Council of the European Union

Brussels, 17 September 2015
(OR. en)

DS 1497/15

LIMITE

MEETING DOCUMENT

From:	Presidency
To:	Delegations
Subject:	The functioning of the Internet Referral Unit (EU IRU) on the basis of the future Europol Regulation

Background

Following the Paris shooting on 7 January 2015, there have been a number of developments that have recently led to the creation of the European Counter-Terrorism Centre (ECTC) and the Internet Referral Unit (EU IRU) within the ECTC at Europol:

- In the Riga Joint Statement[1], following the informal meeting of Justice and Home Affairs Ministers in Riga on 29 and 30 January 2015, the ministers stated the following: "*The internet plays a significant role in radicalization. In this regard, we must strengthen our efforts to cooperate closely with the industry and to encourage them to remove terrorist and extremist content from their platforms. (…) In this context, Internet referral capabilities, also through Check-the-web, could be developed within Europol to support efforts of Member States in detecting illegal content and improving exchange of information.*"

15855/15

- In the informal European Council Statement on terrorism of 12 February 2015 as regards the prevention of radicalisation and safeguarding of values it was called for *"adequate measures to be taken, in accordance with national constitutions, to detect and remove internet content promoting terrorism or extremism, including through greater cooperation between public authorities and the private sector at EU level, also working with Europol to establish internet referral capabilities".*

- To achieve effective progress on enhancing Internet referral capabilities, the Council of 12 March 2015 mandated Europol to establish the EU Internet Referral Unit at Europol as from 1 July 2015 with the involvement of Member States, Commission and other stakeholders and taking into account resources needed for ensuring the work of the Unit. The specific objective of this Unit is reducing the level and impact of terrorist and violent extremist propaganda on the internet on the basis of the principles and tasks set out in document 6891/15, i.e.:

  - *"To coordinate and share the identification tasks (flagging) of terrorist and violent extremist online content with relevant partners,*

  - *To carry out and support referrals quickly, efficiently and effectively, in close cooperation with the industry,*

  - *To support competent authorities, by providing strategic analysis and operational analysis,*

  - *To act as a European Centre of Excellence for the above tasks[2]".*

- In the Commission Communication on the European Agenda on Security[3], the IRU was also mentioned as part of the required efforts to tackle terrorism and prevent radicalisation, namely "*the Internet* Referral *Unit (EU IRU), to be established in Europol by July 2015, would also be part of the [European Counter-Terrorism] Centre. The Unit will build upon Europol and Member States' experience to act as an EU centre of expertise, helping Member States to identify and remove violent extremist content online, in cooperation with industry partners".*

2With a view of carrying out the tasks mentioned above, Europol has also developed its concept note on IRU (see 7266/15).

- In addition to the specific aforementioned counter terrorism-related actions, the special European Council of 23 April 2015 on the migration situation in the Mediterranean sea has called for Europol to carry out internet referral activities in relation to facilitated illegal immigration, by detecting internet content used by traffickers to attract migrants and refugees. Namely it has called to *"use EUROPOL to detect and request removal of internet content used by traffickers to attract migrants and refugees, in accordance with national constitutions"*.

State of play

On the basis of the above, on 1 July 2015 Europol launched the EU IRU to combat terrorist propaganda and related violent extremist activities on the internet as an integral part of the ECTC. A three-staged implementation approach has been identified as the optimal solution. The project began with a six-month Pilot Phase. This will further progress into an Initial Operating Capability by 1 January 2016, followed by a Full Operating Capability by 1 July 2016.

Internet content referral activities are carried out with concerned private industry companies, while Member States support the EU IRU by appointing national EU IRU contact points. Referral activities do not constitute an enforceable act, thus the decision and related implementation of the referral is taken under full responsibility and accountability of the service provider concerned.

From a formal point of view, the functioning of EU IRU is currently mainly based on Article 5(2) of the Council Decision on Europol[4] relating to the tasks of Europol: "*The tasks (…) shall include 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*."

4Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p. 37.)

In accordance with Article 24(4) of the aforementioned Council Decision, "*In addition to the processing of data from private parties in accordance with paragraph 3, Europol may directly retrieve and process data, including personal data, from publicly available sources, such as media and public data and commercial intelligence providers, in accordance with the data-protection provisions of this Decision. In accordance with Article 17, Europol shall forward all relevant information to the national units*."

It should be noted that the Council Decision on Europol has no express provisions regulating the transfer of personal data (for example, the URL link), which is publicly available, to private parties.

The functioning of IRU on the basis of the future Europol Regulation

The Council's general approach on draft Europol Regulation[5] does not contain a specific provision among the tasks of Europol that would be similar to Article 5(2) of the Council Decision on Europol. On the other hand, among the tasks listed in Article 4(1)(a), Europol is first of all tasked to "*collect, store, process, analyse and exchange information, including criminal intelligence"***.**

Article 23(2) also specifies that "*Europol may directly retrieve and process information, including personal data, from publicly available sources, including the internet and public data*."

However, Article 32 on personal data from private parties, in particular paragraph (3a), seriously limits the possibility for Europol to transfer personal data, as required for the purposes of IRU, to private parties: "*Europol may not transfer personal data to private parties except where, subject to any possible restrictions stipulated pursuant to Article 25(2) or (3) and Article 69:*

(a) the transfer is undoubtedly in the interests of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such a consent; or

(b) the transfer is absolutely necessary in the interests of preventing imminent danger associated with crime or terrorist offences."

510033/14

Initial proposal for discussion

In order to provide explicit legal basis in the draft Europol Regulation for the functioning of IRU while ensuring the necessary guarantees for the protection of personal data, the Presidency has developed the following initial proposals to amend the draft Europol Regulation, also aiming to ensure coherence and align certain provisions of the Europol Regulation with the draft Data Protection Directive as regards the exchanges of personal data with private parties, and hereby submits them for discussion by delegations (new proposals compared to the general approach are underlined):

1.1. Proposal for a new indent (m) in Article 4(1) "Tasks of Europol":

"(m) To process information in order to support Member States in preventing and combating forms of crime listed in Annex 1 which are facilitated or committed using the internet, and to process personal data in so far as it is necessary for such a purpose. This includes receiving reports, collecting and analysing information from publicly available sources, notably the internet, identifying content which facilitates or promotes such forms of crime, and taking action to secure its removal in voluntary cooperation with online service providers".

Article 4(1)(m) would be accompanied by a new recital (9a) explaining the new task set out in Art. 4(1)(m):

"(9a) Whilst the internet provides a common global infrastructure for the exchange of ideas, services and goods, it can also be used for cross-border criminal activities. Europol should therefore be able to process information, including personal data, also from the internet and other publicly available sources to support the Member States in preventing and combating forms of crime that fall under Europol's competence when criminal acts are facilitated and committed using the internet. As criminal activity on the internet has increased in recent years, [such as the amount of online material facilitating or promoting terrorism, illegal migrant smuggling], Europol should, in close cooperation with the Member States, identify such content, analyse it, and take appropriate action to secure its removal in voluntary cooperation with online service providers."

1.2. Proposal for a new indent (occ) in Article 14(1) "Functions of the Management Board"

"(occ) adopt the procedures and business processes required for the processing of personal data for the purpose of identifying and requesting the removal of internet content which facilitates or promotes forms of crime referred to in Article 4(1)(m) , having obtained the opinion of the European Data Protection Supervisor;"

1.3. Proposals for new amendments to Article 32:

Article 32: *Exchanges of* Ppersonal data ~~from~~ *with* private parties

1. ***Without prejudice to paragraph 1c,*** in so far as necessary for Europol to perform its tasks, Europol may process personal data ~~originating~~ from private parties on condition that ***they*** are received via:

(a) a ~~n~~*N*ational ~~u~~*U*nit of a Member State in accordance with national law;

(b) the contact point of a third country ***or an international organisation*** with which Europol has concluded a cooperation agreement ***allowing for the exchange of personal data*** in accordance with Article 23 of the Decision 2009/371/JHA prior to date of application of this Regulation; or

(c) an authority of a third country or an international organisation ***which is subject to an adequacy decision as referred to in Article 31(1)(a) or*** with which the Union has concluded an international agreement pursuant to Article 218 of the Treaty.

1a. In cases where Europol nonetheless receives personal data directly from private parties and where the National Unit, contact point or authority concerned referred to in paragraph 1 cannot be identified, Europol may process that personal data solely for the purpose of identifying these entities. Subsequently, the personal data shall be forwarded immediately to the National Unit, contact point or authority concerned who shall define in accordance with Article 25(1), where relevant, the purpose for which Europol may further process the data.[6]

6 Please note that as explained in DS 1371/15 on the preparation of the trilogue of 23 June 2015, despite its initial negative reaction the EP might accept the wording proposed by the Council in Article 32, paragraph 1a, if it is further clarified that such data would be kept separately and would be deleted after their transmission to the National Units or contact points concerned. The exact

1b. If Europol receives personal data from a private party in a third country with which there is no agreement, either concluded on the basis of Article 23 of Decision 2009/371/JHA or on the basis of Article 218 of the Treaty or which is not subject to an adequacy decision as referred to in Article 31(1)(a), Europol may forward that information only to a Member State, or a third country concerned with which such agreement has been concluded.

~~3a~~1c. Europol may not transfer personal data to private parties except where, subject to any possible restrictions stipulated pursuant to Article 25(2) or (3) and Article 69:

(a) the transfer is undoubtedly in the interests of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such a consent; or

(b) the transfer is absolutely necessary in the interests of preventing imminent danger associated with crime or terrorist offences; or

(c) the transfer is strictly necessary for the performance of the task set out in Article 4(1)(m) and the following conditions are fulfilled:

(i) the transfer concerns individual and specific cases; and

(ii) no fundamentals rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand.

2. If the ***personal*** data ~~received~~ ***exchanged*** affect the interests of a Member State, Europol shall immediately inform the National Unit of the Member State concerned.

3. Europol shall not contact private parties directly to retrieve personal data.

[4. The Commission shall evaluate the necessity and possible impact of direct exchanges of personal data with private parties within three years after this Regulation is applicable. Such an evaluation shall specify among others the reasons whether the exchanges of personal data with private parties is necessary for Europol.]

---

additional wording clarifying this matter still needs to be agreed with the EP.

Explanation of amendments in Article 32:

- Change of the **title** in order to better reflect the content of the Article.

- **Amendment in paragraph (1c):** the proposal is to some extent based on Article 36aa of the draft Data Protection Directive as currently discussed in the Council. However, certain requirements in Article 36aa seem to be too restrictive.

- **Amendment in paragraph (2)** would aim to ensure that Member States would always know which personal data Europol exchanges.

- **Reinstating paragraph (4):** given the proposed developments in relation to the exchange of personal data with private parties, it might be useful to explicitly foresee the possibility for the Commission to evaluate such exchanges.

The Presidency would also like to draw the attention of delegations to the following developments: the initial Commission proposal for the draft Europol Regulation did not foresee a possibility for Europol to transfer personal data to private parties. Given the operational necessity to process personal data directly received from private parties in order to identify the National Units concerned, the Council in its general approach added paragraph (1a) in Article 32. On the basis of the recent requests by the Council and the European Council to develop internal referral capabilities at Europol, a further opening with the necessary data protection safeguards - as indicated in the proposals above - seems to be necessary in order to ensure that Europol can take appropriate action to secure the removal of certain internet content in voluntary cooperation with online service providers. A further possibility of deleting paragraphs (1a) and (1b) and allowing Europol to receive personal data directly from private parties could maybe be discussed, if delegations consider that there is an operational need for such direct receipt. However, it should be kept in mind that any further amendments in Article 32, apart from paragraph (1a) as indicated in footnote 7, might be rather difficult for the EP to accept.

The Presidency would like to underline that these are initial ideas for discussion and would welcome any comments from delegations which would help to ensure providing the appropriate

legal basis for Europol to comply with the requests by the Council and the European Council in relation to EU IRU.

_____