers considerable flexibility.

38. The EIS is a reference database used for cross-checking purposes: it enables Member States to share and retrieve information about individuals, events and devices connected with a criminal case. Data stored in the EIS must relate to suspects, convicted criminals or individuals on whom there are factual indications or reasonable grounds to believe that they have committed or will commit crimes that fall within Europol's mandate. The Europol Council Decision sets forth an exhaustive list of the types of data that may be stored in the EIS, the data retention periods, and the rules on access to and use of data stored in the EIS [33].

39. In contrast to the EIS, the AWFs aim at focusing on analysis in specific crime areas. Data stored in AWFs may not only relate to suspects but also to witnesses, victims, contacts, associates and informants[34]. The categories of data that may be stored in the AWFs are broader than for the EIS[35]. However, additional data protection rules apply to AWFs. Prior to its creation, each AWF is subject to an Opening Order. The Opening Order must specify the purpose of the AWF, determine the individuals on whom data may be stored and the nature of the data. Pursuant to Article 16.1 of the ECD, the Opening Order must also describe the general context leading to the decision to open the file, the conditions and procedures for communication of the data to certain recipients as well as the duration of storage[36].

40. Until 2010, 23 AWFs existed, which meant 23 different disconnected databases dealing each with a specific type of organised crime. At the end of 2010, the AWF

[32] See Recital 20 of the Proposal. See also p. 23 and 24 of the Impact assessment.
[33] See Article 12, 13 and 20.
[34] Article 14 of the Europol Council Decision. See also Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules fur Europol analysis work files, OJ L 325, 11.12.2009, p. 14.
[35] Article 6 of the Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files, OJ L 325, 11.12.2009, p. 14 ('AWF rules')
[36] To be complete, Article 10(2) of the Europol Council Decision also allows Europol to set up new systems processing personal data. However such systems may not process personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership or personal data related to health or sex life. However, the ability to create new systems has not been used for the two following main reasons: the lack of operational need and the restrictions on the storage of sensitive personal information (See on this, Evaluation of the Implementation of the Europol Council Decision and of Europol activities, Technical report, p. 80-81, available on Europol website).

system was reorganised and made more flexible. It now allows Europol analysts to have access to relevant information processed in other AWFs. The 23 existing AWFs were merged into two AWFs. One AWF focuses on 'serious and organised crime'; the other on 'counter terrorism'. As a result of the merger, the purposes of the two AWFs are broad and raise concerns as to the purpose specification required by Article 16(2)(d) of Europol Council Decision. Hence, within each of the two AWFs, Focal points[37] and/or Target groups[38] have been created, each one defining a specific purpose for the data it will hold. The specific purpose, together with the nature of the data and the individuals on whom data may be stored on the level of the Focal point or the Target group, are specified in Annexes to the AWF's Opening Orders.

41. Under this new AWF concept, Europol analyst groups have access to all information processed in the AWF they are allocated to. Further use of the information accessed is allowed under the strict conditions that (i) Europol analysts establish a clear link with the purpose of the Focal point or Target group they are responsible for and that (ii) only the necessary data are further processed in the Focal Point or Target Group.

42. This flexibility would allow, for instance, detection of links between investigations and common *modi operandi* across different criminal groups[39]. The picture of organised crime today is quite different from the period when Europol was established. The development of the internal market, the subsequent abolishing of borders, together with the advantages offered by globalisation and technological innovations, have created opportunities for new profits for existing and emerging criminal groups. Criminal organisations are more sophisticated and dynamic. They no longer focus on specific crimes but commit fast-growing diversified offences, shifting from one activity to another, and adding new activities to the ones in which they already specialise. In addition, criminal groups are no longer confined to geographical areas and quite often cooperate with other different organized crime groups. The diversity both of the criminal offences and of the composition of the criminal groups requires a different approach.

Assessment of the EDPS

43. The EDPS understands the need for flexibility in connection with the changing context, as well as in light of the growing roles of Europol, which will further develop as a hub for information exchange between the law enforcement authorities of the Member States, and also have autonomous tasks in processing of information. In this perspective, Europol must be able to fulfil its roles in the most effective and efficient way. The existing information architecture is not necessarily the benchmark for the future. The EDPS will therefore assess the new system on its own merits rather than on the basis of the need for changes of the present system.

[37] *i.e* an area which focuses on a certain phenomenon from a commodity based, thematic or regional angle (e.g. child exploitation, drugs trafficking through the Western Balkans, ...), Impact assessment, p. 33

[38] *i.e* an operational project with a dedicated Europol team to support an international criminal investigation or criminal intelligence operation against a specific target, (e.g. an identified individual criminal group: a criminal organisation from Kosovo, ...) Impact assessment, p. 33.

[39] See Impact assessment, p. 14 ('Aspect 1 of the problem').

44. The EDPS would underline that it is up to the legislators to determine the main lines of the information structure of Europol. In his role as advisor to the legislators he focuses on the question to what extent the choice of the legislators is constrained by - and if so in accordance with - the principles of data protection. In the present context, this means an assessment of the level of protection given to the data subject in the light of the principle of purpose limitation, as applied to the area of police cooperation. On the basis of this assessment, the EDPS will propose introducing further safeguards to the approach of Article 24 of the Proposal.

Purpose limitation

45. The EDPS recalls that purpose limitation is a key principle of data protection, as recognised by Article 8 of the Charter of the Fundamental Rights of the European Union. It is both an essential condition for processing and a prerequisite for other data quality requirements. Purpose limitation contributes to transparency, legal certainty and predictability. This principle aims at protecting data subjects by setting limits on how controllers are able to use their data. This is all the more important in the area of police and judicial cooperation in criminal matters, where data subjects are usually unaware of when data relating to them are being processed.

46. A specified purpose means that it is precisely and fully determined which processing is and is not included within the specified purpose[40]. It will determine the relevant data to be collected, retention periods, and all other key aspects of how personal data will be processed for the chosen purpose(s).

Consequences for Article 24

47. The EDPS has the following comments on Article 24 of the Proposal, in light of the principle of purpose limitation:

    - Article 24(1)(a) allows cross-checking of data aiming at identifying connections between information. The EDPS welcomes that Article 24(2) and Annex 2 limit the cross-checking to data related to (i) persons who are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence, and (ii) persons regarding whom there are factual indications or reasonable grounds that they will commit criminal offences.

    - Under Article 24(1)(b), personal data on suspects but also on witnesses, victims, contacts and associates may be processed both for strategic or thematic analysis. If Article 24(1)(b) aims to refer to the current analysis of general trends and organised crime threat assessments[41], the EDPS takes the view that personal data are not required. He recommends defining the notions of strategic, thematic and operational analysis in the Proposal and deleting the possibility to process

[40] See the Opinion 03/2013 of 2.04.2013 of Article 29 Data Protection Working party on purpose limitation, 39 Section II.2.1., available on the WP29 website at the following address: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[41] See Europol review, General report on Europol's activities, available on Europol's website.

personal data for strategic or thematic analysis, unless a sound justification is given.

- Article 24(1)(c) of the Proposal provides that Europol may process information for the purposes of operational analysis in specific cases. The provision does not require determining a specific purpose for these cases nor to process only the personal data relevant to each specific purpose. In contrast, Article 16 of the Europol Council Decision provides that, for each AWF, a specific purpose and the categories of the data to be processed are described in the opening order. The principle of purpose specification has been implemented through the concepts of Focal points and Target groups. The EDPS therefore recommends including a limitation of the purposes based on the experience of the present Europol Council Decision. He strongly recommends clearly defining a specific purpose for each operational analysis case and requiring that only relevant personal data shall be processed according to the defined specific purpose. Article 24(1)(c) should be amended accordingly.

48. In addition, as regards Article 24(1)(c) of the Proposal, the EDPS understands that due to Europol's core activity (*i.e.* enhancing the information provided by Member States in order to provide additional knowledge on criminal activities) and the diversity of criminal offences and the composition of the criminal groups[42], there is a need for Europol to cross-match data received in the context of operational analysis. The EDPS recalls that under the principle of purpose limitation, personal data may not be further processed in a way incompatible with the purposes for which they have been collected (Article 34(b) of the Proposal). Compatibility needs to be assessed on a case by case basis taking into account all relevant circumstances including the relationship between purposes, the context of the collection and the safeguards applied by the controller. [43]

49. It should be added that in the law enforcement area further processing of data for a purpose considered incompatible with the initial one could be allowed, when it is strictly necessary, in a specific case. Since this could involve a privacy intrusive processing this should be accompanied by very strict conditions.[44]

50. Thus, the EDPS considers that cross-matching data collected for different purposes by Europol analysts requires specific safeguards. Therefore, he recommends adding in the Proposal the following elements: (i) all cross-matching operations by Europol analysts shall be specifically motivated, (ii) retrieval of data following a consultation shall be limited to the strict minimum required and specifically motivated, (iii) traceability of all operations related to the cross-matches shall be ensured, and (iv) only authorised staff in charge of the purpose for which the data were initially collected may modify that data. This would be in line with the current practice within Europol.

[42] See above, point 42.
[43] See Opinion of Opinion 03/2013 of 2.04.2013 of Article 29 Data Protection Working Party on purpose limitation, 39 Section II.2.1, available on the WP29 website at the following address: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion.
[44] Opinion of the EDPS 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.

51. The EDPS considers that the above recommendations are essential to ensure a level of data protection at least as high as in the Europol Council Decision.

b) Strengthening data protection supervision

Introductory remarks

52. The EDPS welcomes the provisions on supervision that foresee a strong architecture for supervision on data processing. Due account is taken of the responsibilities at national level and at EU level, and a system is laid down for coordination between all involved data protection authorities, based on experience and on existing, tried and trusted mechanisms. The comments of the EDPS in this part are designed to further strengthen these mechanisms.

53. The strengthening of the supervision mechanisms is necessary in light of the growing roles of Europol. The extended powers of Europol envisage a clear development of data processing activities, including information processed at EU level that does not directly originate from national authorities. Moreover, Europol is now an EU body: it will need to be fully aligned with the other EU agencies and its activities will fall under the jurisdiction of the Court of Justice of the European Union.

54. In this context, the EDPS welcomes the recognition in the Proposal of the EDPS' role as the authority established to supervise all the EU institutions and bodies. In consequence, Article 46 assigns responsibility for supervising Europol to the EDPS, including the role of advising Europol and data subjects on all matters relating to data processing. This will secure a consistent and effective approach to supervision at EU level.

55. In this respect, Article 45 of the Proposal recognises that supervision of the processing operations foreseen in the Proposal is a task that also requires the active involvement of national data protection authorities[45]. Cooperation between the EDPS and national supervisory authorities is crucial for effective supervision in this area. Article 47 therefore builds on the existing structure of cooperation in related areas of EU law, such as the Schengen Information System (2nd generation), Eurodac and the Visa Information System. Experience shows these structures are efficient because they encourage close cooperation between the national supervisory authorities and the EDPS. This cooperation will be even more important in the present case, because EDPS supervision of processing will not only focus on the technical infrastructure[46] but also on the substance of the data.

[45] See also Resolution 4 of the Spring Conference of European Data Protection Authorities (Lisbon 16-17 May 2013).
[46] This is the case for the information systems mentioned above,

56. Indeed, the EDPS takes the view that the provisions on supervision and cooperation in supervision could well be a model for the proposal of the Commission for data protection at EU level announced in the data protection reform.[47]

57. Finally, the EDPS welcomes Article 48 of the Proposal that provides that Regulation (EC) No 45/2001, including the provisions on supervision, is fully applicable to staff and administrative data.

a) Effective supervision for Europol

58. In view of its activities, Europol needs effective supervision, in terms of independence, expertise and enforcement tools.

59. Independent and effective supervision is an essential component of the protection of individuals with regard to the processing of personal data at national and European level enshrined in Article 8 of the Charter of Fundamental rights and Article 16 TFEU. The Court of Justice has recognised that the EDPS meets all the criteria of independence established by the Court as concerns data protection supervisory authorities, and indeed has employed the EDPS as a benchmark in this respect[48].

60. Moreover, after the end of the transitional period under Article 10 of Protocol 36 to the Lisbon Treaty[49], a natural or legal person will be able to request the Court of Justice for judicial remedies against Europol's acts, including data protection[50]. The same judicial framework should apply to any decisions adopted by the authority supervising Europol, as is also the case with the EDPS[51].

61. The Proposal grants broad investigative and enforcement powers to the EDPS, ranging from offering advice to delivering warnings and imposing bans on processing (see points 68-69 below), which will ensure a strengthened and effective supervision of Europol[52].

b) Role of national data protection authorities

62. The EDPS welcomes Article 45 of the Proposal. This states that data processing by the national authorities and the way they interact with Europol is subject to national supervision, and thus reflects the key role of national supervisory authorities. He

[47] See Communication from the Commission entitled "A comprehensive approach on personal data protection in the European Union", COM(2010)609 final, pp. 18-19 and point 15 above.
[48] See Case 518/07, *Commission v. Germany,* i.e. point 30: '(...) *supervisory authorities* (...) *must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data.*") and Case 614/10, *Commission v. Austria* (i.e. point 43: '*The independence required (...) is intended to preclude not only direct influence, in the form of instructions, but also* (...) *any indirect influence which is liable to have an effect on the supervisory authority's decisions*.'.
[49] on 1 December 2014.
[50] See Recital 46 and Article 52 of the Proposal. See also Explanatory Memorandum, p. 9.
[51] See Article 32(3) of Regulation 45/2001 and Article 50 of the Proposal.
[52] See also Explanatory Memorandum, p.8.

also welcomes the strong emphasis on close cooperation and the requirement that the national supervisory authorities should keep the EDPS informed on any actions they take with respect to Europol.

c) Streamlined and consistent data protection supervision at EU level

63. Following the entry into force of the Lisbon Treaty, the area of police and judicial cooperation has lost its separate intergovernmental status and has become part of the Community method. Europol, as one of the former 'third pillar bodies' has become an EU agency. Therefore, Europol, in terms of data protection supervision, should be treated in the same way as other EU entities, some of which also process law enforcement-related data (OLAF, Frontex and EU Lisa, the new IT Agency playing a key role in the management of large scale information systems).

64. Moreover, the nature of the processing by Europol is significant. Europol not only stores data originating from the Member States, but also actively processes those data for the purpose of its own activities and uses other data that do not originate from national authorities but from other sources interacting directly with Europol (other EU bodies, third parties outside the EU, etc.). Hence, processing by Europol itself at EU level should be consistently supervised at EU level.

65. Finally, taking into account that Europol exchanges data with other EU bodies, it is necessary to ensure consistency and an equal level of protection of the data processing by these other bodies. This requires that these EU entities are subject to the same harmonised and coherent system of comprehensive supervision.

d) Supervision by the EDPS

66. In view of the above, Article 46 provides for streamlined and consistent data protection supervision at EU level by the EDPS. The EDPS supervises the other 60 plus institutions, bodies and agencies active over the whole range of EU policy, with solid experience in supervising EU bodies and agencies that process data in the law enforcement area, such as Frontex and OLAF.

67. The EDPS welcomes Recital 32 of the Proposal, which states that data protection rules at Europol should be strengthened and draw on the principles underpinning Regulation (EC) No 45/2001, and Article 46 of the Proposal, granting the EDPS similar duties and powers to those enjoyed under Regulation (EC) No 45/2001.

68. In this respect, the supervisory role of the EDPS is exercised through various tools, such as prior checks, consultations, complaint handling, visits and inspections[53]. The EDPS has the power to obtain access to all personal data and to all information necessary for his enquiries and to obtain access to any premises in which the EU body carries on its activities[54]. If necessary, a number of formal enforcement actions are available to the EDPS. In particular there are powers to order the rectification,

[53] These supervision tools, investigative and enforcement powers are described in the EDPS policy paper on "Monitoring and Ensuring Compliance with Regulation (EC)45/2001" of 13 December 2010 (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/10-12-13_PP_Compliance_EN.pdf).
[54] Article 47(4) of the Proposal.

blocking, erasure or destruction of data that would be processed in breach of the Proposal[55]; to warn or admonish the controller-EU body[56]; to impose a temporary or definitive ban on the processing[57]; and to refer a matter to the EU Court of Justice[58].

69. Some of these powers, like the power under Article 46 (3)(f) to impose a temporary or definitive ban on processing, are meant as an ultimate sanction and will not be imposed lightly, particularly because of their possible repercussions on the tasks of Europol. However, an effective system of supervision needs strong enforcement tools to be available so as to have a strong preventive effect. Moreover, the use of these powers by the EU supervisory authority will always be subject to judicial review before the Court of Justice.

e) Cooperation between the EDPS and national authorities

70. The Proposal ensures that all EU entities, including Europol, are subject to consistent and comprehensive supervision. In addition, it takes into account the close relationship between the EU and Member States in Europol's tasks and the fact that many of the data processed at Europol originate from the Member States. This requires the legal framework to provide the necessary arrangements for coordinated approaches, to ensure that supervisory activities at all levels are coordinated effectively by way of strong cooperation mechanisms.

71. In this respect, the legal framework for Europol should clearly define the responsibilities of the different supervisory authorities for the different elements of the system, ensuring full accountability and legal certainty.

72. The result should be a fully consistent approach at all the different levels. Consistency calls for an appropriate - and where necessary close - cooperation between the EDPS and the national supervisory authorities and for a consistent approach among the EU and various national processing operations.

73. The EDPS therefore welcomes Article 47 on cooperation and coordination with the national supervisory authorities, which are essential to ensure a consistent application of the Proposal throughout the EU, as highlighted in Recital 42[59].

74. This cooperation and coordination has additional advantages, namely the optimal use of resources and the benefit of accumulated expertise. Consistent supervision will permit the EDPS to build on the experience gained under coordinated supervision and can take advantage of all accumulated knowledge both at national and EU sides. This could be achieved by staff exchanges, secondment of national experts to the EDPS, and participation of national experts in EDPS' inspections. In this respect, the EDPS welcomes the provision in Article 47(2) for the exchange of relevant information, mutual assistance in carrying out audits and inspections, the

[55] Article 46(3)(e) of the Proposal.
[56] Article 46(3)(d) of the Proposal.
[57] Article 46(3)(f) of the Proposal.
[58] Article 46(3)(h) of the Proposal.
[59] Recital 42 states: *'The European Data Protection Supervisor and national supervisory authorities should co-operate with each other on specific issues requiring national involvement and to ensure coherent application of this Regulation throughout the Union'*. See also Explanatory Memorandum, p. 9.

studying of problems relating to the exercise of independent supervision or the exercise of the rights of data subjects, the development of harmonised proposals for joint solutions to any problems, and the promotion of awareness of data protection rights.

75. Article 47(3) regulates the coordination meetings between national supervisory authorities and the EDPS. The EDPS welcomes this provision and its presumption of cooperation based on needs. The current wording leaves room for sufficient flexibility. For instance, it provides both for meetings with all national authorities, and, where more appropriate and cost effective, for additional meetings with a smaller and more targeted attendance. This approach can be further developed in the rules of procedure mentioned in the provision.

76. In order to ensure efficient cooperation, the EDPS suggests clarifying in Article 47 that the cooperation envisaged includes both bilateral and collective cooperation. In addition a recital should further emphasise the importance of cooperation between the different supervisory authorities and provide examples of how such cooperation could be best enhanced.

c) Transfer of personal data

Definition

77. The Proposal (Article 2(l)) defines the transfer of personal data as 'the communication of personal data, actively made available, between a limited number of identified parties, with the knowledge or intention of the sender to give the recipient access to the personal data'.

78. The Proposal allows Europol to exchange a significant amount of personal data with competent authorities at national, EU and international level, which may include direct access to data held by Eurojust, OLAF and the Member States. The EDPS welcomes the addition of a definition of transfer[60] that regulates not only deliberate transfers of personal data ('push' systems) but also data access provided to the recipient ('pull' system). He also calls the attention of the EU legislator to the fact that consistency with the future general data protection Regulation should be ensured as far as the definition of transfer is concerned[61].

Direct and indirect access by Member States and by OLAF and Eurojust

79. Article 26 of the Proposal provides for Member States to have (i) direct access to information stored by Europol for the purposes of cross-checking aimed at identifying connections between information and of analyses of a strategic or thematic nature and (ii) indirect access to the same information on the basis of a hit/not hit system for the purpose of operational analyses in specific cases. In the case of a hit, Europol shall initiate the procedure by which the information that

[60] See No. 108-109 of the Opinion of the EDPS on the data protection reform package of 7 March 2012.
[61] The proposed DP Regulation does not contain any definition of transfer. Such a definition is inserted as Amendment No. 86 in the Draft Report of the LIBE Committee of the European Parliament on this proposal, the wording of which is similar to the one contained in Article 2(l) of the Proposal.

generated the hit may be shared. Article 27 of the Proposal provides for similar rules regarding direct and indirect access to Europol information by OLAF and Eurojust.

80. In view of the broad access provided to the Member States and OLAF/Eurojust by the Proposal, a particular attention should be paid to data quality. Therefore, the EDPS recommends inserting a sentence in Article 26(1) of the Proposal laying down that the competent authorities of the Member States may access and search information on a need-to-know basis and to the extent necessary for the legitimate performance of their tasks.

81. Moreover, the EDPS recommends that the provisions of Article 26(2) further require that, in case of a hit, (i) the competent authorities of the Member State should specify which data they need and (ii) Europol may share the data with the authorities in question only to the extent that the data that generating the hit are necessary for the legitimate performance of their tasks. Similar changes should be made to Article 27(1) and 27(2) regarding access by OLAF and Eurojust. Equally, an obligation to log access should be included.

82. Article 26(2) provides that in case of a hit, Europol shall initiate the procedure by which the information that generated the hit may be shared, 'in accordance with the decision of the Member State that provided the information to Europol'. However, as mentioned in Article 26(1) of the Proposal, the information to be shared may originate from Member States, Union bodies, third countries or international organisations. Therefore, Article 26(2) should be amended accordingly, and aligned with Article 27(2) which specifies that Europol shall share the information in accordance with the decision of the Member State, Union body, third country or international organisation that provided that information to Europol.

Relations with partners

83. As stated before, the processing of information, including the exchange of personal data, is one of the main reasons for the existence of Europol. It is also evident that the data which Europol exchanges are quite often of an extremely sensitive nature since they deal with the (possible) implication of individuals with criminality.

84. The EDPS welcomes the inclusion of Chapter VI of the Proposal on the relations with partners, and in particular that it includes provisions that regulate transfers to Union bodies, third countries and international organisations.

85. In an increasingly connected world, effective police and judicial cooperation within EU borders depends more and more on cooperation with third countries and international organisations. The development of such international cooperation is likely to rely heavily on exchanges of personal data, which is complex due to the fact that information will be exchanged also with countries that do not guarantee a high level of personal data protection. It is therefore all the more important for the EU to develop these exchanges in full respect for human rights, including privacy and data protection. A system for the exchange of personal data with third countries has to find a fair balance between the need for effective law enforcement and the need for sound protection of personal data.

86. The EDPS therefore welcomes that, in principle, transfer of personal data to third countries and international organisations can only take place on the basis of adequacy or a binding agreement providing adequate safeguards. A binding agreement should ensure legal certainty as well as full accountability of Europol for the transfer. In any event, in principle, a binding agreement should always be used in case of massive, structural and repetitive transfers[62].

87. From time to time there will be situations in which a legally binding agreement cannot be obtained. Those situations should be exceptional based on real necessity in limited cases, and they should be supported by strong safeguards - substantial as well as procedural.

Common provisions (Article 29)

88. Article 29 of the Proposal provides for common provisions on the exchange of information between Europol, EU bodies, third countries, international organisations and third parties. When the data to be transferred have been provided by a Member State, Europol should seek the Member State's consent, unless:
    - the authorisation can be assumed as the Member State has not expressly limited the possibility of onward transfers;
    - the Member State has granted its prior authorisation to such onward transfer, either in general terms or subject to specific conditions, knowing that such authorisation may be withdrawn at any moment.[63]

89. The EDPS considers that Member State's consent for the transfer of personal data should be explicit and cannot be 'assumed' as presently provided under Article 29(4)(a) of the Proposal. Member States should limit the transfer at the time they provide the data to Europol. If they do not mention any restriction at that time, they should at least be given the possibility to object or formulate restrictions before the transfer is made. Consent at that stage would also be useful to ensure data quality and accuracy of data. Therefore, the EDPS strongly recommends removing the possibility for Europol to assume Member States' consent by deleting Article 29(4)(a). The EDPS also advises adding that the consent should be given 'prior to the transfer', in the second sentence of Article 29(4).

90. Finally, in view of the sensitive nature of the transfer operations and although Article 29(5) of the Proposal prohibits any onward transfer without Europol's explicit consent, the EDPS recommends adding that data shall be transferred only if the recipient - either a EU body or a third country or international organisation - gives an undertaking that the data shall be used for the sole purpose for which they were transmitted[64]. The EDPS also recommends adding to Article 29 a paragraph requiring that Europol should keep detailed records of the transfers of personal data as well as of the grounds for such transfers, in line with Article 44(2)(b) of the Proposal (see point 148 below).

[62] See Working Document of the Article 29 Working Party of 24 July 1998 on "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" (WP12).
[63] Article 29(4) of the Proposal.
[64] This requirement is included in Article 24(2) of Europol Decision.

Transfers to EU bodies (other than Eurojust and OLAF) (Article 30)

91. Article 30 of the Proposal allows Europol to directly transfer personal data to Union bodies in so far as it is necessary for the performance of Europol's tasks or of those of the recipient Union body and subject to any possible restrictions stipulated by the Member State, Union body, third country or international organisation that provided the information in question.

92. This provision, read in connection with Article 41(5) of the Proposal, is in line with Article 7 of Regulation (EC) No 45/2001 that deals with data transfers within or between Union bodies[65]. Since transfers to OLAF and Eurojust[66] are already dealt with in Article 27 of the Proposal, the EDPS recommends, for the sake of clarity, adding in Article 30 that the latter applies without prejudice to Article 27.

93. Finally, for the sake of transparency, the EDPS recommends that Europol makes public the list of the EU institutions and bodies with whom it shares information, by posting such a list, regularly updated, on its website. Article 30 of the Proposal should be amended accordingly.

Transfer to third countries and international organisations (Article 31)

94. The EDPS welcomes Article 31 setting up strong rules regarding the transfer of personal data to third countries and organisations.

95. As a general rule, Article 31(1) of the Proposal provides that a transfer may take place only where the Commission has decided that the third country or international organisation ensures an adequate level of protection. If there is no adequacy decision, the transfer may take place only on the basis of a binding agreement between the EU and the third country or international organisation. This agreement must adduce adequate safeguards with respect to the protection of privacy as well as fundamental rights and freedoms of individuals.

96. The EDPS welcomes the inclusion of the adequacy principle as the basis for international transfers. He also welcomes the reference to the need to adopt adequate safeguards of a binding nature when no adequacy decision has been adopted. These adequate safeguards, as data protection guarantees which are created *ad hoc*, should include the core elements described by the Article 29 Data Protection Working Party in the framework of the adequacy assessment of third countries[67]. The EDPS suggests adding to Article 31(1) *in fine* that he should be consulted in a timely manner during the negotiation of any international agreement between the EU and a third country or an international organisation, and in particular before adoption of the negotiating mandate as well as before the finalisation of the agreement.

97. Besides the conclusion of future international agreements, Article 31(1)(c) of the Proposal states that Europol may also transfer personal data to authorities of third

[65] See however point 143 below EDPS' comments on Article 41(5) of the Proposal.
[66] Including access (See definition of transfer in Article 2(l) of the Proposal).
[67] See Working Document of the Article 29 Working Party of 24 July 1998 on "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" (WP12). Restrictive interpretation of an exception to data protection is also in line with case law of the CJEU. See also Opinion of 7 March 2012 on the data protection reform package, §§ 224 and fol., 417.

countries or to international organisations on the basis of existing international cooperation agreements concluded with these countries and organisations prior to the entry into force of the Proposal. The EDPS recommends adding to the Proposal a transitional clause regarding already existing cooperation agreements regulating personal data transfers by Europol. This clause should provide a deadline for the review of these agreements within a reasonable time in order to align them with the requirements of the Proposal. This clause should be included in the substantive provisions of the Proposal, with a deadline of no longer than two years after the entry into force of the Proposal[68].

98. For the sake of transparency, the EDPS also recommends adding at the end of Article 31(1) that Europol shall make publicly available the list of its international and cooperation agreements with third countries and international organisations, by posting this list, regularly updated, on its website.

Derogations and ad hoc instruments

99. Article 31(2) of the Proposal provides for derogations to the adequacy and adequate safeguards requirements of Article 31(1) in a number of specific circumstances. In this context, the EDPS notes that Recital 29 erroneously refers to an additional derogation (data subject's consent) that is not mentioned in Article 31(2). Hence, the words 'if the data subject has consented' should be deleted from Recital 29.

100. The EDPS welcomes the fact that Article 31(2) states that these derogations, as a justification for a transfer without any prior authorisation from the EDPS, must be used on a case by case basis (see however point 102 below)**.** The EDPS would however recall that the use of any derogation as a justification for a transfer should be interpreted restrictively and be valid only for occasional transfers that cannot be qualified as frequent, massive or structural[69]. For the avoidance of doubt, the EDPS recommends adding expressly in Article 31(2) that derogations may not be applicable to frequent, massive or structural transfers, in other words for sets of transfers (and not just for occasional transfers).

101. Moreover, the current wording of the derogations referred to in Article 31(2) (a), *i.e* transfers necessary to safeguard the '*essential interests'* of a Member State, and Article 31(2)(c) transfers required on '*important public interests grounds*' are too vague. Article 31 should mention that this exception can only be used if the transfer is of interest to the authorities of the EU or of the Member States, and not only to one or more public authorities in the third country or to an international organisation[70]. As regards the derogation of public interest, Article 31 should at least require that this public interest is recognised in Union law or in national law of a Member State of the European Union.

102. Besides the use of derogations on a case by case basis, Article 31(2) *in fine* of the Proposal provides for the authorisation of "a set of transfers". This provision

[68] See also No. 217 of EDPS opinion of 7 March 2012 on the Data Protection Reform Package.
[69] See p. 7 of Working document of the Article 29 Working Party of 26 November 2005 on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP114).
[70] See p. 15 of the Working document of the Article 29 Working Party of 26 November 2005 on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (WP114).

does not respect the principle that derogations/exceptions should be limited to occasional transfers.

103. It would be highly undesirable to permit Europol to make significant transfers to a third country or an international organisation that is not recognised as ensuring adequacy, without providing an appropriate framework for the transfer, through the adoption of a binding instrument containing adequate safeguards (see point 86 above). The EDPS acknowledges that in certain cases, it may not be possible in practice to adopt 'adequate safeguards' in the form of a 'binding instrument' between the EU and the third country or international organisations in question[71]. The Proposal should limit these exceptional cases where there is neither adequacy nor an international agreement in place, or likely to be concluded, with the country or international organisation of destination and where the derogations described could not be applicable because the transfers are frequent, massive or structural (see point 100 above).

104. In such cases, and only where it is impossible to obtain a binding agreement, another type of protective instrument *ad hoc* should be considered[72]. This *ad hoc* instrument should be tailored to the specific elements of the transfers envisaged, such as the size and number of envisaged data transfers, the type of data (whether they concern special categories of data subjects or not) and the quality of the recipient. Irrespective of the type of instrument adopted and its non-binding nature, an *ad hoc* instrument should include a description of the data protection principles that should be respected by Europol and the importer-recipient authority, together with the means put in place to ensure supervision of compliance and enforcement (necessary mechanisms to make this protection effective). Europol should be accountable for compliance with the data protection requirements of the instrument in question. Therefore, in the event that an EU data subject were to suffer any harm as a result of a data transfer covered by an *ad hoc* instrument, Europol should bear ultimate liability and the costs of any damages resulting from the acts and omissions from the recipient. Finally, the use of such a non-binding instrument should always be subject to prior authorisation by the EDPS.[73]

105. In the light of the above, the EDPS recommends providing a specific paragraph dedicated to transfers authorised by the EDPS. This paragraph, which should logically precede the paragraph on derogations (see point 99 above), should provide that the EDPS may authorise a transfer or a set of transfers where Europol adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals, and as regards the exercises of the corresponding rights. In addition, this authorisation may be granted prior to the transfer / set of transfers, for a period not exceeding one year, renewable.

106. Furthermore, if Article 31 (2) *in fine* were to remain in the text, the EDPS has two recommendations relating hereto:

[71] As an EU agency, Europol may no longer conclude international binding agreements. as it used to do before the entry into force of the Lisbon Treaty.
[72] See also points 222-223 of the Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012, available at:
[73] See Article 9 (7) of Regulation 45/2001.

- transfers are authorised provided that Europol adduces 'safeguards', when Europol should adduce adequate safeguards, as referred to in Recital 29 of the Proposal,
- the authorisation is delivered by the Management Board 'in agreement with the EDPS', when the authorisation should be delivered (or not) by the EDPS alone, acting as the independent supervisory authority.

107. Finally, Article 31(3) of the Proposal states that Europol must inform the EDPS of cases where Article 31(2) is applied. To this effect, the EDPS recommends that any transfers based on derogations should be specifically documented (e.g. data transferred, time of transfer, data about the recipient, reason for the transfer, etc.).

SPECIFIC COMMENTS

Definition of administrative personal data (Article 2)

108. Article 2(o) of the Proposal defines 'administrative personal' data as 'all personal data processed by Europol apart from those that are processed to meet the objectives laid down in Article 3(1) and (2)'. The EDPS welcomes this definition as it makes a clear distinction between the personal data processed by Europol in the context of its administrative tasks ('administrative data') and the personal data processed for the fulfilment of its main tasks ('operational data'). This also clarifies the applicable legal framework to the processing of these data (*i.e* Regulation (EC) No 45/2001 for administrative personal data and the Proposal for operational data).[74]

109. Considering that the definition of administrative personal data includes Europol staff data, the EDPS suggests, for the sake of clarity, to delete the references to staff data in the title and the content of Article 48.

Tasks related to training for law enforcement officers (Articles 9-11)

110. Article 9(1) states that the Europol Academy will support, develop, deliver and coordinate training for law enforcement officers, in particular to raise awareness and knowledge on several issues referred to in the provision. Since the processing of personal data is a major activity of law enforcement authorities, the EDPS recommends including in Article 9(a) data protection as one of the issues to be dealt with in the training developed by the Europol Academy[75].

Functions of the Management Board and work programme (Articles 14 and 15)

111. The EDPS suggests including in Article 14 that the Data Protection Officer will be appointed by the Management Board and removing this point from Article 44. This will group all main Management Board functions in one Article. Also, adding the EDPS as a recipient of the annual activity report in Article 14(1)(d) and in Article 15. The EDPS should be provided a copy of Europol's annual work programme once it has been finalised and approved by the Management Board. Moreover, including in Article 14(1) that the Management Board shall ensure an

[74] See also points 154-155 below.
[75] See also points 164 to 166 below.

adequate follow-up to the findings and recommendations stemming from inspections carried out by the EDPS in the same manner as already described for internal or external audit reports, evaluations and for OLAF investigations in Article 14(1)(o).

Sources of information (Article 23)

Access to national, EU or international information systems

112. Article 23(3) of the Proposal allows Europol to access information systems of a national, Union or international nature - including by means of computerised direct access - insofar as authorised by Union, international or national legal instruments. The applicable provisions of such instruments shall govern the access and the use of that information insofar as they provide for stricter rules on access and use than those of the Proposal.

113. As regards access to national information systems, Article 7(5) of the Proposal already requires Member States to supply Europol with information and intelligence[76]. Therefore, the EDPS considers that access to national databases is not justified. Furthermore, direct access by Europol to national databases raises data protection and data security concerns. By providing a direct access to the data, there is a risk that the controller owning the data loses control of the transfer, in particular as regards the purposes of the transfer, the categories of data transferred as well as the conditions of the transfer. None the less, it remains responsible for the legality of the transfer and the accuracy of the data transmitted. The EDPS therefore recommends deleting the possibility for Europol to directly access national databases.

114. Where the access concerns EU information systems - in particular databases the initial purposes of which are not law enforcement purposes - the necessity and proportionality of such access should be demonstrated[77]. If sufficiently demonstrated, the law authorising the access should contain explicit and detailed provisions specifying at least (i) the objectives of the processing, (ii) the personal data to be processed, (iii) the purposes and means of processing, (iv) the appointment of the controller, and (v) the procedure to be followed for the processing of personal data.

115. In addition, access should only be granted on a hit/no hit basis (*i.e.* a positive or a negative answer). Any information related to the hit should be communicated to Europol after the explicit approval and authorisation of transfer by the Member State (if the access concerns data supplied by a Member State), the EU body or the international organisation and be subject to the assessment referred to in Article 35 of the Proposal. The EDPS recommends laying down these conditions in Article 23 of the Proposal.

[76] See also impact assessment which explicitly refers to the legal clarification that Member States are obliged to provide data to Europol (p. 21).
[77] See for instance EDPS opinions on VIS, Eurodac, PNR.

Determination of the purposes (Article 25)

116. Under Article 25 of the Proposal, Member States, Union bodies, third countries or international organisations shall determine the purpose for which the information they provide will be further processed. If it has not done so, Europol shall determine the relevance of such information as well as the purpose for which it shall be processed. According to the EDPS, the Member State, as the data controller, must always ensure compliance, *inter alia,* with the purpose limitation principle and transmit the personal data only for a specific and well defined purpose. In view of the above, the EDPS recommends deleting the last sentence of Article 25 according which Europol shall determine the purpose of the information provided by a Member State if the latter has not done so.

Different degrees of accuracy and reliability (Article 35)

117. The EDPS wishes to underline the importance of distinguishing the data according to their degrees of accuracy and reliability both for data subjects and for law enforcement authorities. This is in particular relevant when data are processed far from their source and completely out of the context in which they were originally collected and used. The failure to designate their degree of accuracy and reliability could actually undermine the effectiveness of data exchanges as the recipient would not be able to ascertain whether the data should be construed as 'evidence', 'fact', 'hard intelligence' or 'soft intelligence'. The data subject might also be disproportionately affected by the possible lack of accuracy in data relating to suspicions about him or her.[78]

118. In view of the above, the EDPS considers that Article 35 of the Proposal should be strengthened by making the assessment by the Member State providing the information mandatory. He suggests deleting in Article 35 (1) and (2) the wording 'as far as possible' and amending Article 36(4) accordingly.

119. Under Article 35(6) of the Proposal, Europol shall assess the information retrieved from publicly-available sources. The EDPS points out that these sources do not offer guarantees as to the quality of the data. Unless and as long as the accuracy of the information and the reliability of its source have not been corroborated by other reliable sources, Europol should attribute to such information or data the evaluation code (X) and (4) referred to in paragraphs 1 and 2. The EDPS recommends amending Article 35(6) accordingly.

Special categories of personal data and categories of data subjects (Article 36)

120. Article 36 of the Proposal provides for specific safeguards as regards the processing of special categories of data (*i.e.* data revealing racial or ethnic origin, political opinions, religion or beliefs, trade-union membership and data concerning health or sex life) and categories of data subjects (*i.e* victims of a criminal offence, witnesses or other persons who can provide information on criminal offences and persons under the age of 18).

[78] See EDPS' opinion of 7 March 2012 on the data protection reform package, points 355-358: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf

121. The special categories of personal data referred to in Article 36(1) are by their nature particularly sensitive and deserve specific protection.[79] The categories of data subjects mentioned in Article 36(2) are not supposed to be part of the common and usual processing carried out by Europol for the fulfilment of its core activities. The EDPS therefore welcomes that the Proposal foresees additional safeguards for the processing of both sensitive data and data related to specific categories of data subjects.

122. The EDPS welcomes in particular that (i) the processing of the above-mentioned data shall be prohibited unless strictly necessary (and additionally for the sensitive data that they supplement other data already processed by Europol) and that (ii) the access to these data is restricted to a limited number of Europol officials designated by the Executive Director. However, the EDPS considers that the existence of strict necessity should be duly justified. This is important to ensure an efficient supervision and also for Europol to demonstrate compliance with data protection rules in accordance with the principle of accountability (see points 161-163 below). The EDPS therefore recommends adding in Article 36(1) and (2), the terms 'and duly justified'.

123. Under Article 36(5), the transmission of sensitive data or specific categories of data subjects to Member States, Union bodies, third countries or institutional organisations shall be prohibited unless strictly necessary in individual cases concerning crimes that fall under Europol's objectives. The EDPS recalls that such transmission must be done in accordance with the rules laid down in Chapter VI of the Proposal. For the avoidance of doubt, he recommends adding this criterion in Article 36(5). In addition, in line with his comment on Article 36(1) and (2), he recommends adding in Article 36(5) after 'strictly necessary', the terms 'and duly justified'.

124. Finally, the EDPS notes that under Article 36(6) of the Proposal, Europol shall provide the EDPS with an overview of the sensitive data every six months. While the EDPS is entitled, as part of his mandate, to have access to personal data where necessary for the fulfilment of his supervisory tasks[80], this does not necessarily require knowing the details of all personal data that have been processed. The EDPS recommends replacing the overview of all personal data referred to in Article 36(2) by statistics on these data for each purpose. As the specific categories of data subjects referred to Article 36(1) also deserve a specific attention, the EDPS suggests including statistics on these data.

Time-limits for storage and erasure of personal data (Article 37)

125. Article 31 (1) mentions that personal data shall be stored by Europol only as long as necessary for 'the achievement of its objectives'. The EDPS considers that the criterion chosen to determine the retention period is too broad and should be limited to the purpose for which the data is processed. Therefore, the EDPS recommends replacing the terms 'for the achievement of its objectives' by 'the purpose for which data are processed'.

[79] See Convention No 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981 as well as Directive 95/46/EC.
[80] Article 47(2) of Regulation 45/2001.

126. The EDPS welcomes the specification in Article 31 of time limits for the storage and deletion of personal data and provides for a regular review of the data stored. In particular, he notes with satisfaction that:

(i) continued storage of personal data shall be justified and recorded and that in the absence of a decision of the continued storage, data shall be erased automatically;

(ii) if sensitive data and data related to specific categories of data subjects are stored for a period exceeding five years, the EDPS shall be informed accordingly;

(iii) situations where personal data shall not be erased in order to protect the interest of data subjects are enumerated.

Security of processing (Article 38)

127. The EDPS welcomes the safeguards in Article 38 that aims at ensuring a sufficient level of security to protect personal data against threats. However, appropriately securing personal data only is not sufficient: information that is not personal data may be used to compromise automated data processing facilities, which could eventually lead to a compromise of security for personal data. For example, results of audits, risk assessments, security incident reports, reports on technical vulnerabilities etc. typically do not contain personal data; however, knowledge of their content is of significant value for malicious people looking to compromise facilities or gain additional information that may include personal data.

128. Furthermore, the EDPS recommends specifying in Article 38(1) that Information Risk Management practices shall be used on order to define the appropriate technical and organisation measures to implement in order to protect all Europol data, taking into account all data protection needs. It should be laid down that proper Information Risk Management practices are used, based on (i) recognised international standards and regular reviews of all analysis performed in that context and (ii) monitoring and review of all technical and organisational measures implemented in this context. Additionally, for reasons explained in the previous paragraphs, the goals listed in Article 38.2 should be reviewed in order to cover all data.

129. The EDPS welcomes the collaboration between Europol and Member States mentioned in Article 38.3 in order to tackle security across information system boundaries. In addition to Article 7.9, the EDPS would welcome specifying in Article 38.3 that collaboration between Europol and Member States covers Information Risk Management.

Data subjects rights (Articles 39 and 40)

130. First, the EDPS would highlight that transparency is a crucial part of data protection, not only because of its inherent value but also because it enables other data protection principles to be exercised. Individuals are only able to exercise their rights if they know about the processing of their data. This is even more important in the law enforcement area, where the use of personal data inevitably has an enormous impact on the lives and freedoms of private individuals. Therefore, the EDPS recommends including in the Proposal a requirement that Europol must adopt a transparent and easily accessible policy explaining its processing of personal data

and the means availablefor the exercise of the data subjects' rights. This should be in an intelligible form, using clear and plain language. The provision should also state that this policy should be easily available on Europol's website and on the websites of the national supervisory authorities.

131. Articles 39 and 40 of the Proposal deal with data subjects' rights of information, access, rectification and erasure. The EDPS welcomes these provisions since they provide for a set of rights for data subjects while taking into account the particular nature of processing by law enforcement and judicial authorities.

132. Article 39(1) of the Proposal specifies the information to be communicated to the data subject. The EDPS recommends adding the following information:
- the period for which the data will be stored;
- the existence of the right to request from Europol rectification, erasure or restriction of processing of personal data concerning the data subject;
- any further information in so far as such further information is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are processed.

133. In addition, in order to ensure consistency with the applicable data protection rules under Regulation (EC) No 45/2001 and with the rules foreseen in the Reform Package, the EDPS suggests adding the right for the data subject to obtain from Europol a copy of the data undergoing processing.

134. The Proposal provides that the right of access is exercised through a request to the authority appointed for this purpose in the Member State of the data subject's choice, that will then refer the request to Europol within one month of receipt[81]. Europol must answer the request within three months of receiving it[82]. In order to avoid any confusion regarding the two time-limits mentioned above, the EDPS suggests mentioning expressly that Europol must answer the request within three months of its receipt of the request from the national authority.

135. Under Article 39(2) of the Proposal, any data subject wishing to exercise the right of access may make a request to that effect "*without excessive costs*". By contrast, Article 13 of Regulation (EC) No 45/2001 states that the data subject should be able to exercise its right 'without constraint' and 'free of charge'. For the sake of consistency, the EDPS recommends deleting '*without excessive costs*' from the provision.

136. The Proposal provides that Europol must consult the competent authorities of the Member States concerned by the access of the data subject to such data, and if a Member State objects to Europol's proposed response, it shall notify Europol of its objection[83].

137. Article 39(6) of the Proposal mentions that information on the factual and legal reasons on which Europol's decision on the right of access is based may be omitted where the provision of such information would deprive the grounds for restriction imposed by Article 39(5) of their effect. In such case, the EDPS recommends

[81] Article 39(2) of the Proposal.
[82] Article 39(3) of the Proposal.
[83] Article 39(3) and (4) of the Proposal.

requiring that Europol documents the grounds for omitting the communication of the factual or legal reasons on which the decision is based. More generally, if the provision of information in response to a request of access is refused, the Proposal should provide that Europol shall notify the data subject that it has carried out checks without giving any information which might reveal to him or her whether or not personal data concerning him or her are processed by Europol.

138. As far as the right to rectification, erasure and blocking is concerned, Article 40 (4) states that if data to be rectified, erased or blocked held by Europol have been provided to it by third countries, international organisations or are the result of Europol's own analyses, Europol shall rectify, erase or block such data. In line with the sharing of responsibilities provided in Article 41 of the Proposal, Europol should also be charged with the rectification, erasure and blocking of data provided by other EU bodies.

139. In Article 40(6) of the Proposal, it is not clear what is referred to by 'incorrect data transferred *by another appropriate means*'. This should be clarified.

140. Finally, Article 40 the Proposal should also mention the grounds and conditions for restricting right to rectification, erasure and blocking in the same way as for the right of access.

Responsibility in data protection matters (Article 41)

141. Article 41 determines the allocation of responsibilities in data protection matters. The EDPS considers that it does not clearly define the responsibility of all parties involved. With regard to Article 41(4), it should be made clear that the responsibility for compliance with all applicable data protection principles (and not only the 'legality of the transfer') lies with the sender of the data. The EDPS recommends amending Article 41 accordingly.

142. With regard to Article 41(2), the EDPS notes that, while Member States are considered responsible for the quality of the data they provide, Europol is considered responsible for data provided by EU bodies. The EDPS recommends for reasons of consistency that EU bodies are made responsible for the quality of the data until and including the moment of the transfer.

143. Article 41(5) of the Proposal establishes the respective responsibilities of Europol and the recipient EU body when the data are transferred following a request from the recipient. However, in line with similar requirements contained in Article 7 of Regulation (EC) No. 45/2001, the EDPS recommends adding the following specifications:
- Europol must verify the competence of the recipient and make a provisional evaluation of the necessity for the transfer of the data;
- if doubts arise as to this necessity, Europol shall seek further information from the recipient;
- the recipient shall ensure that the need for the transfer of the data can be subsequently verified;
- the recipient shall process the personal data only for the purposes for which they were transmitted.

Article 41(5) should be amended accordingly. It should also be ensured that exchanges with Eurojust and OLAF under Article 27 of the Proposal are covered.

Prior checking (Article 42)

144. Article 42 of the Proposal provides the intervention of the EDPS by way of a prior check notification by Europol on the processing of operational personal data that will form part of a new filing system to be created, where:
- the processing of personal data involves special categories of data referred to in Article 36(2), *i.e* data revealing racial or ethnic origin, political opinions, religion or beliefs, trade-union membership, and data concerning health or sex life;
- the type of processing, in particular using new technologies, mechanisms or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.
By contrast, administrative personal data[84] are subject to the prior checking procedure provided by Article 27 of Regulation (EC) No 45/2001 (see point 57 above).

145. The EDPS welcomes the requirement of prior checking, notably when the type of processing presents specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects[85].

146. The Proposal invites every 'new filing system' to be prior checked. As already mentioned (see points 35-36 above), the Proposal focuses on purposes for which the data have been provided rather than pre-defined filing systems. The EDPS points out therefore that it is not the system itself but its use for a single or several related purposes that will determine whether or not a prior check is required. In view of this evolution, there is no need to refer to "filing systems" as a trigger for prior checking. Instead, Europol should file a prior check notification with the EDPS for any set of processing operations that serve a single purpose or several related purposes in relation to its core activities, to the extent that these processing operations fall within the scope of the prior checking requirements. Therefore, the EDPS recommends modifying Article 42 in this sense.

Data Protection Officer (Article 44)

147. The EDPS welcomes not only that the data protection officer (DPO) is directly appointed by the Management Board, but also the other provisions of Article 44 of the Proposal aiming at ensuring the independence of the DPO, such as the fact that he/she will act independently, may only be dismissed with the consent of the EDPS, and may not receive any instructions with respect to the performance of his or her duties.

148. The EDPS also values the obligation for the DPO to ensure a specific record of the transfer and receipt of personal data (Article 44(7)(b)). The EDPS suggests that this specific record is part of the register of processing operations carried out by Europol (see point 151 below).

[84] Administrative personal data are defined in Article 2(o)of the Proposal as 'all personal data processed by Europol apart from those that are processed to meet the objectives laid down in Article 3(1) and (2)'. See points 108-109 above.
[85] Article 42(1)(a) of the Proposal.

149. Article 44(8) provides that the DPO shall carry out the functions laid down by Regulation (EC) No 45/2001 with regard to 'personal data of Europol staff members as well as administrative personal data'. As the definition of administrative personal data[86] includes Europol staff data, the EDPS recommends, for the sake of consistency, to refer in this provision to administrative personal data only.

150. The DPO's task to ensure lawfulness and compliance with the provisions of the Proposal concerning the processing of personal data is without prejudice to Europol's obligation to comply with the obligations incumbent upon it. The EDPS therefore recommends modifying Article 44(7)(a) by replacing the words 'ensuring, in an independent manner, *lawfulness and compliance with* the provisions of this Regulation concerning the processing of personal data' by 'ensuring, in an independent manner, *the internal application* of the provisions of this Regulation concerning the processing of personal data'.

151. As already mentioned (see point 149 above), the DPO shall carry out the functions foreseen by Regulation (EC) No 45/2001 with regard to administrative personal data. Concerning Europol's core data processing activities (operational data), the DPO's tasks are described in Article 44(7) of the Proposal. In order to ensure consistency of the DPO's tasks regarding both administrative and operational data, the EDPS recommends adding the following tasks in Article 44(7):
- keeping a register of all processing operations carried out by Europol, containing sufficient information (purpose(s) of the processing, description of the categories of data subjects and of the data, recipients, time limits for blocking and erasure, transfers to third countries or international organisations, security measures);
- notifying the EDPS of the processing operations referred to in Article 42 (prior checking)[87].

152. The DPO should be given the means for monitoring the incidents affecting personal data. This would allow him/her to identify the main security issues and areas of improvement, in cooperation with the security team. Thus, the EDPS suggests adding in Article 44(7) the task of keeping a register of such incidents affecting both operational and administrative personal data.

153. Article 44(9) provides that in the performance of his or her tasks, the DPO shall have access to all the data processed by Europol and to all Europol premises. Article 44(11) grants the same access to the DPO staff members to the extent necessary for the performance of their tasks. The EDPS suggests adding in both articles that such access is possible at any time and without prior request.

Administrative personal data and staff data (Article 48)

154. Considering that the definition of administrative personal data includes Europol staff data, (see points 108-109 above), the EDPS suggests, for the sake of clarity, to delete the references to staff data in the title and the content of Article 48.

[86] Article 2(o) of the Proposal defines the administrative personal data as the 'personal data processed by Europol apart from those that are processed to meet the objectives laid down in Article 3(1) and (2)'
[87] Regarding prior checking, see comments above under points 144-146.

155. In addition, in order to avoid any confusion as regards the scope of the Proposal, the EDPS recommends mentioning expressly in Article 48 that Regulation (EC) No 45/2001 shall apply to all administrative personal data to the exclusion of the provisions of the Proposal.

Right to lodge a complaint with the EDPS (Article 49)

156. Article 49 of the Proposal provides for the right of any data subject to lodge a complaint with the EDPS regarding alleged breaches of the provisions governing the processing of personal data contained in the Proposal.

157. According to Article 49(2) of the Proposal, where a complaint relates to the exercise of the right of access (*i.e* refusal or restriction of access by Europol) or the right to rectification, erasure and blocking (*i.e* refusal of restriction, erasure or blocking by Europol), the EDPS shall consult the national supervisory bodies or the competent judicial body in the Member State that was the source of the data or the Member State directly concerned. The EDPS' decision about the complaint shall be taken in close cooperation with the national supervisory authority or the competent judicial body.

158. The EDPS welcomes that Article 49(2) of the Proposal includes the cooperation of the national authorities and their close involvement in the EDPS' decision when the data at stake were provided by Member States. However, this provision does give rise to the following comments:

-Although the EDPS fully agrees to the need for consultation, he does not understand how the decision can be made 'in close cooperation'. In order to ensure legal certainty, including the data subject, it must be clear that the EDPS takes the decision subject to review by the Court of Justice, but that authorities of the Member States can not be co-decision makers. He suggests deleting the second sentence of Article 49 (2).

- The text should reflect the fact that more than one Member State may have provided data on the data subject or may be concerned by the communication of data to the data subject.

- It should be clarified that when the data at stake do not originate from Member States, the national authorities should not be consulted.

159. It is not clear whether Article 49(3) and 49(4) of the Proposal cover situations where a complaint relates to the exercise of the right of access or the right to rectification, erasure and blocking, or whether these provisions relate to complaints in general. In line with the sharing of responsibilities provided in Article 41 of the Proposal, these provisions aim at clarifying the scope of the EDPS' powers regarding complaints relating to Europol's data processing, depending on the origin of the data. In particular, if the complaint relates to data that originate from Member States, the EDPS shall cooperate with the national supervisory authorities to check whether the data processing at the level of the Member States concerned was lawful.

160. However, these provisions do not mention the processing operations of data generated by Europol itself, for example when it retrieved data from publicly available sources. They do not clearly state that although the national supervisory authorities need to be involved when the data at stake originate from a Member State, the EDPS is the only competent supervisory authority with regard Europol's

further processing of data, whatever their origin. Moreover, the reference to 'necessary checks' which need to be performed is unclear and insufficient. The EDPS' supervision powers provided by the Proposal (see Article 46) are not limited to ensuring that the 'necessary checks' have been carried out by the data controller. Therefore, Article 49(3) and (4) should be redrafted so as to clarify the issue raised by the EDPS.

The accountability principle

161. In the context of the data protection reform, the EDPS emphasised the need to reinforce the responsibility of data controllers. He also underlined that the new framework should contain incentives for data controllers to pro-actively include new tools in their business processes to ensure compliance with data protection (accountability principle)[88]. The EDPS therefore welcomed the introduction of general provisions on 'accountability' and 'privacy by design' in the proposed data protection Regulation[89].

162. As a general rule, the data controller must adopt policies and implement appropriate measures to ensure and be able to *demonstrate* compliance with the data protection rules, and to ensure that the effectiveness of the measures is verified. In this context, the proposed data protection Regulation introduces, amongst others, the principles of data protection by design and by default and the obligation for the controller to perform a data protection impact assessment before starting certain processing operations. The proposed data protection Directive contains a simplified version of the same principle.

163. For the sake of consistency with the data protection reform and to ensure that all the data protection requirements are taken into account, the EDPS recommends adding in substantive provision(s) of the Proposal that: (i) an impact assessment similar to what is described in the proposed DP Regulation shall be carried out for all processing operation on personal data,(ii) the principle of privacy by design and by default shall be applied for the creation of or improvement to systems processing personal data, (iii) the controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate compliance with the data protection rules, and to ensure that the effectiveness of the measures is verified, and (iv) the Europol DPO and, where necessary, the supervisory authorities, shall be included in all the key discussions surrounding the processing of personal data.

IV. COMMENTS ON THE COMMUNICATION

164. The Communication proposes a European Law Enforcement Training Scheme (hereinafter the 'Training Scheme') to equip law enforcement officers with the knowledge and skills they need to prevent and combat cross-border crime effectively through efficient cooperation with their EU colleagues. The Training

[88] See the EDPS Opinion of 14 January 2011 on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - 'A comprehensive approach on personal data protection in the European Union', paragraphs 99 to 117.
[89] See the EDPS Opinion of 7 March 2012 on the data protection reform package, point II.6.

Scheme aims *inter alia* to ensure that law enforcement cooperation instruments that the EU has developed over time (such as the Prüm information system[90] and Europol's criminal intelligence databases) are better known and used both in bilateral and multilateral contacts between Member States.

165. The Communication mentions that the Training Scheme should focus on improving knowledge, skills and competence across four strands from generic knowledge to highly specialised competencies. The first strand is the basic knowledge of the EU dimension of law enforcement and should include principles of effective law enforcement cooperation, fundamental rights, the role of Europol, Frontex and Eurojust and the use of EU information management tools and channels such as the 'Swedish Initiative'[91] and the 'Schengen Information System'. The EDPS emphasises that knowledge in this first strand should also include specific knowledge of data protection. This should be included in the Training Scheme.

166. Paragraph 5.5 defines the roles and responsibilities, and mentions a number of stakeholders that should play a role in the implementation of the Training Scheme. The EDPS is not mentioned, but is available to play a role in the implementation. In the Strategy 2013-2014 the EDPS has been positioned as a Centre of Excellence, with the task *inter alia* of raising awareness of data protection.[92]

V. CONCLUSIONS

General

167. The EDPS emphasises that the Proposal is of great importance from the perspective of processing of personal data. The processing of information, including personal data, is a principal reason for the existence of Europol, and the Proposal already contains strong data protection. This detailed opinion has therefore been adopted with the aim of further strengthening the Proposal.

168. The EDPS notes that the present Europol Decision provides for a robust data protection regime and considers that this level should not be lowered, independently of the discussions on the proposed data protection Directive. This should be specified in the recital.

169. The EDPS welcomes the fact that the Proposal aligns Europol with the requirements of Article 88 (2) TFEU, which will ensure that that the activities of Europol will benefit from the full involvement of all the EU institutions concerned.

170. The EDPS welcomes Article 48 of the Proposal that provides that Regulation (EC) No 45/2001, including the provisions on supervision, is fully applicable to staff and administrative data. However, he regrets that the Commission has not chosen to apply Regulation 45/2001 to Europol's core business and to limit the Proposal to additional special rules and derogations which duly take account of the specificities of the law enforcement sector. However, he notes that Recital 32 of the proposal explicitly mentions that data protection rules at Europol should be

[90] Council Decision 2008/615/JHA and Council Decision 2008/616/JHA, OJ, L 210, 06.08.2008.
[91] Council Framework Decision 2006/960/JHA, OJ L 386, 29.12.2006, p.89
[92] EDPS Strategy 2013-2014, available on EDPS Website.

strengthened and draw on the principles underpinning Regulation 45/2001. These principles are also an important reference point for the present opinion. .

171. The EDPS recommends specifying in the recitals of the Proposal that the new data protection framework of the EU institutions and bodies will be applicable to Europol as soon as it is adopted. In addition, the application of the data protection regime for EU institutions and bodies to Europol should be clarified within the instrument replacing Regulation (EC) No 45/2001, as first announced in 2010, in the context of the review of the data protection package. At the latest from the moment of the adoption of the new general framework, the main new elements of the data protection reform (i.e. accountability principle, data protection impact assessment, privacy by design and by default and notification of personal data breach) should also be applied to Europol. This should also be mentioned in the recitals.

New Europol information structure

172. The EDPS understands the need for flexibility in connection with the changing context, as well as in light of the growing roles of Europol. The existing information architecture is not necessarily the benchmark for the future. It is at the discretion of the EU legislator to determine the information structure of Europol. In his role of advisor to the EU legislator the EDPS focuses on the question to what extent the choice of the legislators is constrained by the principles of data protection.

173. In relation to Article 24 of the Proposal, he:
- recommends defining the notions of strategic, thematic and operational analysis in the Proposal and deleting the possibility to process personal data for strategic or thematic analysis, unless a sound justification is given.
- Recommends concerning Article 24(1)(c) clearly defining a specific purpose for each operational analysis case and requiring that only relevant personal data shall be processed according to the defined specific purpose.
- recommends adding in the Proposal the following elements: (i) all cross-matching operations by Europol analysts shall be specifically motivated, (ii) retrieval of data following a consultation shall be limited to the strict minimum required and specifically motivated, (iii) traceability of all operations related to the cross-matches shall be ensured and (iv) only authorised staff in charge of the purpose for which the data were initially collected may modify that data. This would be in line with the current practice within Europol.

Strengthening data protection supervision

174. Article 45 of the Proposal recognises that supervision of the processing operations foreseen in the Proposal is a task that also requires the active involvement of national data protection authorities[93]. Cooperation between the EDPS and national supervisory authorities is crucial for effective supervision in this area.

[93] See also Resolution 4 of the Spring Conference of European Data Protection Authorities (Lisbon 16-17 May 2013).

175. The EDPS welcomes Article 45 of the Proposal. This states that data processing by the national authorities is subject to national supervision, and thus reflects the key role of national supervisory authorities. He also welcomes the requirement that the national supervisory authorities should keep the EDPS informed on any actions they take with respect to Europol

176. The EDPS welcomes:

- the provisions on supervision that provide a strong architecture for supervision on data processing. Account is taken of the responsibilities at national level and at EU level, and a system is laid down for coordination between all involved data protection authorities

- the recognition in the Proposal of the EDPS' role as the authority established to supervise all the EU institutions and bodies.

- Article 47 on cooperation and coordination with the national supervisory authorities, but suggests clarifying that the cooperation envisaged includes both bilateral and collective cooperation. A recital should further emphasise the importance of cooperation between the different supervisory authorities and provide examples of how such cooperation could be best enhanced.

Transfer

177. The EDPS suggests inserting a sentence in Article 26(1) of the Proposal stating that the competent authorities of the Member States shall access and search information on a need-to-know basis and to the extent necessary for the legitimate performance of their tasks. Article 26(2) should be amended and aligned with Article 27(2).

178. The EDPS welcomes that, in principle, transfer to third countries and international organisations can only take place on the basis of adequacy or a binding agreement providing adequate safeguards. A binding agreement will ensure legal certainty as well as full accountability of Europol for the transfer. A binding agreement should always be needed for massive, structural and repetitive transfers. However, he understands that there are situations in which a binding agreement can not be required. Those situations should be exceptional, should be based on real necessity and only allowed for limited cases, and strong safeguards - substantial as well as procedural - are needed.

179. The EDPS strongly recommends deleting the possibility for Europol to assume Member States' consent. The EDPS also advises adding that consent should be given 'prior to the transfer', in the second sentence of Article 29(4). The EDPS also recommends adding in Article 29 a paragraph stating that Europol shall keep detailed records of the transfers of personal data.

180. The EDPS recommends adding to the Proposal a transitional clause regarding existing cooperation agreements regulating personal data transfers by Europol. This clause should provide for the review of these agreements within a reasonable

deadline in order to align them with the requirements of the Proposal. This clause should be included in the substantive provisions of the Proposal and contain a deadline of no longer than two years after the entry into force of the Proposal

181. For the sake of transparency, the EDPS also recommends adding at the end of Article 31(1) that Europol shall make publicly available the list of its international and cooperation agreements with third countries and international organisations, by posting this list, regularly updated, on its website.

182. The EDPS recommends adding expressly in Article 31(2) that derogations may not be applicable to frequent, massive or structural transfers, in other words for sets of transfers (and not just for occasional transfers).

183. The EDPS recommends providing a specific paragraph dedicated to transfers with the EDPS' authorisation. This paragraph, that logically would come before the paragraph on derogations would provide that EDPS may authorise a transfer or a set of transfers where Europol adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals, and as regards the exercises of the corresponding rights. In addition, this authorisation would be granted prior to the transfer / set of transfers, for a period not exceeding one year, renewable.

Other

184. The opinion includes a large number of other recommendations, aiming at further improving the proposal. Here, some more significant recommendations are listed.

a. Deleting the possibility for Europol to directly access national databases.(Article 23).
b. Where access concerns EU information systems, granting access only on a hit/no hit basis (i.e. a positive or a negative answer). Any information related to the hit should be communicated to Europol after the explicit approval and authorization of transfer by the Member State (if the access concerns data supplied by a Member State), the EU body or the international organisation and be subject to the assessment referred to in Article 35 of the Proposal. The EDPS recommends laying down these conditions in Article 23 of the Proposal.
c. Strengthening Article 35 of the Proposal by making the assessment by the Member State providing the information mandatory. The EDPS suggests deleting in Article 35 (1) and (2) the wording 'as far as possible' and amending Article 36(4) accordingly.
d. Replacing the overview of all personal data referred to in Article 36(2) by statistics on these data for each purpose. As the specific categories of data subjects referred to Article 36(1) also deserve a specific attention, the EDPS suggests including statistics on these data.
e. Including in the Proposal a provision that Europol must have a transparent and easily accessible policy with regard to the processing of personal data and for the exercise of the data subjects' rights, in an intelligible form, using clear and plain language. The provision should also state that this policy should be easily available on Europol's website, as well as on the websites of the national supervisory authorities.

f. Since Article 41 does not clearly define the responsibility of all parties involved, it should, with regard to Article 41(4 be made clear that the responsibility for compliance with all applicable data protection principles (and not only the 'legality of the transfer') lies with the sender of the data. The EDPS recommends amending Article 41 accordingly.
g. adding in substantive provision(s) of the Proposal that: (i) an impact assessment similar to what is described in the proposed data protection Regulation shall be carried out for all processing operation on personal data,(ii) the principle of privacy by design and by default shall be applied for the creation of or improvement to systems processing personal data,(iii) the controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate compliance with the data protection rules, and to ensure that the effectiveness of the measures is verified, and(iv) the Europol DPO and, where necessary, the supervisory authorities, shall be included in the discussions surrounding the processing of personal data.

He also made a few suggestions in relation to the Communication that was adopted in parallel to the proposal.

.

Done in Brussels, 31 May 2013

Peter HUSTINX

European Data Protection Supervisor

Annex 1: Comments on the financial impact of the proposal

The EDPS has carefully analysed the Commission's estimations concerning the impact that the supervision of Europol may have for the institution, both in terms of financial and human resources.

This potential impact was already assessed by the EDPS in the context of the Multiannual Financial Framework exercise (2014-2020) and our estimations were sent to the Commission and the Budgetary Authority end of March 2013 following the budgetary procedure and were based on the following assumptions:

- **General objective**: Monitor and ensure compliance with the data protection rules of ex third pillar agencies. Budgetary estimations were made on the basis of the most likely scenario at the time (i.e. supervision of one agency, taking effect as from 2016).

- **Specific objectives**: Perform supervisory activities relating to both the processing of staff data and core business data.

    1. Supervision of processing operations of staff data: this supervision activity would not have significant budget implications as it would be included in EDPS supervision activities.

    2. Supervision of Europol core activities: this task would include activities such as:
        - coordination meetings with the national data protection authorities (1 day, Brussels)
        - at least 1 inspection a year (5 days, The Hague)
        - meetings in connection with the annual inspection, 3 times a year (1 day, The Hague)
        - publication and translation of reports/minutes of meetings and opinions

The allocation of additional human and financial resources would be absolutely necessary for the achievement of these specific objectives. Additional credits would be necessary to cover the costs of missions, organisation of meetings and the preparation and translation and publication of documents and at least three additional FTE: 1 AD6, 1 AST3 and 1 SNE/CA would be required.

The table with detailed cost calculations that was produced in the context of the Multiannual Financial Framework is enclosed to this annex for information.

A comparison between the estimations included in the Commission proposal and the EDPS forecast shows some similarities and one important difference. Concerning the estimated requirements of additional administrative expenditure (page 92 of the Commission proposal), the costs foreseen for meetings and missions are quite similar in both proposals. On the contrary, the cost estimated for publications and translations are different because EDPS forecasts include a possible publication in the Official Journal.
As regards the estimated requirements of human resources (page 91 of the Commission proposal), it seems that the minimum number of posts necessary to perform supervision activities has been greatly underestimated in the Commission proposal. On the basis of

our experience in this kind of activities, we are strongly of the view that at the very least three full time equivalents are necessary to be able to achieve the objectives assigned (see for example, the own estimations of the Commission for non-supervision activities which amount to five FTE).

On the basis of these considerations, we would recommend that the reasonable costs estimated by the EDPS and communicated to the Budgetary Authority in the context of the Multiannual Financial Framework are taken into consideration and the Commission proposal is amended accordingly.

MFF 2014-2020 - EUROPOL SUPERVISION

	Persons	Days	Times/ year	Daily allowance	Hotel	Transport	Eurest	2013	2014	2015	2016	2017	2018	2019	2020	MFF 2014-2020
Gneral objective: monitor and ensure compliance with the DP rules of ex 3rd pillar agencies																
3 Coordination meetings in Bxl with national DPAs (meetings)	27	1	3	92	2.700	48.600	364	59.116,14	-	-	62.734,52	63.989,21	65.269,00	66.574,38	67.905,86	326.472,97
1 Inspection (5 days) at The Hague (DPAs experts - meetings)	8	5	1	93	6.800	4.800		15.320,00	-	-	16.257,71	16.582,86	16.914,52	17.252,81	17.597,86	84.605,76
Subtotal meetings								**74.436,14**	**-**	**-**	**78.992,23**	**80.572,07**	**82.183,51**	**83.827,18**	**85.503,73**	**411.078,72**
1 Inspection (5 days) at The Hague (EDPS staff - missions)	2	5	1	93	1.700	250		2.880,00	-	-	3.056,28	3.117,40	3.179,75	3.243,35	3.308,21	15.905,00
3 Meetings at The Hague in connection with the annual inspection (EDPS staff - missions)	2	1	3	93	1.020	750		2.328,00	-	-	2.470,49	2.519,90	2.570,30	2.621,71	2.674,14	12.856,54
Subtotal missions								**5.208,00**	**-**	**-**	**5.526,77**	**5.637,31**	**5.750,05**	**5.865,05**	**5.982,35**	**28.761,54**
Publications								**20.460,01**			**21.712,33**	**22.146,57**	**22.589,50**	**23.041,29**	**23.502,12**	**112.991,82**
Translations								**132.308,06**			**140.406,38**	**143.214,50**	**146.078,79**	**149.000,37**	**151.980,38**	**730.680,42**
Total other administrative expenditure								**232.412,21**	**-**	**-**	**246.637,70**	**251.570,45**	**256.601,86**	**261.733,90**	**266.968,58**	**1.283.512,50**
Staff																
1 AD7											96.000,00	99.360,00	102.837,60	106.436,92	110.162,21	514.796,72
1 AST5											84.000,00	86.940,00	89.982,90	93.132,30	96.391,93	450.447,13
1 END / 1 AC											60.000,00	62.100,00	64.273,50	66.523,07	68.851,38	321.747,95
Total staff cost								**-**	**-**	**-**	**240.000,00**	**248.400,00**	**257.094,00**	**266.092,29**	**275.405,52**	**1.286.991,81**
GRAND TOTAL								**232.412,21**	**-**	**-**	**486.637,70**	**499.970,45**	**513.695,86**	**527.826,19**	**542.374,10**	**2.570.504,31**