COUNCIL OF THE EUROPEAN UNION

Brussels, 10 July 2012

12406/12

ENFOPOL 231
TELECOM 139

COVER NOTE

from:	Peter Hustinx, European Data Protection Supervisor
date of receipt:	29 June 2012
to:	President of the Council of the European Union
Subject:	Opinion of the European Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre

Delegations will find attached EDPS document C 2012-0159.

Encl.: C 2012-0159

Opinion of the European Data Protection Supervisor

on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre

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[2],

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

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 28 March 2012, the Commission adopted a Communication titled "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre"[4].

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] OJ L 350, 30.12.2008, p. 60.
[4] Cybercrime is not defined in EU legislation.

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

2. The EDPS notes that the Council published its Conclusions on the establishment of a European Cybercrime Centre on 7-8 June 2012[5]. The Council endorses the goals of the Communication, supports the establishment of the Centre (also referred to as "EC3") within Europol and the use of the existing structures to cross-work with other crime areas, confirms that the EC3 should serve as a focal point in the fight against cybercrime, and that the EC3 will cooperate closely with relevant agencies and actors at international level, and calls the Commission in consultation with Europol to further elaborate the scope of the specific tasks that will be required to make the EC3 operational by 2013. However, the Conclusions do not refer to the importance of fundamental rights, and in particular, to data protection in the establishment of the EC3.

3. Before the adoption of the Commission Communication, the EDPS was given the possibility to provide informal comments on the draft Communication. In its informal comments, the EDPS emphasized that data protection is an essential aspect to be taken into consideration in the setup of the European Cybercrime Centre (hereafter 'EC3'). Unfortunately, the Communication did not take into account the comments made at informal stage. Moreover, the Council Conclusions ask to ensure that the Centre will be operational already by next year. This is why data protection should be taken into consideration in the next steps that will be taken already on a very short term.

4. This opinion addresses the importance of data protection when setting up the EC3, and provides specific suggestions that could be taken into consideration in the course of the set up of the terms of reference for the EC3 and in the legislative revision of the Europol legal framework. Acting on his own initiative, the EDPS has therefore adopted the current Opinion based on Article 41(2) of Regulation (EC) No 45/2001.

1.2. Scope of the Communication

5. In its Communication, the Commission indicates the intention to create a European Cybercrime Centre as priority of the Internal Security Strategy.[6]

6. The Communication non-exhaustively lists several strands of cybercrime which the EC3 is supposed to focus on: cybercrimes committed by organised crime groups, particularly those generating large criminal profits such as online fraud, cybercrimes which cause serious harm to their victims, such as online child sexual exploitation, and cybercrimes seriously affecting critical Information Communication Technology (ICT) systems in the Union.

7. In terms of the Centre's work, the Communication lists four main tasks[7]:
   - serving as the European cybercrime information focal point;
   - pooling European cybercrime expertise to support Members States in capacity building;
   - providing support to Member States' cybercrime investigations;
   - becoming the collective voice of European cybercrime investigators across law enforcement and the judiciary.

[5] Council conclusions on the establishment of a European Cybercrime Centre 3172nd JUSTICE and HOME AFFAIRS Council meeting Luxembourg, 7 and 8 June 2012.
[6] The EU Internal Security Strategy in action: five steps towards a more secure Europe. COM(2010)673 final, 22 November 2010. See also the EDPS opinion on this Communication, issued on 17 December 2010, OJ C 101/6.
[7] Communication p. 4-5.

8. The information processed by the EC3 will be gathered from the *widest array of public, private and open sources*, enriching available police data, and it would *concern cybercrime activities, methods and suspects*. The EC3 will also collaborate directly with other European agencies and bodies. This will happen via the participation of these entities in the EC3's Programme Board and also through operational cooperation where relevant.

9. The Commission proposes that the EC3 would be the natural interface to Europol's cybercrime activities and other international police cybercrime units. The EC3 should also, in partnership with Interpol and other strategic partners around the globe, strive to improve coordinated responses in the fight against cybercrime.

10. In practical terms, the Commission proposes to create this EC3 as part of Europol. The EC3 will *be part of Europol*[8] and, therefore, it will be placed under the legal regime of Europol[9].

11. According to the European Commission[10], the main novelties that the proposed EC3 will bring to Europol´s current activities will be: (i) increased resources to more efficiently gather information from various sources (ii) exchange of information with partners beyond the law enforcement community (mainly from the private sector).

1.3. Focus of the Opinion

12. The EDPS seeks in this opinion to:
    - ask the Commission to clarify the scope of the activities of the EC3, as far as they are relevant for data protection;
    - assess the foreseen activities in the context of the current Europol legal framework, especially their compatibility with the framework;
    - highlight relevant aspects where the legislator should introduce further detail in the context of the future review of Europol´s legal regime to ensure a higher level of data protection.

13. The opinion is organised as follows. Part 2.1 elaborates why data protection is an essential element in the creation of the EC3. Part 2.2 deals with the compatibility of the goals set for the EC3 in the Communication with Europol's legal mandate. Part 2.3 deals with the cooperation with private sector and international partners.

2. COMMENTS

2.1. Data protection as an essential element in the creation of the Centre

14. The EDPS regards the fight against cybercrime as a cornerstone in building security and safety in the digital space and generating the required trust. It can also enhance the security in the digital space and consequently improve the level of data protection in this area. Indeed, protection of individuals in cyberspace will inherently benefit if the

[8] As recommended by the feasibility study published in February 2012 evaluating the different options available (status quo, hosted by Europol, owned/be part of Europol, virtual Centre). http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf.
[9] Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA).
[10] Press release of the 28 March. Frequently Asked Questions: the new European Cybercrime Centre Reference: MEMO/12/221 Date: 28/03/2012 http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/221.

Centre can achieve its goals while at the same time fully respecting fundamental rights and in particular the right to data protection. Against this background, the EDPS would like to express his support for the creation of mechanisms to fight against cybercrime, such as the proposed Centre.

15. The fight against cybercrime will often require processing personal data in the context of investigations. It consequently entails risks of intrusions into the citizens' privacy. This is why privacy concerns should be taken into consideration together with the objectives of the EC3.

16. The EDPS is convinced that effective action to fight cybercrime cannot be put in place without the support of a solid data protection scheme complementing it. Appropriate safeguards are needed to ensure that monitoring and processing of personal data will only be done in a strictly targeted way, and that misuse of this mechanism is prevented by adequate measures. The EDPS wishes to ensure that this monitoring is carried out under a clear framework with adequate data protection safeguards put in place.

17. Unfortunately, the Communication does not mention data protection as an element to be considered in the activities of the Centre. The EDPS calls on the Commission to consider that activities of EC3 should be based on a solid data protection scheme and that this should be reflected in its establishment, both in the terms of reference of the Centre and in the upcoming review of Europol's legal framework.

2.2. Compatibility of EC3´goals with Europol's legal mandate

From the Europol CyberCrime Center to the EC3

18. The EDPS notes that no specific legal instrument is foreseen for the establishment of the EC3. It will rely on existing structures. The Centre will be located in Europol and the activities of the EC3 will, therefore, need to comply with the provisions of the Europol Council Decision, including the data protection framework of Europol.

19. Europol has been providing support to Member States in the fight against cybercrime from 2002 with the establishment of the Europol's High Tech Crime Centre. During this time, Europol has developed a European platform to service the needs of Member States specific to the fight against cybercrime.

20. According to the General Report on Europol's activities in 2011[11] a Europol Cyber Crime Centre has been set up in 2011 and it seems that, according to the results mentioned in the Report, it has already produced significant contributions in terms of fighting cybercrime activities[12]. That triggers the question of what is new in terms of activities and tasks in the Commission Communication since a Europol Cybercrime Centre is already functioning in Europol since 2011.

21. The Communication does not refer to these previously existing activities of Europol and seems to point to the creation of an entirely new structure within Europol. In this

[11] General Report on Europol's activities in 2011, 10036/12, ENFOPOL 141, Brussels, 24 May 2012.
12 "In 2011, Europol supported major cybercrime operations Crossbill (malware) and Mariposa II (Butterfly bots). In the area of online child exploitation, Europol supported Operation Rescue in a successful bid to take down a worldwide network of child sex-offenders. Operation Icarus is another such operation involving 23 countries.". See p. 59 of the Europol 2011 Report for more information.

sense, the EDPS calls for greater clarity as regards the new activities foreseen for the EC3 and also for an analysis of the impact in terms of data protection.

Offences that will be investigated by the EC3

22. The EDPS notes the importance of assessing how the goals expressed in the Communication for the EC3 match with Europol´s current legal framework and in particular its current mandate.

23. Article 4(1) of the Europol Decision and the Annex include the fight against "computer crime" under the competences of Europol. Yet, the concept of "computer crime" is not defined, neither in the Europol Decision nor in any other EU legal instrument. The notions of "computer crime" and "cybercrime" are related, but not necessarily identical. Neither can it automatically be assumed that all tasks the EC3 is expected to carry out are covered by Europol's tasks.

24. In the absence of a legal definition for cybercrime in EU legislation, the EDPS considers that it is important to clarify the competences of the Centre. At a minimum, it should be clarified what "types of cybercrimes" will be investigated. For instance, it should be established if the EC3 should tackle certain offences already specified in the EU legal framework or not:

- Council Framework Decision 2005/222/JHA on attacks against information systems[13] and the proposed Directive[14] that will replace this Framework Decision. The Framework Decision covers for instance illegal access to information systems, illegal system interference or illegal data interference;
- Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography[15]. This covers for instance, images of child sexual abuse spread through the use of new technologies and the Internet;
- Council Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment. This covers for instance, intentionally performing or causing a transfer of money with the intention of procuring an unauthorised economic benefit for the person committing the offence or for a third party, by altering, deleting or suppressing computer data, in particular identification data, or interfering with the functioning of a computer programme or system.

25. Moreover, as part of the European Strategy for Identity Management, the Commission is currently working on a proposal on criminalisation of identity theft. Furthermore, the 2001 Budapest Convention on Cybercrime[16] mentions a number of offences, such as offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; offences related to infringements of copyright and related rights). It should be clarified whether all these crimes will also be covered.

---

[13] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 69, 16.03.2005, p. 67-71.

[14] The Proposal 2010/273 for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA is currently under ordinary legislative procedure.

[15] Directive 2011/92/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 27.11.2011, p. 1-14.

[16] Convention on Cybercrime, Budapest, 23.11.2001.
http://conventions.coe.int/Treaty/en/Treaties/html/185.htm

26. As the legal instrument that will be providing a legal basis for the activities of the Centre is Europol´s present legal framework which is currently under review[17], the EDPS recommends that this review process should take into consideration, among other aspects, the definition of the competences of the EC3.

27. Also, the EDPS recommends that until a revised legal framework becomes applicable, the scope of activities of the EC3 should at least be specified in the form of terms of reference[18]. These terms of reference should be set forth prior to the start of the operations of the EC3 (according to the Communication by the end of 2013) and should set out *inter alia* which offences will fall under the EC3's competences and which not.

EC3´s Operational support activities

28. The EC3 is supposed to provide, according to the Communication, "*operational support*" to cybercrime investigations, for example by encouraging the establishment of joint investigation teams. One of its proposed tasks is to "*provide high-level forensic assistance (facilities, storage, tools) and encryption expertise for cybercrime investigations*."[19] Another example given in the Communication is the work of a Europol analyst in "*cracking the security features*"[20] of a computer system in a past investigation.

29. The general legal basis in Article 88 TFEU[21] defines Europol's tasks and it is further specified in the Europol Decision. Article 5(2) of the Europol Decision spells out its tasks in more detail, including supporting Member States through support, advice and research regarding "*technical and forensic methods and analysis, and investigative procedures*" and "*providing support to Member States in their tasks of gathering and analysing information from the Internet in order to assist in the identification of criminal activities facilitated by or committed using the Internet*".

30. Also, under Article 6 of the Europol Council Decision, Europol staff may participate in supporting capacity in joint investigation teams but it explicitly forbids the participation in the taking of any coercive measures.

31. Europol's tasks, as defined in the Council Decision, are limited, as a general rule, to providing support in terms of knowledge of best practices and analysis of information. However, the line between operational activities and assistance activities in the context of cybercrime is quite unclear, "*cracking the security features*" of a computer system

[17] According to Article 88(2) of the Treaty on the Functioning of the European Union, the European Parliament and the Council, by means of regulations adopted in accordance with the ordinary legislative procedure, shall determine Europol's structure, operation, field of action and tasks. The European Commission Work Programme 2012 includes this legislative initiative in point 64.
http://ec.europa.eu/atwork/programmes/docs/cwp2012_annex_en.pdf

[18] According to Article 37(7)(c) of the Europol Council Decision, the Management board shall take any decision or implementing measures in accordance with the Europol Decision.

[19] Communication, p. 5.

[20] Ibid.

[21] Article 88(1) provides that the main mission of Europol is to support and strengthen action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.

or providing "*operational support*" can, in some cases, go beyond the provision of assistance and knowledge. Consequently, the EDPS recommends to:

- define in the context of the fight against cybercrime very clearly in which operational support activities the Centre's staff could be engaged and to what extent, alone or in collaboration with joint investigation teams, and
- establish clear procedures for engaging in operational support activities that on the one hand ensure the respect of individual rights and in particular the right to data protection, and on the other hand provide guarantees that the evidence has been lawfully obtained and could be used before a court.

Use of Privacy Enhancing Technologies

32. The practical implementation of the EC3 activities will likely build upon the use of an advanced IT infrastructure processing massive amounts of personal data to support the actions envisaged in the Communication. Privacy Enhancing Technologies (PETs) can be seen as enablers of the correct balance between the achievement of the objectives of the EC3 and respect of the rights of individuals.

33. The EDPS strongly recommends that the IT infrastructure should be carefully assessed in advance and that concrete measures for the application of PETs are taken into consideration. This approach will be fully in line with the "privacy by design" approach foreseen in the recent proposal of the Commission for the review of the data protection framework.[22]. This is even more important in this case given the short deadline for making the Centre operational, by 2013, and the fact that by then the revised Europol legal framework will most probably not be applicable yet.

34. Applying "privacy by design" will therefore help to ensure proportionality of the Centre's activities and to minimise interference with fundamental rights.

2.3. Cooperation of the EC3 with private sector and international partners

35. Chapter 2.1 of the Communication describes the goal of the EC3 to become a focal point of the fight against cybercrime. In particular, it lays down that one of the functions of the EC3 will be the collection of information on cybercrime from the *widest array of public, private and open sources, enriching available police data*. The Communication indicates that such information will also concern suspects of cybercrime activities. Therefore, the EC3 will be processing personal data in the sense of Article 2(a) of Council Decision 2008/977/JHA[23] in this context.

36. The EDPS notes that the Europol Decision regulates strictly the exchange of personal data between Europol and the private sector and, in most cases, as will be analysed below, data exchanges between Europol and the private sector are only to take place with the intermediation of national law enforcement authorities.

[22] Article 19 of the Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. COM/2012/010 final - 2012/0010 (COD).

[23] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJ L 350, 30/12/2008 P. 0060 - 0071.

37. The EDPS analyses, in this chapter, how the legal restrictions imposed by the Europol Decision should be applied in practice by the EC3.

Cooperation with private sector

38. The Communication states that Europol will be collecting data from any available source (private, public or open) in order to enrich police data. The EDPS notes with concern that this approach is in line with the general trend of ensuring that the principle of availability of information to enhance the efficiency of law enforcement bodies is achieved without counterbalancing it with the proportionality and necessity principles required by Article 8 of the Charter of Fundamental Rights of the Union, Article 8 of the ECHR and Article 16 of the TFEU.

39. The fight against cybercrime is likely to often require the cooperation of the private sector as most of the data relevant to investigate cybercrime offences are stored by private entities that keep records of electronic transactions and communications in the course of their regular activities or in compliance with specific legislative requirements. For instance, telecom operators retain data of internet and telecom communications for commercial purposes or in compliance with the Data Retention Directive.[24]

40. It is obvious that the fight against cybercrime constitutes a purpose unrelated to the commercial activities carried out by such companies. Therefore, issues with regard to lawful processing and compatible use of personal data have to be considered as this collection and further use of the associated data in the fight against cybercrime could amount to an infringement of the right to the protection of personal data.

41. The EDPS referred to the cooperation with the private sector in law enforcement activities on different occasions[25], recognising its sensitive nature. In particular, the EDPS is concerned about the issues raised by the involvement of a commercial actor, offering a specific service, in a sphere such as law enforcement where in principle only competent authorities are supposed to intervene, under the conditions foreseen in national law.

42. Moreover, the Communication seems to strive for a direct communication between the EC3 and the private sector. However, Europol and subsequently the EC3 are not entitled to interact directly with private entities without restrictions. Article 25 of

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

[25] Opinion of the European Data Protection Supervisor of 23 June 2008 on the Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies. OJ C 2, 7.1.2009, p. 2–6.
Opinion of the European Data Protection Supervisor of 22 February 2010on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA). OJ C 147, 5.6.2010, p. 1–13.
Opinion of the European Data Protection Supervisor of 7 October 2011on net neutrality, traffic management and the protection of privacy and personal data. OJ C 34, 8.2.2012, p. 1–17.
Opinion of the European Data Protection Supervisor of 24 April 2012 on the proposal for a Council Decision on the Conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America, published in www.edps.europa.eu.

Europol Council Decision lays down that Europol is allowed to process information, including personal data in so far as it is necessary for the legitimate performance of its tasks, from private parties under certain conditions:

- Under Article 25(3)(a), personal data from private parties which are established under the law of a Member State may be processed by Europol, only if they are transmitted via the national unit of that Member State in accordance with its national law. This Article explicitly forbids Europol to contact directly private parties to retrieve information.
- Under Article 25(3)(b), personal data from private parties which are established under the law of a third State with which Europol has a cooperation agreement may be processed, only if the data has been received via the contact point of that State.
- Under Article 25(3)(c), personal data from private parties which are established under the law of a third State with which Europol has no cooperation agreement may be processed, only if that private party is included in a list that the Europol management board is entitled to draw up and Europol has concluded with that party a memorandum of understanding on the transmission of information, confirming the legality of the collection and transmission and specifying that the personal data may be used only for the legitimate performance of Europol´s task. Article 25.6 clarifies that Europol will only be entitled to process this information to include it in the Europol Information System or other analysis work files or systems referred to in that Article.
- Under Article 25(4), Europol may process personal data retrieved from publicly available sources.

43. Also, a direct interaction with private entities will be complex as it would be subject to different national legislations and different procedural safeguards depending on the Member State where the private entity is placed (for instance in a country the disclosure of a particular type of data might be subject to judicial authorisation while in another country this is not required).

44. The EDPS notes that the restriction that Europol can only process data that has been obtained previously through national units will simplify the interaction and contribute to data protection, as the national units will normally ensure that the exchange of information with the EC3 is done lawfully and that the adequate safeguards are put in place in accordance with the legislation of each Member State. Therefore, the EDPS recommends that this safeguard is maintained both in the terms of reference of the EC3 and in the review of Europol's legal framework.

Cooperation with international partners

45. The investigation of cybercrime offences often requires the collection and processing of data originating from different countries (some of which could be outside of the European Union). The Communication sets out that one of the goals of the EC3 is to become the collective voice of European cybercrime investigators across law enforcement and the judiciary, as mentioned in the text of the Communication. In order to achieve this goal, the EC3 would be the natural interface to Interpol´s activities against cybercrime and other international police cybercrime units.

46. In principle, this activity is in line with Article 23 of the Europol Council Decision, which sets out that Europol may exchange information, including personal data in so

far as it is necessary for the legitimate performance of its tasks with third states and with some concrete organisations.

47. In particular, under Article 23(3) Europol may receive and use personal data provided by third states and organisations. Under Article 23(6), Europol is entitled to transmit personal data to third states and organisations if the following conditions are fulfilled:
    - it has obtained the consent of the Member State that originally transmitted the data concerned to Europol;
    - where it is necessary in individual cases for the purposes of preventing and combating criminal offences in respect of which Europol is competent;
    - when Europol has concluded an agreement with the recipient entity that permits the transmission of the data on the basis of an assessment of the existence of an adequate level of data protection;
    - the Director of Europol may authorise transmissions of personal data after having assessed the adequacy of the level of protection of the recipient entity if the transmission of the data is absolutely necessary to safeguard essential interests of the Member States concerned within the Europol´s objectives or in the interests of preventing imminent danger associated with crime or terrorist offences.

48. The EDPS notes that according to these provisions, EC3 should not exchange personal data unless it is justified in individual cases and where the recipient entity provides an adequate level of data protection. These conditions must also be assessed in the light of the implementing rules laid out in Council Decision 2009/934/JHA governing Europol's relations with partners.

49. Against this background, and given the importance that the exchange of information at international level has in the fight against cybercrime, the EDPS recommends that it is assessed if the current international agreements signed by Europol allow for the exchange of the information needed, in the amounts and with the speed required in this context. Also, the EDPS notes that the terms of reference to be created by the EC3 implementation team should address specifically international cooperation since it will be one of the main tasks of the EC3 as the collective voice of European cybercrime investigators and the information focal point for international partners.

3. CONCLUSIONS

50. The EDPS regards the fight against cybercrime as a cornerstone in building security and safety in the digital space and generating the required trust. The EDPS notes that compliance with data protection regimes should be regarded as an integral part of the fight against cybercrime and not as a deterrent of its effectiveness.

51. The Communication refers to the establishment of a new European Cybercrime Centre within Europol while a Europol Cybercrime Centre has already been in existence for a number of years. The EDPS would welcome if more clarity is provided concerning the new capacities and the activities that will distinguish the new EC3 from the existing Europol Cybercrime Centre.

52. The EDPS advises that the competences of the EC3 should be clearly defined and not just laid out by referring to the concept of "Computer Crime" included in current Europol's legislation. Also, the definition of the competences and data protection safeguards of the EC3 should be part of the review of the Europol legislation. Until the

new Europol legislation becomes applicable, the EDPS recommends that the Commission sets forth such competences and data protection safeguards in the terms of reference for the Centre. These could include:

- a clear definition in which data processing tasks (in particular, investigations and operational support activities) the Centre's staff could be engaged, alone or in collaboration with joint investigation teams, and
- clear procedures that on the one hand ensure the respect of individual rights (including the right for data protection), and on the other hand provide guarantees that evidence has been lawfully obtained and can be used before a court.

53. The EDPS considers that the exchanges of personal data of the EC3 with the *"widest array of public, private and open source actors"* imply specific data protection risks as they will often involve the processing of data collected for commercial purposes and international data transfers. These risks are addressed by the current Europol Decision which establishes that, in general, Europol should not exchange data directly with the private sector, and with specific international organisations only in very concrete circumstances.

54. Against this background, and given the importance of these two activities for the EC3, the EDPS recommends that appropriate data protection safeguards should be provided in compliance with the existing provisions in the Europol Decision. These safeguards should be embedded in the terms of reference to be elaborated by the implementation team for the EC3 (and later in the revised Europol legal framework) and should in no event result in a lower level of data protection.

Done in Brussels, 29 June 2012

(signed)

Peter HUSTINX
European Data Protection Supervisor