Council of the
European Union

Brussels, 4 July 2019
(OR. en)

10494/19

LIMITE

ENFOPOL 310
JAI 780
COSI 141

NOTE

From:	Presidency
To:	Delegations
Subject:	Europol's cooperation with strategic partners: strengths and possible inefficiencies in cooperation with Private Parties

Europol's objective is to support and strengthen action by competent authorities of the Member States and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States.[1] In addition to Member States authorities, Europol cooperates with the following partners: Union bodies, third country authorities, international organisations and private parties. This cooperation is regulated in the Europol Regulation Chapter V[2].

[1] Recital 1 of the REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

[2] REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

Large-scale criminal and terrorist networks pose a significant threat to the internal security of the Union and threat assessments show that criminal groups cross borders in a large part of their activities. The Europol Regulation underlines that it is necessary to equip Europol to better support Member States in crime prevention, analyses and investigations.[3] The Presidency's aim is to identify and conclude the Council's views regarding Europol's cooperation with its strategic partners, namely private parties, and the Agency's role in supporting Member States tackling cross-border serious and organized crime.

The foreseen discussion and process in the LEWP are linked to the *Twenty Years of Europol – what next* discussion started at informal COSI, 9th of July. Moreover, the aim is to concretize discussions related to the *Future direction of the EU internal security,* a topic addressed under the Finnish Presidency of the Council.

The LEWP discussion should identify whether the Agency's abilities should be increased and it could thus be more effective in its cooperation with private parties. The initiated discussion focuses exclusively on the articles referring to the cooperation with private parties of the Europol Regulation. The initiative is based on the needs and changes in the operative environment of the law enforcement authorities in the EU. For instance, during the last few years Europol's cooperation needs and assignments with service and internet providers have increased considerably.[4] Serious and organized crime is more and more tackled and prevented online and the cooperation with private parties within the current Europol Regulation could be seen as insufficient.

---

[3] Recital 4 of the Europol Regulation

[4] An example of such cooperation with the service providers is the SIRIUS platform run by Europol together in close cooperation with Eurojust. Sirius is a platform available to law enforcement and judicial authorities developed by Europol and deployed in a closed and secure environment. It is a one-stop shop for authorities to share best practices, know-how and technical information/tools on internet investigations. The platform does not process personal data. Europol has received calls for further expansion of the platform, e.g. to allow processing of open source or requested data for the purposes of cross-referencing of investigations, identification of other ongoing investigations, or enrichment of the data. Currently, Europol's exchange of personal data with private parties is mostly limited to so-called referrals.

The Europol Regulation foresees a full review and evaluation by 1 May 2022 by the Commission. The Commission has indeed launched the procedures for a study into the practice of Europol's direct exchange of personal data with private parties[5]. The results of the study should be available in the first half of 2020. The Presidency assesses that the issue affects the work of the law enforcement authorities of the Member States and Europol in their daily work. Hence the Council, respecting the mandate of the Commission, could provide its input in order to support the Commission in evaluating the Agency's cooperation with its partners and present its views to the Commission and the Member States and their law enforcement authorities well in time. The Presidency notes that Europol's cooperation with private parties touches upon the issue of executive powers of law enforcement authorities and the topic should be addressed thoroughly at the Council. Cooperation and information exchange between Europol and private parties are justified on the basis of the tasks of Europol laid down in the Europol Regulation. Moreover, data protection and privacy as well as other fundamental rights should be taken into account in the process.

Europol's cooperation with private parties - Regulation

In so far as necessary for the performance of its tasks, Europol may establish and maintain cooperative relations with private parties, including the direct exchange of all information with the exception of personal data.[6] The Agency may also conclude working arrangements to formalise such cooperation, and has concluded more than 60 memoranda of understanding with private parties. A further list of private parties for concluding such MoUs was adopted at the 110th Management Board on 1 March 2019.

Its current legal framework largely restricts Europol's possibilities to exchange personal data directly with private parties – such transfers should occur indirectly via a Member State national unit, or the contact point of a third country or international organisation. If Europol receives personal data directly from a private party, it may only process that personal data in order to identify the national authority via which an indirect transfer should take place. In order for Europol to act as the EU information hub and central point of contact for law enforcement in Europe, it should be discussed whether this should also involve the ability to do that in relation to private parties globally with information related to Europe.

5 As foreseen in Article 26(10) of the Europol Regulation
6 Article 23 of the Europol Regulation

Europol’s cooperation with private parties - changes and challenges in the operational environment

The operational environment of law enforcement authorities is rapidly changing. Law enforcement must engage more in its cooperation with strategic partners, such as the private sector. The cooperation with private parties is primordial in a variety of activities of combating and preventing crime. For instance, crime occurs more online or is facilitated by a technological dimension. Law enforcement authorities tackle cybercrime that wouldn't occur without the current and on-going technological development. In addition, some of the previous so-called off-line crime has transferred into the on-line environment, including a growing threat represented by the dark net, and law enforcement authorities are facing new forms of crime. Fraud and related crimes can be seen as one example. Here, both law enforcement authorities' and criminals' methods and actions follow the technological development.

Tackling and preventing cross-border serious and organized crime requires enhanced resources, up to date partnerships and fluent cooperation between various state and non-state actors. Electronic evidence of criminal activities stored on networks and digital infrastructure spread around the world are mostly owned by private entities. Member States and Europol have been investing in combatting cybercrime, which requires a different approach from that which has been traditionally used in respect of most crimes. In practice, cybercrime confronts police forces and other law enforcement authorities with new types of challenges. Cybercrime and cyber attacks require quick responds and new know-how at national and EU level. This calls for much stronger cross-border cooperation and orientation. Cybercrime is a key priority for Europol and within the EU Policy Cycle. Efforts to keep up with the current development should be highlighted.

As regards the cooperation with private parties, certain shortcomings between the reality of policing and the expectations towards Europol have been identified. These expectations do not seem to match with the current legal mandate of Europol. For instance, cooperation with private parties on personal data may be required repeatedly in joint operations specifically on the cybercrime aspects. The current legal framework could be seen as insufficient. Companies are in possession of significant amounts of personal data that can be relevant for Europol’s purposes but they cannot share with the Agency. The data and information is operationally relevant but may lack a specific recipient or victim or is so massive and consistent that the private party does not even report them anymore.

When analysing crime and making threat assessments, the external and internal security of the EU are linked in an inseparable way. Tackling, preventing and combating cross-border serious and organized crime and terrorism call for a strong and all-round network of cooperation. This includes but is not limited to the law enforcement authorities of the Member States and Europol. For instance, during the last few years, Europol's cooperation needs and assignments with service and internet providers have increased considerably. For instance, the GDPR has had an effect on the ability and willingness of other entities like service providers to share or disclose information relevant for investigations with law enforcement authorities, thus affecting the operative environment of law enforcement. In the context of cybercrime investigations, for instance, authorities often rely on so-called WHOIS information about domain name registrations held by private sector organisations responsible for the registration of domain names and the Internet Cooperation for Assigning Names and Numbers (ICANN). Following the entering into force of the GDPR however, these private sector providers of domain name registrations no longer make publicly available WHOIS personal data, which has affected the ability of law enforcement authorities to conduct their criminal investigations. In particular, Europol is currently limited in the extent to which it can exchange this information with private sector domain name registration service providers and is also limited in the extent to which it can facilitate the cooperation between EU law enforcement authorities and domain name registries and registrars.

Cooperation with the private parties is also important in the investigation of terrorism and terrorist financing, as private entities hold much information of potential value. The Europol Financial Intelligence Public Private Partnership (EFIPPP) brings together over a dozen banks and several EU Member States, to share financial information and support efforts to combat terrorist financing. However, the partnership is limited to sharing information at a strategic level because of Europol’s inability to exchange operational data with private entities. Therefore, the partnership’s exchanges are not exploited for operational purposes.

Cooperation with the private sector is crucial also in the context of fighting terrorism online. While the mandate of Europol allows for the Internet Referral Unit (EU IRU) to transfer and receive personal data for the referrals it sends, it is limited in its ability to serve as a channel for private parties to report proactive takedown of content. There is an operational interest to allow for systematic provision of personal data to Europol due to a referral or a proactive takedown of terrorist content. Investigators should have at their disposal a one-stop shop to create, send and receive the results from their requests.

To conclude, it could be useful to discuss areas where crime prevention and investigation could benefit from sharing information between private parties and law enforcement authorities. This information does not only concern the exchange of information on actual suspects, but also information exchange in general, including phenomena and other information held by private entities that can facilitate combatting crime. More generally, cooperation with private parties would also facilitate effective cross-border cooperation and would also enable earlier detection of criminal activities and therefore have an effect on the prevention of serious and organised crime, including cybercrime.

Moreover, the cooperation between Europol and certain private parties is discussed under numerous agenda points of the meetings of LEWP networks and experts groups. Expert groups and networks, such as CARPOL and ENLETS, cooperate with the private sector and international partners on a daily basis. It is worth evaluating, whether the LEWP networks and expert groups could better support Europol in its work with private parties. Law enforcement analysis of the technological development, especially related to artificial intelligence and 5G networks, requires a multi-stakeholder approach involving the relevant EU Agencies, Member States and private businesses. For instance, Europol has launched its analysis regarding the opportunities and challenges for law enforcement in the "Position paper on 5G by Europol" (8268/19), and the CTC has expanded on this topic in “Law enforcement and judicial aspects related to 5G” (8983/19). Key challenges are linked to the identification and localization of users and availability and accessibility of information. Private parties and companies are at the source of technological innovations and have the expertise and knowledge on technology that is misused by criminals. In addition, private parties can have essential information on what is required to detect online criminal activities.

The way forward

The Finnish Presidency invites Member States to express their views on the cooperation between Member State law enforcement authorities, Europol, and private parties; and to discuss possible future activities, e.g. direct exchange of personal data, in this area. In addition, the Presidency seeks the LEWP to take a more active role in addressing Member States' views regarding the legislative work of the EU. Possible suggestions and direction of the future work are based on the discussion related to the following questions.

The Presidency invites the Member States to address the following:

- To what extent does the cooperation between Europol and private parties add value to law enforcement work both at the EU and Member State level? How could the existing cooperation be improved or is there a need to improve it?
- In what other areas would Member States find cooperation between Europol and private parties useful?
- How do Member States assess Europol's cooperation with private parties, when considering key functions of the Agency in supporting Member States tackling cross-border and serious and organized crime? Should some tasks be enhanced? From the Member States' point of view, what are the key operational obstacles to be considered in the cooperation?
- How do Member States assess current procedures related to Europol's cooperation with private parties, especially regarding the exchange of personal data? These procedures are described in the Chapter V, articles 23 and 26, of the Europol Regulation. For instance, the national contact points play a central role in providing and exchanging personal data. How do the Member States evaluate this procedure?
- What risks, if any, do Member States see concerning the existence of otherwise potentially unavailable information in the absence of Europol being able to receive information directly?
- What general safeguards from a Member State perspective would be suitable to address any concerns regarding Europol being able to receive personal data directly?