ANNEX

Study on the practice of direct exchanges of personal data between Europol and private parties

Final Report

HOME/2018/ISFP/FW/EVAL/0077

September 2020

milieu
Law & Policy Consulting

EXECUTIVE SUMMARY

Study objectives, scope and methodology

The *Study on the practice of direct exchanges of personal data between Europol and private parties,* commissioned by DG HOME, **aims to provide a comprehensive overview** of the current practice of **direct exchanges of personal data** between Europol and private parties. The study also provides an overview of how the practice of **indirect exchanges of personal data** between Europol and private parties works. It showcases some possible limitations of both systems, including cases when exchanges of personal data do not take place despite operational needs.

The study was developed based on **desk research**, which did not, however, result in sufficiently robust evidence, given that only a limited amount of literature is publicly available on the subject matter of the study. Therefore, **stakeholder consultation** played a vital role in the implementation of the study. Stakeholder views were gathered via:

- **Scoping interviews**: completed with DG HOME and Europol representatives;
- **Downloadable questionnaire**: completed by representatives of the Europol National Units (ENUs), contact points / competent authorities in third countries or international organisations; national law enforcement authorities (LEAs); national internet referral units (IRUs); national data protection authorities;
- **Online survey**: completed by private parties;
- **Semi-structured interviews**: completed with representatives of national ENUs, contact points / competent authorities in third countries or international organisations; national LEAs; private parties; EDPS, Europol and the Finnish Interior Ministry;
- **Online workshop**: attended by representatives of the ENUs, contact points / competent authorities in third countries or international organisations; national LEAs; private parties; Europol; DG HOME and the Research Team.

The study covers all EU Member States, as well as the United Kingdom, which at the start of the project was still an EU Member State. Some data were also collected in relation to third countries. The study was completed between September 2019 and September 2020.

Sharing of personal data between Europol and private parties in the context of referrals

According to the Europol Regulation, **Europol**, as a general rule, is **prohibited from transferring personal data directly to private parties**. It is allowed to do so in three cases, one of which concerns the subject matter of the study, the so-called **'system of referrals'**. Europol is allowed to transfer personal data directly to private parties if the transfer concerns publicly available personal data, and if it is necessary for preventing and combatting internet-facilitated crimes.

Under the Europol Regulation, Europol may only exceptionally receive personal data directly from private parties. This is allowed under the **'system of responding to referrals'**, under which private parties may decide to transfer personal data to Europol in response to a prior referral.

Within Europol, the **EU IRU is in charge** of flagging online terrorist content for referrals, which is then sent to **OSPs**. The system of referrals is **well-documented** at EU-level and publicly available sources suggest that the **EU IRU sends a large volume of referrals to OSPs**. The EU IRU tracks 'clear-cut' cases, based on the manual tracking of branded terrorist content. These are sent to the OSPs who can then check the referrals against their own terms of references. Whilst the **OSPs are not**

under the legal obligation of taking the online content down, **in the majority of the cases they do so**.

Upon submission of referrals to the ●SPs, Europol **often receives automatically generated responses**. These often merely confirm the safe receipt of the referral, but do not provide Europol with any personal data. **Substantial responses to referrals**, providing some personal data to Europol, are specifically followed up by Europol.

The responses provided by the stakeholders to the survey and the questionnaire suggest that **the system of referrals and responding to referrals is 'partially suitable'**. This seems to result from the fact that it is not suitable for addressing emerging needs, stemming from the increasing willingness of ●SPs to proactively share personal data with Europol, beyond the data contained in the referrals. Whilst the Europol Regulation provides for rules on the proactive sharing of personal data outside the context of referrals, these are perceived to be insufficient by both Europol and the ●SPs. From Europol's perspective, the system of proactive sharing is insufficient in its current form, given that it severely limits Europol's data processing activities. Europol is only allowed to process personal data with the sole purpose of identifying the ENU, which can then resubmit the personal data to Europol. However, the ENUs may not have sufficient grounds to resubmit the data under their legal system, so there is no guarantee that the personal data would ultimately reach Europol. Moreover, while carrying out the limited data processing activity mentioned above, Europol can only rely on the data received from the ●SPs, without having the ability to seek clarification or additional information from the ●SPs. This constitutes a challenge for the identification of the ENUs. From the ●SPs' perspective, proactive sharing can be burdensome and might raise capacity issues, if it necessitates prior data processing at their end, in order to submit tailor-made datasets for the relevant jurisdictions. In many instances, private parties will not be able to identify the relevant jurisdiction based on the data available to them, allowing for the identification of the responsible national ENUs by Europol.

Therefore, **there is a clear need for the revision of the rules of the Europol Regulation on proactive sharing**. Such a revision should allow ●SPs to share personal data with Europol. It should also allow Europol to carry out more extensive data processing activities while analysing the datasets. At the same time the technical and human resources' capacity of Europol should be consolidated. In that respect, it was noted that any proactive sharing from a private party would need to be initiated by that private party in line with Article 6(1)(f) of the General Data Protection Regulation (GDPR).

Europol receiving personal data from private parties via an intermediary

Europol receiving personal data from private parties through an intermediary constitutes the most **'traditional way' of personal data exchange between the private parties and Europol**. Under this system, private parties share personal data with national LEAs, typically because they are subject to the regulatory obligation to do so (e.g. legal obligation to respond to requests received in the context of investigations). Whilst generally, no statistical data are collected on the matter, it seems that **large volumes of personal data are shared by private parties with national LEAs**. Also, it seems that data sharing is relatively fast. However, compared to the actual physical transfer of the data, more time is needed for the preparation thereof.

National LEAs may transfer these data further to the ENUs, which may then pass the personal data on to Europol. Whilst no precise statistical data exist on the matter, it seems that **only a fraction of the personal data shared by the private parties are transferred further from the LEAs to the ENUs**. Also, only a **fraction of these original datasets reaches Europol in the end**, even though these data

could relate to serious and organised cross-border crime. The main reason for national LEAs to refrain from sharing personal data with the ENUs relates to their lack of competence to act on the case (such as no legal basis to initiate an investigation, or no on-going investigation). When ENUs do not transfer the data further, this is mainly due to similar legal reasons.

It seems that the fact that personal data is not always transferred further from the LEAs to the ENUs and from the ENUs to Europol is only one of the **many issues that hinder the functioning of the system**. Some of the other issues concern the speed of the transfer, which is perceived to be slow; collaboration with private parties being challenging; the legal framework being insufficient in providing grounds for the private parties to share personal data with the national LEAs; the legal framework preventing the private parties from sharing multi-jurisdictional personal data with all national LEAs concerned, etc. All of these issues seem to hint towards **the existence of missed opportunities for Europol to receive important datasets from private parties**.

The stakeholders suggested several possible solutions to the current challenges, including:

- Amending the Europol Regulation **reinforcing Europol's capacity to exchange personal data directly with private parties** and to subsequently process these datasets for analytical purposes;
- Amending the national and EU regulatory frameworks, **allowing private parties to share personal data with national LEAs on more grounds** and/or **with an extended group of national competent authorities**;
- Establishing a **platform** for private parties operating in the same sector to **exchange personal data among themselves**; and for **private parties and national LEAs** to **intensify dialogues** leading to the more targeted use of the current system;
- **Designating a person** within the private parties to coordinate the exchanges of personal data with national LEAs;
- **Raising awareness** of stakeholders regarding the current system, thereby reinforcing its use.

Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing)

The system of proactive sharing constitutes a derogation from the traditional way of exchange, whereby Europol receives personal data from private parties through an intermediary. Under the system of proactive sharing, **private parties may transfer personal data directly to Europol**. Europol's data processing activity, however, is limited to the identification of the national ENU. Europol is obliged to transfer the data received from the private parties further to the national ENUs, which may decide to resubmit the datasets to Europol, with or without involving the national LEAs in the resubmission process.

The research did not reveal any statistical data on the use of the system. Evidence suggests, however, that **the system is rarely used**. When used, the **speed** of transfer of personal data between the different actors is **case-specific**. The **involvement of national LEAs** in the context of resubmissions is **not systematic**, but when they are consulted, the LEAs tend to transfer the data back to national ENUs. Multiple reasons may lie behind the decision **not to resubmit the personal data**, including legal reasons, e.g. data sets do not relate to an on-going investigation in the country or do not result in the initiation of investigations.

As the system is rarely used, little information could be gathered on the main shortcomings thereof. Evidence could mainly explain its rare use, which are: the system being **overly complex**; its use being **complicated** in practice; due to the multiple actors involved, the exchange is perceived as **slow**. The **rare use of the system results in missed opportunities** and thus there is a need to reinforce it . Such reinforcement is also necessary to address the challenges of the current systems of referrals and the traditional way of Europol receiving personal data from the private parties through an intermediary (see above).

Possible changes might entail the **revision of the Europol Regulation**, leading to an enhanced capacity of Europol to directly exchange personal data with private parties. These regulatory changes could be coupled with measures to boost the **capacity** of Europol to deal with its enhanced data processing ability.

National law enforcement authorities sharing personal data with private parties via Europol

The study also captures a scenario which is not currently regulated by the Europol Regulation, referring to a presumed operational need. This results from the presumed difficulty faced by national LEAs when trying to obtain personal data from private parties without judicial authorisation or similar. The scenario presumes that national **LEAs might either fail to obtain personal data from private parties this way, or risk receiving incomplete data or data with some delays**. The scenario captures one of the possible solutions to the issue: **Europol acting as an intermediary** between the LEAs and the private parties. The study aimed to verify the existence of the issue and explore whether the suggested solution would be the best approach to overcome the challenge.

The research confirmed a growing need for LEAs to obtain personal data from private parties in their investigations. The research also showed that LEAs face difficulties in obtaining personal data from private parties. This manifests itself in their requests being refused, not answered or the receipt of incomplete or delayed responses from private parties. The research revealed that these issues mainly arise in connection with **cross-border cases**. In the **national context,** the issues arise when the LEAs request personal data from the private parties 'non-officially', e.g. when despite being required by law, requests are being filed without the necessary judicial authorisation or similar.

A number of stakeholders **saw a need for a change of the current system**. Most stakeholders recommended the channelling of the requests and the responses through a dedicated platform, and many stakeholders suggested Europol in that regard. Some others were doubtful about the intermediary role Europol might play between the private parties and the LEAs, noting that the source of the request (whether it comes from Europol or the national LEAs) is irrelevant for private parties. These stakeholders reiterated the importance of receiving official requests. Some stakeholders also suggested the establishment of platforms for the exchange of good practices.