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

Final Report

TABLE OF CONTENTS

LIST OF ABBREVIATIONS 5
ABSTRACT 6
EXECUTIVE SUMMARY 7
1 INTRODUCTION 11
1.1 Study objectives and scope 11
1.2 Structure of the study 11
2 BACKGROUND TO THE DIRECT AND INDIRECT EXCHANGES OF PERSONAL DATA . 12
2.1 Direct exchanges of personal data 12
2.2 Indirect exchanges of personal data 13
3 METHODOLOGY 17
3.1 Desk Research 17
3.2 Stakeholder consultation 18
3.3 National-level stakeholders – Questionnaires 19
3.3.1 Private party stakeholders – Online survey 24
3.3.2 Selected stakeholders - Semi-structured interviews 25
3.3.3 Workshop 27
4 ANALYSIS OF FINDINGS 29
4.1 Direct exchanges of personal data 29
4.1.1 Sharing of personal data between Europol and private parties in the context of referrals 29
4.2 indirect exchanges of personal data 35
4.2.1 Europol receiving personal data from private parties via an intermediary 35
4.2.2 Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) 52
4.2.3 National law enforcement authorities sharing personal data with private parties via Europol 63
5 CONCLUSIONS AND RECOMMENDATIONS 70
ANNEXES 72
Annex 1 – Bibliography 72
Annex 2 – Survey questionnaire targeting private parties 74
Profiling questions: 74
1. Sharing of personal data between Europol and private parties in the context of referrals 76
1. a. Europol transferring (publicly available) personal data to you as a private party via referrals 76
1.b. Your organisation responding to a referral received from Europol 78
2.a. Private parties sharing personal data with national law enforcement authorities 80

2.b. Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) 84
2.c. National law enforcement authorities sharing personal data with private parties via Europol 87
Annex 3 – Downloadable questionnaire targeting the ENUs 88
Profiling questions: 88
1. Sharing of personal data between Europol and private parties in the context of referrals 90
1.a. Europol transferring (publicly available) personal data to a private party via referrals 90
1.b. Private party responding to a referral received from Europol 90
2.a. Private parties sharing personal data with national law enforcement authorities 91
2.b. Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) 93
Annex 4 – Downloadable questionnaire targeting the LEas 96
Profiling questions: 96
1. Sharing of personal data between Europol and private parties in the context of referrals 98
1. a. Europol transferring (publicly available) personal data to a private party via referrals 98
2.a. Private parties sharing personal data with national law enforcement authorities 98
2.b. Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) 101
2.c. National law enforcement authorities for sharing personal data with private parties via Europol 103
Annex 5 – Downloadable questionnaire targeting the national IRUs 105
Profiling questions: 105
1. Sharing of personal data between Europol and private parties in the context of referrals 107
1.a. Europol transferring (publicly available) personal data to a private party via referrals 107
2.a. Private parties sharing personal data with national law enforcement authorities 110
2.b. Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) 110
Annex 6 – Downloadable questionnaire targeting the national Data protection authorities 111
Profiling questions: 111
1. Sharing of personal data between Europol and private parties in the context of referrals 113
1.a. Europol transferring (publicly available) personal data to a private party via referrals 113
1.b. Private party responding to a referral received from Europol 113
2.a. Private parties sharing personal data with national law enforcement authorities 115
2.b. Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) 116

This Final Report has been prepared by Milieu Consulting SRL under Contract No. HOME/2018/ISFP/FW/EVAL/0077.

Milieu Consulting SRL (Belgium), Chaussée de Charleroi 112, B-1060 Brussels, tel.: +32 2 506 1000; e-mail: claire.dupont@milieu.be, katalin.csaszar@milieu.be and anthea.galea@milieu.be; web address: www.milieu.be.

LIST OF ABBREVIATIONS

DG HOME – European Commission, General Directorate for Migration and Home Affairs

DPA – Data Protection Authority

EC3 – Europol's European Cybercrime Centre

EDPS – European Data Protection Supervisor

EU – European Union

EU IRU – Europol's Internet Referral Unit

Europol – European Union Agency for Law Enforcement Cooperation

ENUs – Europol National Units

GDPR – General Data Protection Regulation (EU) 2016/679

HENU – Heads of Europol National Units

OSPs – Online Service Providers

IRUs – Internet Referral Units

LEAs – Law Enforcement Authorities

NCMEC - National Center for Missing and Exploited Children

NGOs – Non-Governmental Organisations

PP – Private party

PPP - Public-Private Partnerships

ABSTRACT

The *Study on the practice of direct exchanges of personal data between Europol and private parties,* commissioned by DG HOME, aims to provide an overview of the current practice of direct and indirect exchanges of personal data between Europol and private parties, including cases when exchanges of personal data do not take place despite operational needs.

The study was developed based on desk research and the following stakeholder consultation methods: scoping interviews, questionnaire and online survey, semi-structured interviews and an online workshop.

The study's main findings are the following:

- System of referrals and responses to referrals: the system functions well and it is well-documented. However, online service providers (OSPs) and Europol would both see benefits in exchanging personal data directly, outside the context of referrals. The current system of proactive sharing, as regulated by the Europol Regulation, is not suitable to address these operational needs. Therefore, its revision, empowering Europol with more extensive data processing ability, is recommended;
- Europol receiving personal data from private parties via an intermediary: the system is commonly used; however, only a fraction of personal data from the private parties reaches Europol. Therefore, it is recommended to reinforce Europol's capacity to exchange personal data directly with private parties. Other recommendations include raising awareness about the system to reinforce its use, the revision of the regulatory framework to allow private parties to share personal data with the national law enforcement authorities (LEAs) on more grounds or with an extended group of national authorities, etc.;
- Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing): the system is rarely used, as it is perceived to be complex, complicated and slow. Its rare use results in missed opportunities. Therefore, it is recommended to reconsider the provisions of the Europol Regulation to allow for direct exchanges of personal data with private parties, and to empower Europol with a more extensive data processing mandate;
- National LEAs sharing personal data with private parties via Europol: the study proved that LEAs often require access to personal data held by private parties during their investigations, but might face obstacles when trying to obtain personal data from private parties. Channelling requests from LEAs to private parties through a dedicated platform such as Europol was one of the solutions recommended by the stakeholders.

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 interview**s: completed with representatives of 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 also 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 OSPs, 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 OSPs 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 OSPs. 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 OSPs, without having the ability to seek clarification or additional information from the OSPs. This constitutes a challenge for the identification of the ENUs. From the OSPs' 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 OSPs 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 exchanging personal data 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 ongoing 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 ongoing 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 its main shortcomings. Evidence could mainly explain its rare use: the system being **overly complex**; its use being **complicated** in practice; and due to the multiple actors involved, the exchange is perceived as **slow**. As the **system is rarely used it 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 'unofficially', 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.

1 INTRODUCTION

1.1 STUDY OBJECTIVES AND SCOPE

This study has been commissioned by the European Commission's Directorate General for Migration and Home Affairs (hereinafter: DG HOME) under the title *Study on the practice of direct exchanges of personal data between Europol and private parties* (request for service HOME/2018/ISFP/FW/EVAL/0077).

The study will feed into the European Commission's report on the evaluation of the practice of the direct exchanges of personal data with private parties, the preparation of which is foreseen by Article 26(10) of Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (hereinafter: Europol Regulation)[1]. The report is to be presented to the Council and the European Parliament.

In line with the above, the current study **aims** to provide the European Commission with a comprehensive overview of the current practice of the **direct exchanges** of personal data between the European Union Agency for Law Enforcement Cooperation (hereinafter: Europol) and private parties, including some lessons learned from the current practice and, to the extent applicable, the limitations thereof.

The study acknowledges that personal data is also exchanged with Europol through indirect ways. Therefore, it also provides an overview of how the practice of the **indirect exchanges** of personal data between Europol and private parties works. Moreover, it showcases some possible limitations of the system, including cases when the indirect exchanges of personal data between Europol and the private parties do not take place, despite the operational needs.

The study has assessed the practices of the direct and indirect exchanges of personal data between Europol and the private parties in **all Member States**[2]. Some data were also collected from third countries.

1.2 STRUCTURE OF THE STUDY

This study is structured as follows:

- **Section 2: Background to the direct and indirect exchanges of personal data.** This section outlines the main provisions of the Europol Regulation relating to the direct and indirect exchanges of personal data between Europol and private parties, thereby defining how the two practices are intended to work in practice.
- **Section 3: Methodology.** This section outlines our methodological approach to the study and the tasks carried out for its completion. It also sets out some methodological limitations that were encountered during the completion of the study.
- **Section 4: Analysis of the direct and indirect exchanges of personal data.** This section outlines the results of the study, structured around the existing practices used for the exchanges of personal data between Europol and private parties.
- **Section 5: Conclusions and recommendations.** This section provides a set of overall conclusions and recommendations as to how the current practices could be changed.

[1] 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, OJ L 135, 24.5.2016, p. 53–114, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1591603899224&uri=CELEX:32016R0794.

[2] This also includes the United Kingdom, which at the time of signature of the contract for the study was still considered an EU Member State.

2 BACKGROUND TO THE DIRECT AND INDIRECT EXCHANGES OF PERSONAL DATA

Prior to describing the existing practices, it is important to clarify the notion of the term **'private party'**. As set out in Article 2(e) and (f) of the Europol Regulation, private parties are entities or bodies established under the law of a Member State or a third country. This category includes companies, firms, business associations, non-profit organisations and other legal persons. It does not cover international organisations.

It is also noted that in the context of the study, the term **'personal data'** refers to any information on a data subject that relates to, or could relate to, preventing and combatting serious crime, terrorism or forms of crime that affect the common interests of the Union, affecting two or more Member States.

The term **'transfer'** captures any 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.

2.1 DIRECT EXCHANGES OF PERSONAL DATA

The direct exchanges of personal data between Europol and private parties is regulated by Article 26(3) and (5) of the Europol Regulation.

Under the current regulatory framework, as a general rule, Europol is **prohibited from transferring personal data directly** to private parties. Article 26(5) of the Europol Regulation sets out three **exceptions** to this rule::

- If the transfer is undoubtedly in the interest of the data subject;
- If the transfer is absolutely necessary in the interest of preventing the imminent perpetration of a crime;
- If the transfer concerns publicly available data and is strictly necessary for preventing and combatting crimes, which are facilitated, promoted or committed by using the internet[3] (hereinafter: **referrals**).

In all three cases mentioned above, the direct transfer of personal data may only happen in the context of specific and individual cases. The direct transfer of personal data are subject to the restrictions stipulated by Article 19(2) and (3) of the Europol Regulation. In accordance with this provision, Member States, Union bodies, third counties and international organisations while providing information to Europol, may restrict access rights to this information or otherwise restrict the use or processing of information by Europol, including its transfer. Europol has to comply with these restrictions, also in the context of the direct transfer of personal data to private parties.

Moreover, the direct exchanges of personal data should respect the rules on the obligations of discretion and confidentiality and on the protection of sensitive non-classified information, as set out in Article 67 of the Europol Regulation.

The direct receipt of personal data is also regulated by Article 26(3) of the Europol Regulation, setting out rules for receiving personal data from private parties, as a **response to a referral**. In accordance with this system, Europol may receive in connection with the transfers of referrals, personal data directly from private parties. Such a data transfer is conditional upon the private party declaring that it is legally allowed to transmit the personal data to Europol, in accordance with the laws applicable thereto, in order

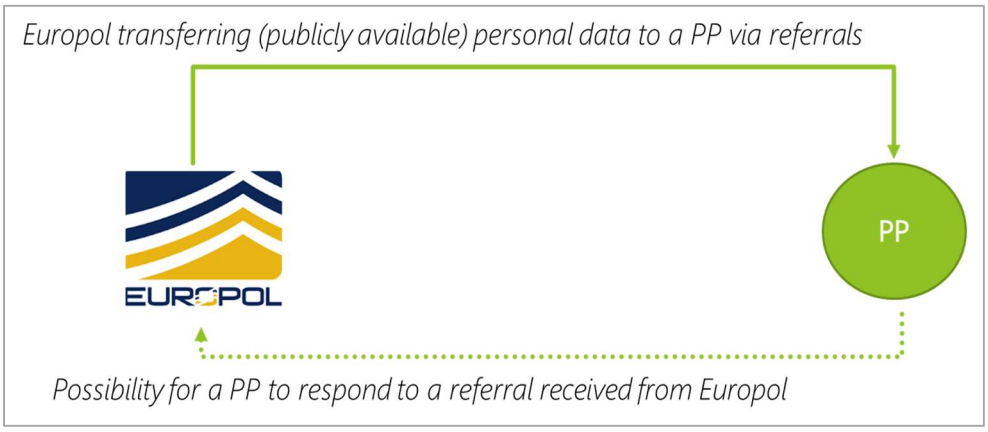
[3] See Article 4(1)(m) of the Europol Regulation.

for Europol to prevent and combat crimes, which are facilitated, promoted and committed by using the internet.

The current study focuses on the systems of referrals and responses to referrals. Thus, each time the study mentions the concept of 'direct exchanges of personal data', it refers only to these two systems.

This practice is illustrated in the figure below.

Figure 1: Direct exchanges of personal data between Europol and private parties (PP)



2.2 INDIRECT EXCHANGES OF PERSONAL DATA

The indirect exchanges of personal data between Europol and private parties is mainly regulated by Article 26(1) and (2) of the Europol Regulation[4].

These provisions set out rules for two systems:

- Europol receiving personal data from private parties via an intermediary;
- Private parties sharing personal data with Europol proactively, outside the context of referrals (hereinafter: proactive sharing).

The first system, regulated by Article 26(1) of the Europol Regulation, refers to the case when **Europol receives personal data from private parties through**:

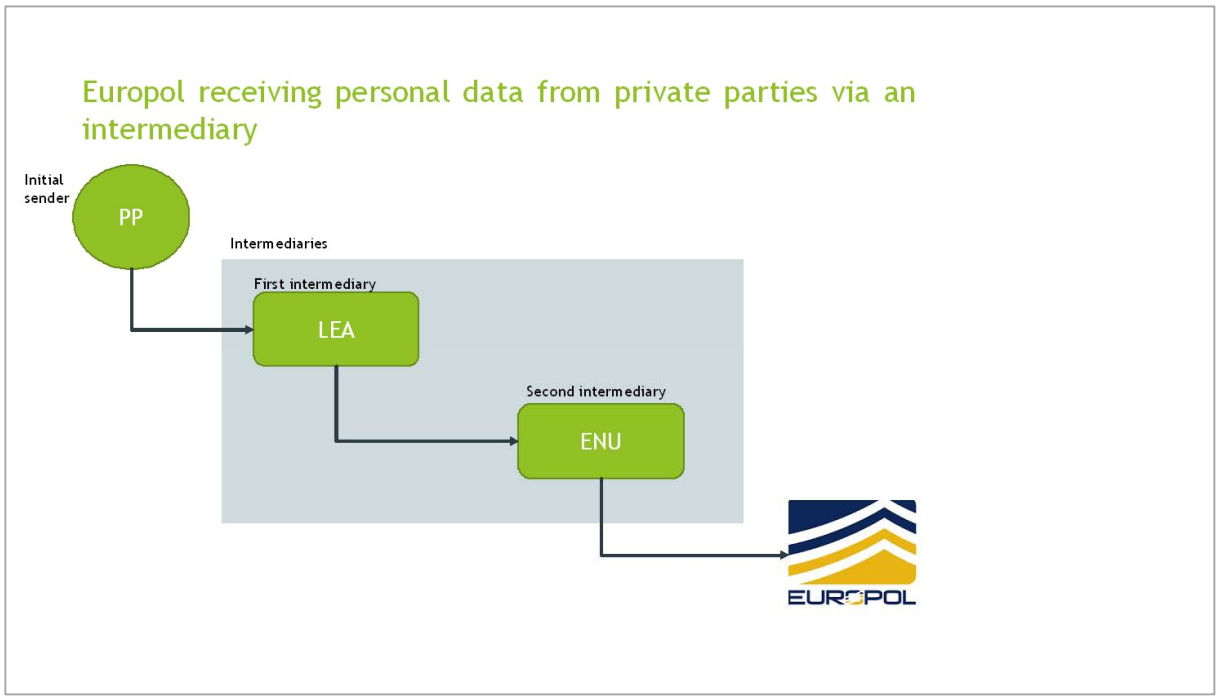
- An ENU;
- A contact point in a third country or international organisation with which Europol has concluded a cooperation agreement, allowing for exchanges of personal data;
- An authority of a third country or an international organisation, which is subject to an adequacy decision[5] or with which the European Union (EU) has concluded an international agreement[6].

[4] It is noted that Article 26(4) and (9) also contains some relevant provisions, which are not, however, covered by this study.
[5] Pursuant to Article 25(1)(a) of the Europol Regulation, adequacy decision is a decision of the European Commission, finding that a third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of data protection. See also, Article 36 (on the transfers on the basis of an adequacy decision) of Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
[6] Pursuant to Article 218 of the Treaty on the functioning of the European Union, international agreements are agreements concluded between the European Union and third countries or international organisations.

It is noted that the aforementioned organisations would typically act as a second intermediary between private parties and Europol. As further described under *Section 4: Analysis of the direct and indirect exchanges of personal data*, private parties typically transfer personal data to national law enforcement authorities first (hereinafter: LEA), which then transfer the personal data to the ENUs, contact points or authorities in third countries or international organisations. These organisations would then transfer the data forward to Europol.

This practice is illustrated in the figure below.

Figure 2: Europol receiving personal data from private parties via an intermediary



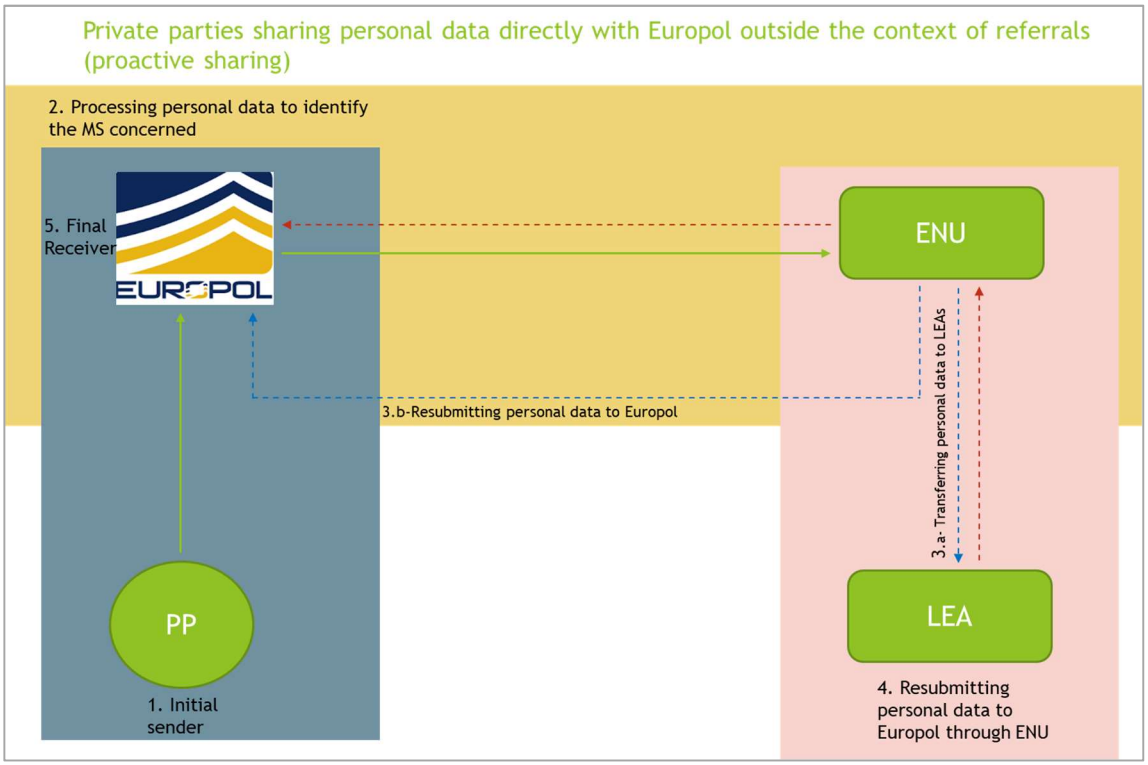
The second system, regulated by Article 26(2) of the Europol Regulation, refers to the case when Europol receives personal data directly from private parties, by means other than as a response to a referral (**proactive sharing**). In these cases, Europol may process the personal data received from the private parties, solely with the purpose of identifying the responsible ENU, contact point or authority in a third country or international organisation.

Europol should immediately transfer the personal data concerned to these entities. Europol should delete the personal data received from the private parties within four months after the transfer takes place, unless the ENU, contact point or authority concerned resubmits the same personal data.

The ENU, contact point or authority concerned might resubmit the personal data to Europol, on the basis of its own decision, when such powers are granted thereto. Alternatively, the ENU, contact point, or authority concerned would first have to transfer the personal data to the national LEA, for the latter to consider possible actions, which might entail the resubmission of personal data to Europol through the ENU, contact point or authority in a third country or international organisation. It is noted that neither the ENU, contact point or authority in a third country or international organisation, nor the national LEAs are under an obligation to resubmit the personal data to Europol.

This practice is illustrated in the figure below.

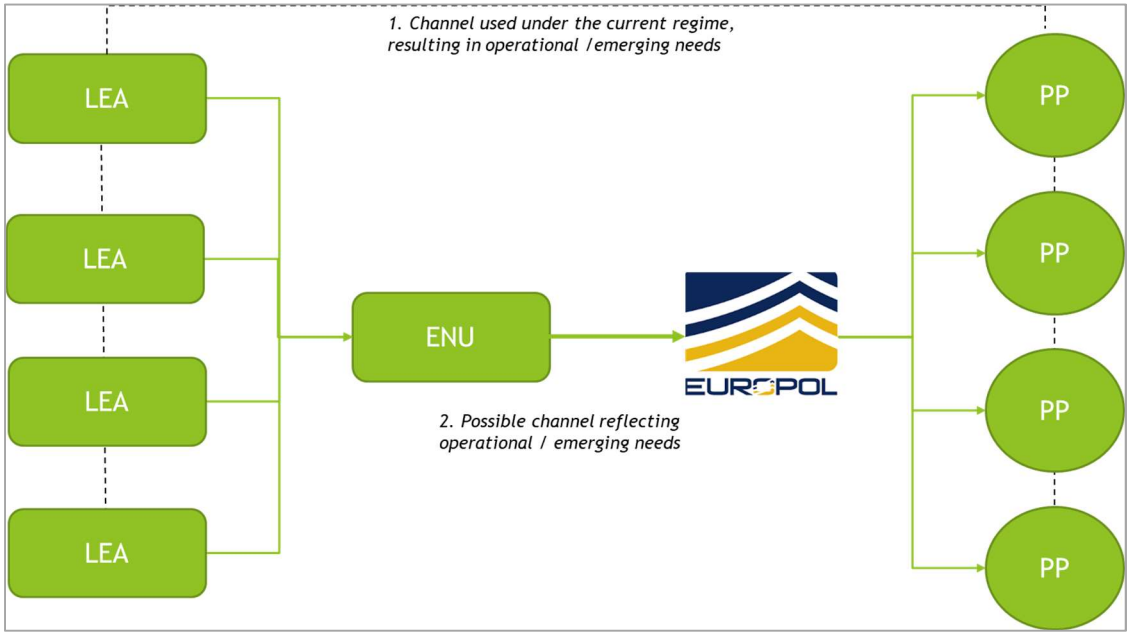
Figure 3: Private parties (PP) sharing personal data directly with Europol outside the context of referrals (proactive sharing)



This study also covers a **scenario** which is not currently regulated by the Europol Regulation. Considering that this scenario also entails the involvement of intermediaries, it is presented under this section of the study, dedicated to the indirect exchanges of personal data between Europol and private parties. This scenario captures a presumed operational need, resulting from the potential difficulties faced by national LEAs when trying to obtain personal data from private parties without a judicial authorisation or similar. It is understood that national LEAs might fail to obtain personal data from private parties this way, or might risk receiving only partial data, or data with some delays. In connection with this particular scenario, the study aims to verify the existence of this operational need and map possible solutions thereto, including the possibility for private parties to share personal data with national LEAs via Europol. As the national LEAs typically coordinate with Europol via the ENUs, the possible channel for the transfers of personal data between the LEAs and the private parties, also factors in a role for this organisation.

This scenario is illustrated in the figure below.

Figure 4: National law enforcement authorities (LEA) obtaining personal data from private parties (PP) via Europol



3 METHODOLOGY

This section describes the methodology that guided the design and implementation of the study. It presents the data collection methods used for the completion of the study and provides an overview of the challenges and limitations encountered while implementing them.

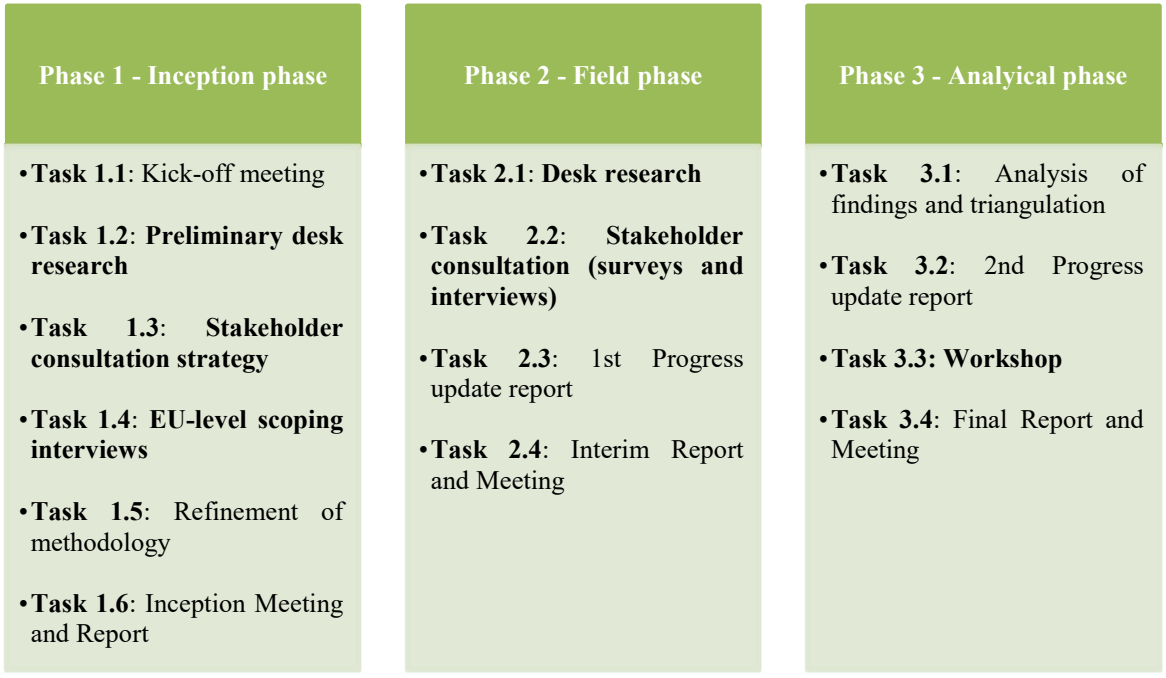
The work on the study took place between September 2019 and September 2020 and consisted of three phases:

- **Phase 1: Inception phase**. Phase for the refinement of the methodological approach and tools and the identification of stakeholders;
- **Phase 2: Field phase**. Information collection phase;
- **Phase 3: Analytical phase**. Phase for the analysis of the information gathered and its presentation in the form of the current study.

These phases were completed as a series of tasks, and regular communication with the client was ensured by means of regular meetings and reporting.

The figure below provides an overview of all phases and tasks of the study, the meetings held with DG HOME and all formal deliverables.

Figure 5: Approach to study implementation



The narrative below provides an overview of the methodological tools used for data collection under the study. Related tasks are bolded in the figure above.

3.1 DESK RESEARCH

The Research Team carried out extensive **desk research** (Tasks 1.2 and 2.1) in order to identify and analyse literature on the topic of the study.

In carrying out the desk research, the Research Team consulted **the following sources**:

- Websites of the following EU institutions and agencies: European Commission, Council of the European Union; European Parliament, Europol and the European Data Protection Supervisor (EDPS);
- Relevant documents shared by DG HOME and stakeholders;
- Other open source information.

The amount of publicly available information on the exchanges of personal data between Europol and private parties is **limited**. To tackle this challenge, the Research Team asked several stakeholders to share information in this regard, namely the desk officers of DG HOME, officers from Europol and EDPS and stakeholders who were interviewed as part of the stakeholder consultation.

Annex 1 to this study provides the list of literature consulted during the implementation of the study.

3.2 STAKEHOLDER CONSULTATION

Due to the limited amount of publicly available literature on the exchanges of personal data between Europol and private parties, as well as to ensure the robustness of the information gathered, stakeholder consultation (Tasks 1.4, 2.2 and 3.3) played a vital role in the implementation of the project. Through the **various stakeholder consultation activities**, the Research Team aimed to involve a variety of stakeholders, bringing in a blend of theoretical, practical and operational expertise as well as knowledge of the relevant provisions of the Europol Regulation.

A combination of **different consultation tools** was prepared to target different stakeholders with the aim of gathering high-quality and balanced input from the stakeholders.

The sections below provide an overview of the different stakeholders consulted, the consultation tools used to target the stakeholders, the approach taken towards dissemination of the consultation tools and the difficulties encountered by the Research Team and the means used to mitigate these.

3.2.1 EU-level stakeholders – Scoping interviews

Officials from **DG HOME and Europol** were consulted at the beginning of the project in order to provide the Research Team with a further understanding of the current practices of direct and indirect exchanges of personal data between Europol and private parties, the emerging needs, the private parties most involved in these exchanges of personal data, as well as to collect documents relevant for the study.

These face-to-face scoping interviews were carried out by the Research Team with the following stakeholders:

Table 1: Stakeholders targeted by the scoping interviews

Stakeholder	Stakeholder representatives
European Commission	▪ DG HOME, Counter-Terrorism Unit ▪ DG HOME, Radicalisation Unit ▪ DG HOME, Cybercrime Unit ▪ DG HOME, Organised Crime Unit
Europol	▪ EU Internet Referral Unit ▪ Cybercrime Centre, EC3 ▪ Representative of the Analysis project, Counterfeiting of Goods ▪ Legal Affairs Unit

On 25 November 2019, the Research Team held a **follow-up meeting with the Europol representatives** in the Hague, to discuss the content of the future questionnaires. The meeting was also attended by the DG HOME officials responsible for the study.

3.3 NATIONAL-LEVEL STAKEHOLDERS – QUESTIONNAIRES

National LEAs, ENUs, and contact points / competent authorities in third countries or international organisations, national **Internet referral units** (IRUs) and **data protection** authorities were identified as important stakeholders to consult due to their knowledge of and experience with exchanging personal data between Europol and private parties.

The table below provides an overview of the **reasons** why these stakeholders were targeted during the stakeholder consultation.

Table 2: Reasons for the selection of stakeholders

Stakeholder	Reasons for selection
LEA	LEAs play a central role in the context of indirect exchanges of personal data between Europol and private parties. LEAs collect or request personal information from private parties which can then be passed on to the ENU for onward submission to Europol in cross-border cases. On the other hand, the LEAs may play a role when private parties share personal data directly with Europol outside the context of referrals (proactive sharing), in which case the personal data needs to be processed and resubmitted to Europol via the ENU with the possible involvement of the LEA. Finally, the LEAs needed to be consulted in the context of the fictional scenario, reflecting upon the existence of potential operational needs.
ENUs, contact points / competent authorities in third countries or international organisations	ENUs, contact points / competent authorities in third countries or international organisations, are involved in the indirect exchanges of personal data and have a coordinating role between the LEAs and Europol.
National IRUs	National IRUs with responsibilities similar to the EU IRU were consulted to understand the main differences between the national and the EU referral systems and to gain an understanding of how the national IRUs perceive the current practice of direct exchanges of personal data between Europol and the private parties.
Data protection authorities	National data protection authorities were consulted to better understand possible data protection issues around the transfers of personal data through the direct and indirect channels.

Downloadable questionnaires were considered to be the best methodological tools to target these groups of stakeholders. The questionnaires were prepared and circulated in Word format to allow the stakeholders to download them, circulate them among colleagues and coordinate within the same unit and/or department, and provide one coordinated reply on behalf of their respective organisation. The downloadable questionnaires designed for the different stakeholder groups are provided in *Annexes 3 to 6* to this Final Report.

The questionnaires were prepared based on the information collected during the preliminary desk research, the EU-level scoping interviews and the meeting held in The Hague in November 2019. The

questionnaires were structured around the different forms of direct and indirect exchanges of personal data, as defined under *Section 2: Background to the direct and indirect exchanges of personal data*.

To target the **relevant LEAs and the IRUs** from all the Member States, the Research Team relied on the contact list of the Heads of Europol National Units (HENU) Group representatives shared by DG HOME / Europol. The HENU Group representatives were contacted by the Research Team and were asked to provide the most relevant national contacts of their respective national LEAs and the national IRUs. This approach aimed to ensure that the questionnaire reaches those national level stakeholders who have experience with the sharing of personal data between Europol and private parties.

The main difficulties faced by the Research Team related to the low response rate and/or late responses from some of the HENU Group representatives when sending national contacts for LEAs and IRUs. To address the low response rate of the HENU Group Representatives, reminders were sent, and telephone calls were held. This caused a delay in targeting the LEAs and IRUs with the respective questionnaires. When the contacts of the national LEAs and IRUs were shared with the Research Team, the respective questionnaire was circulated to the contact points. Several reminders were sent by the Research Team to the LEA and IRU contact points to ensure a high response rate.

Table 3: Responses to the LEA and IRU questionnaires

Contacted States	**Responses**	
	LEA Questionnaire	IRU Questionnaire
Member States of the European Union		
Austria		
Belgium		✓
Bulgaria	✓	✓
Croatia		
Czech Republic		
Cyprus		
Denmark		
Estonia		
Finland		
France	✓	
Germany	✓	✓
Greece	✓	✓
Hungary	✓	✓
Ireland		
Italy		
Malta		✓
Poland	✓	
Romania	✓	
Slovakia		
Slovenia	✓	✓
Spain	✓	
Sweden	✓	✓
United Kingdom[7]		
Non-Member States of the European Union		
Albania		
Australia		
Canada	✓	

[7] This study covers the United Kingdom as at the start of the project, the United Kingdom was still a Member State of the European Union.

Contacted States	Responses	
	LEA Questionnaire	IRU Questionnaire
Columbia		
Georgia		
Iceland		
Liechtenstein	✓	
Monaco	✓	
North Macedonia		
Serbia	✓	✓
Switzerland	✓	✓
Ukraine		
United States of America		
Total No. of States contacted: 36		
Total No. of responses:	39 responses from 15 states	11 responses from 10 states

In targeting the **ENUs, contact points / competent authorities** in third countries and international organisations, the Research Team relied on the HENU Secretariat to forward the questionnaire to the HENU Group representatives. The main difficulties faced by the Research Team related to the low response rate from the HENU Group in answering the questionnaire. In addition, the HENU Group was targeted via two different channels: by the Research Team to provide contacts for the LEAs and the IRUs, and by the HENU Secretariat to reply to the questionnaire addressed to the ENUs. This caused some lack of clarity as to what was required by the HENU Group which was rectified by the Research Team by means of a clarification email circulated to the HENU Group. The Research Team provided the HENU Group with all the necessary clarifications, including explaining via email which questionnaire concerned them, thereby reducing any risk or error. It is also noted that the title of the questionnaire specified its target group, thus made it clear that it targeted the ENUs, contact points / competent authorities in third countries or international organisations, exclusively. Notwithstanding, some respondents did not identify themselves as ENUs, contact points / competent authorities in third countries or international organisations when completing the related profiling question of the questionnaire. Rather, some marked themselves as, for example representatives of the LEA or representatives of the IRU. In fact, some ENUs would typically belong to the LEAs or in some Member States, the ENUs would consist of representatives of different authorities, e.g. customs or police. In view of this and in order to avoid arbitrary decisions on what answers to keep and discard, all replies to this questionnaire were taken into consideration.

The profile of the respondents was systematically checked via the interviews with the selected stakeholders, as the issue referred to above was already identified prior to the interviews.

Table 4: Responses to the questionnaire for ENU, contact points / competent authorities in third countries and international organisations

Contacted States	Responses
Member States of the European Union	
Austria	✓
Belgium	✓
Bulgaria	✓
Croatia	✓
Cyprus	✓
Czech Republic	✓
Denmark	✓
Estonia	✓
Finland	✓
France	
Germany	✓
Greece	✓
Hungary	✓
Ireland	
Italy	
Latvia	✓
Lithuania	✓
Luxembourg	✓
Malta	
Netherlands	✓
Poland	✓
Portugal	✓
Romania	✓
Slovakia	✓
Slovenia	✓
Spain	✓
Sweden	✓
United Kingdom	✓
Non- Member States of the European Union	
Albania	
Australia	
Canada	✓
Columbia	
Georgia	
Iceland	✓
Liechtenstein	
Moldova	
Monaco	
Montenegro	
North Macedonia	✓

Contacted States	Responses
Norway	
Serbia	
Switzerland	
Ukraine	
United States of America	
Total No. States contacted: 44	
Total No. of responses: 44 responses from 27 states	

To target the **data protection authorities**, the Research Team relied on the circulation of the respective questionnaire through the Europol Cooperation Board. The Europol Cooperation Board is an advisory body which facilitates cooperation between the EDPS and the national supervisory authorities[8]. Given this role, the Europol Cooperation Board was considered as the best channel to reach out to all of the Member States' data protection authorities. The main difficulties encountered by the Research Team were the late approval by the Europol Cooperation Board of the request to circulate the questionnaire to the national data protection authorities, as well as the low response rate from the national data protection authorities. In order to mitigate the low response rate, the Research Team – via the Europol Cooperation Board – sent several reminders to the national data protection authorities and the deadline for submission of the questionnaires was extended. However, the response rate remained low.

Table 5: Responses to the questionnaire for DPAs

Contacted DPAs	Responses
Austria	
Belgium	
Bulgaria	
Croatia	
Cyprus	✓
Czech Republic	
Denmark	
Estonia	✓
Finland	
France	
Germany	
Greece	
Hungary	✓
Ireland	
Italy	
Latvia	✓
Lithuania	
Luxembourg	
Netherlands	
Malta	✓
Poland	

[8] Article 45 of Regulation (EU) 2016/794

Contacted DPAs	Responses
Portugal	
Romania	
Slovakia	✓
Slovenia	
Spain	
Sweden	
United Kingdom	
Total No. of DPAs contacted: 28	
Total No. of responses: 6	

3.3.1 Private party stakeholders – Online survey

Private parties were another group of stakeholders targeted during the stakeholder consultation due to their central role in exchanging personal data directly or indirectly with Europol. Several different types of private parties were identified as stakeholders namely, private parties from the financial sector, online service providers, internet service providers, payments and payment technology companies, mobile network operators, representatives of the tele-communications' sector, e-commerce services, airline industry, courier and postal services, and non-governmental organisations (NGOs).

An online survey tool disseminated through SurveyGizmo[9] was used to target the different types of private parties. Similarly to the questions prepared for the questionnaires (See Section 3.2.2), the questions for the private parties were prepared based on the information collected throughout the desk research, the EU-scoping interviews and the meeting held in The Hague on 25 November 2019, and were structured around the different systems used for the exchanges of personal data between Europol and the private parties. The survey questions are provided in *Annex 2* to this Final Report.

To target the private parties from all the relevant sectors, the Research Team relied on desk research to identify relevant contacts, as well as a list of contacts provided by DG HOME. Europol was also consulted to assist in completing this list. The Research Team contacted the private parties, which included some individual organisations, as well as some umbrella organisations and shared the link to the online survey. The response rate to the online survey was very low. In order to address this challenge, several reminders were sent to the private parties. In addition, after consultation with DG HOME, a list of 'must-have' private parties – whose input was considered essential for the study - was identified. Private parties on this list were contacted once again, urging them to provide their contributions to the online survey.

It is noted that the online survey tool registers the number of people who have accessed the survey, including those who did not necessarily complete and submit responses. For the purpose of this Study, the Research Team has taken into consideration only those responses that were completed and submitted by respondents.

[9] SurveyGizmo is an online survey solution that makes it easy for businesses of all sorts to create and conduct surveys, polls, quizzes, and questionnaires.

Table 6: Responses to the online survey

Type of stakeholders contacted	No. of stakeholders contacted	No. of completed responses
Airline industry	5	/
Couriers and postal services	2	/
Cybersecurity	1	/
E-commerce services	5	/
Financial institutions, Payments and payment technology companies	17	6
Internet service providers; Online content providers; Audio-visual media content providers	14	3[10]
Mobile network operators	1	/
Non-profit organisations	5	3[11]
Tele-communications	3	/
Other	/	1
Total No. of stakeholders contacted: 53		
Total No. of completed responses: 13		

3.3.2 Selected stakeholders - Semi-structured interviews

After the collection of all responses from the national-level stakeholders and the private parties (see sub-sections 3.2.2 and 3.2.3), the Research Team carried out a **preliminary analysis of the replies** in order to map out the stakeholders to be invited for a semi-structured interview. In line with the reasons provided in the above sub-sections as to the practical involvement of LEAs, ENUs and private parties in the exchanges of personal data, the Research Team targeted this group of stakeholders for the semi-structured interviews.

By analysing the replies provided to the questionnaires and the online survey by the LEAs, ENUs and private parties, the Research Team identified a **balanced group of stakeholders** which could provide further information on the direct and indirect exchanges of information, obstacles encountered when exchanging information, practices and/or suggestions which could improve the current exchange of personal data. When selecting LEAs and ENUs, the Research Team also ensured a balanced geographical coverage. As for the selection of private parties, the Research Team sought to keep a balance of the different sectors represented by the private parties. The selection of the private party interviewees also took into account the fact that one important stakeholder group (Internet service providers, Online content providers, Audio-visual media content providers), provided a very limited contribution to the survey, especially in the context of the direct exchanges of personal data between Europol and the private parties. To ensure that the stakeholders from the internet service providers, online content providers, and audio-visual media content providers were adequately represented during the semi-structured interviews, the Research Team reached out to private parties within this stakeholder group other than those that contributed to the survey.

Moreover, the Research Team **also targeted**:

[10] It is noted that three of these organisations self-identified as 'other' organisations. Given their activities, as well as the way the Research Team, DG HOME and Europol had originally categorised them, they should have categorised themselves under the category 'Internet service providers; Online content providers; Audio-visual media content providers'.
[11] It is noted that one of these organisations self-identified as 'other' organisation. Given its activities, as well as the way the Research Team, DG HOME and Europol had originally categorised the organisation, it should have categorised itself under the category of 'non-profit organisation'.

- a representative of the Finnish Interior Ministry who was involved in the development of the Council Conclusions on Europol's Cooperation with Private Parties during the Finnish Presidency[12] in order to provide the Research Team with a better understanding of the context within which the Council Conclusions were discussed among the Member States in Council;
- a representative of the Croatian Presidency holding the rotating Presidency of the Council of the European Union between 1 January and 30 June 2020, to understand the state-of-play in Council;
- a representative of the European Data Protection Supervisor (EDPS) to gain a better understanding of any data protection issues when exchanging personal data between Europol and private parties;
- a representative of Europol (EU IRU) to gain a better understanding of the system of referrals and responding to referrals.

The table below presents the stakeholders with whom a semi-structured interview was held.

Table 7: Stakeholders for the semi-structured interviews

Stakeholders	Interviewees contacted	Interviews completed
EU-level stakeholders	▪ Representative of the Finnish Presidency ▪ Representative of the Croatian Presidency ▪ Representative of EDPS ▪ Representative of Europol (EU IRU)	▪ Representative of the Finnish Presidency ▪ Representative of EDPS ▪ Representative of Europol (EU IRU)
National-level stakeholders	LEAs: ▪ Slovene Criminal Police Directorate ▪ Spanish National Police ▪ Spanish Gaurdia Civil ▪ Romanian General Inspectorate ▪ Bulgarian General Directorate, Drugs Sector ▪ Bulgarian General Directorate, Property Crime ▪ Canadian Royal Police ▪ Hungarian National Bureau of Investigation ▪ Swedish Customs Service ▪ Serbian MOI ENUs: ▪ Cyprus ENU ▪ Czech Republic International Police Cooperation Unit ▪ Hungary Europol Liaison Bureau ▪ Slovakia ENU ▪ Croatia ENU ▪ Belgian Federal Judicial Police ▪ United Kingdom ENU ▪ Estonia HENU	LEAs: ▪ Slovene Criminal Police Directorate ▪ Spanish National Police ▪ Romanian General Inspectorate ▪ Bulgarian General Directorate, Drugs Sector ▪ Bulgarian General Directorate, Property Crime ▪ Canadian Royal Police ▪ Hungarian National Bureau of Investigation ▪ Swedish Customs Service ENUs: ▪ Cyprus ENU ▪ Czech Republic International Police Cooperation Unit ▪ Hungary Europol Liaison Bureau ▪ Slovakia ENU
Private party stakeholders	▪ Three NGOs	▪ Three NGOs

[12] Council of the European Union, Council Conclusions on Europol's cooperation with Private Parties – Council Conclusions 2 December 2019, 14745/19, available from: https://data.consilium.europa.eu/doc/document/ST-14745-2019-INIT/en/pdf

Stakeholders	Interviewees contacted	Interviews completed
	▪ Two private parties from the financial sector ▪ One payment service provider ▪ Three private parties falling under the category of 'internet service providers; online content providers; audio-visual media content providers'	▪ Two private parties from the financial sector ▪ One payment service provider
Total No. of interviewees contacted: 31		
Total No. of completed interviews: 21		

3.3.3 Workshop

The Research Team organised an online workshop aiming to:

- Validate the results of the analysis;
- Develop conclusions and recommendations.

To ensure an adequate turnover and participation, the Research Team invited all of the LEAs and ENUs which were interviewed (See Table 7 above) to participate in the workshop. Due to the low response rate from the ENUs in confirming their attendance for the workshop and to ensure an adequate representation of this group of stakeholders, after consulting with DG HOME, the Research Team contacted Europol to provide a list of 'must-have' ENUs with ample experience in direct and indirect exchanges of personal data between Europol and private parties. The contacts of three ENUs were shared with the Research Team. All three ENUs were then contacted.

Several private parties were also invited for the workshop. The Research Team contacted all of the private parties that contributed to the survey and/or the interview. In addition, a few other private parties which were considered by DG HOME as 'must-have' private parties were also approached to attend the workshop.

The table below sets out the LEAs, ENUs and private parties which were contacted and those which attended the workshop.

Table 8: Stakeholders' participation in the workshop

Stakeholders	Contacted stakeholders	Workshop attendees
LEAs	▪ Slovene Criminal Police Directorate ▪ Spanish National Police ▪ Romanian General Inspectorate ▪ Bulgarian General Directorate, Drugs Sector ▪ Bulgarian General Directorate, Property Crime ▪ Canadian Royal Police ▪ Hungarian National Bureau of Investigation ▪ Swedish Customs Service	▪ Canadian Royal Police ▪ Hungarian National Bureau of Investigation ▪ Swedish Customs Service
ENUs	▪ Cyprus ENU ▪ Czech Republic International Police Cooperation Unit ▪ Hungary Europol Liaison Bureau	▪ Cyprus ENU ▪ Spanish ENU ▪ French ENU ▪ Swedish ENU

Stakeholders	Contacted stakeholders	Workshop attendees
	▪ Slovakia ENU ▪ Spanish ENU ▪ French ENU ▪ Swedish ENU	
Private party stakeholders	▪ Three NGOs ▪ Seven private parties from the financial sector ▪ Two payment service providers ▪ Two private parties falling under the category of 'internet service providers; online content providers; audio-visual media content providers' ▪ One 'other' private party	▪ Two NGOs ▪ Six private parties from the financial sector ▪ Two payment service providers ▪ Two private parties falling under the category of 'internet service providers; online content providers; audio-visual media content providers'
Total No. of stakeholders contacted: 30		
Total No. of stakeholder attendees: 19		

The workshop was also attended by policy officers from DG HOME and Europol, the Research Team and the Senior Expert.

The Research Team hosted the workshop online via GoToMeeting[13] as several attendees were stationed across Europe and beyond, including in the United States of America and Canada, and due to the COVID 19 situation it would not have been possible to organise an in-person meeting.

The workshop was held under Chatham House Rules to ensure confidentiality.

[13] GoToMeetings is a tool for online meetings, desktop sharing and video-conferencing.

4 ANALYSIS OF FINDINGS

4.1 DIRECT EXCHANGES OF PERSONAL DATA

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

4.1.1.1 The concept of sharing personal data between Europol and private parties in the context of referrals

As also described under *Section 2: Background to the direct and indirect exchanges of personal data*, under the current regulatory framework, **Europol is generally prohibited from transferring personal data directly to private parties**. There are three exceptions to this rule, as set out in Article 26(5) of the Europol Regulation, allowing Europol to transfer personal data directly to private parties:

- if the transfer is undoubtedly in the interest of the data subject;
- if the transfer is absolutely necessary in the interest of preventing the imminent perpetration of the crime; or
- if the transfer concerns **publicly available data** and is strictly necessary for **preventing** and **combatting internet-facilitated crimes** (**referral**).

This study and thus the description below focus on the analysis of the system of referrals.

Under the Europol Regulation**, private parties** are, as a general rule, also **prohibited from transferring personal data directly to Europol**. There are **two exceptions** to this rule:

- as a **response to a referral**, Europol may receive personal data directly from private parties, which the latter declares as being legally allowed to transmit (Article 26(3) of Europol Regulation);
- the current practice of proactive sharing, as analysed under *Section 4.2.2* of this study.

The box below provides an illustrative example of the practice of referrals.

Box 1: Example of the sharing personal data between Europol and private parties in the context of referrals

The EU IRU of Europol, which has been operational since July 2015, carries out open source and internet monitoring activities. The EU IRU may flag, in the context of these activities, suspicious internet content related to terrorism and violent extremism. Any identified suspicious internet content is then referred to the relevant online service providers (OSPs)[14].

4.1.1.2 Overview of the current practice

The box below provides a snapshot of the main characteristics of the current practice.

Box 2: Main characteristics of the system of referrals and responding to referrals

Quantitative findings:

- The practice of referrals is well-documented at EU level and the EU IRU sends a large volume of referrals to OSPs;

[14] Europol, 'EU Internet Referral Unit – Year one report – Highlights', available at: https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights.

- In the majority of the cases, following receipt of a referral, the OSPs remove the online terrorist content;
- While there is statistical data on the removal of illegal content following a referral, no statistical data are collected on the number of cases when OSPs respond to referrals by sending additional personal data to Europol.

Qualitative findings:

- The EU IRU manually tracks branded online terrorist content and flags only 'clear-cut' cases to the OSPs. The OSPs review these referrals against their own terms of references;
- In many cases the EU IRU receives an automatically generated response from the OSPs, confirming safe receipt of the referral. The EU IRU isolates from these responses those that contain substantive feedback and follows up on these.

Quantitative findings

The practice 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**. Since the establishment of the EU IRU in July 2015, the EU IRU has detected 116,847 pieces of content, 111,355 of which were assessed to constitute terrorist propaganda and were referred to the respective OSPs. The detected content was found on 361 online platforms[15].

An interview, carried out with Europol's representative, confirmed that the EU IRU sends around 20,000 referrals to OSPs in a year[16].

The Europol representative noted that since its set-up, the EU IRU has engaged over 200 OSPs, out of which the EU IRU is in contact with around 80[17]. The survey targeted 13 OSPs with questions linked to the system of referrals and responses to referrals. Only two OSPs addressed the survey question on the frequency of cases when OSPs receive referrals from the EU IRU, which given the overall number of OSPs the EU IRU is in regular contact with, does not seem to be representative. One of the OSPs noted that it has not received any referrals from the EU IRU, whereas the other reported receiving referrals 'less than 50 times a year'.

EU-level sources also provide **quantitative information on the removal of terrorist content** upon receipt of a referral, suggesting that **in the majority of the cases following receipt of a referral, the OSPs remove the online content**. According to one source '*[o]n average, the content flagged for referrals has been removed in 86% of the cases (figures of December 2017)*[18]'. According to a different source in 67% of the cases the referrals were successful. Whilst the source does not define what the term 'successful' means, this category is understood as referrals leading to the removal of online content by the OSPs[19].

The Europol representative explained that the EU IRU has an automated system in place to check the status of the URLs that were targeted by the referrals. Data retrieved from this system suggest that in around 85-90% of the cases the OSPs take the online content down. Most OSPs are cooperative, especially the ones attracting a large number of users, which have a removal rate of above 97%[20].

[15] Europol, European Union Terrorism Situation and Trend Report, 2020, pg 92, available at: https://www.europol.europa.eu/sites/default/files/documents/european_union_terrorism_situation_and_trend_report_te-sat_2020_0.pdf.
[16] Information obtained from a representative of Europol via phone interview (held on 17 July 2020).
[17] Information obtained from a representative of Europol via phone interview (held on 17 July 2020).
[18] Europol 'EU Internet Referral Unit – EU IRU', available at : https://www.europol.europa.eu/about-europol/eu-internet-referal-unit-eu-iru.
[19] Europol, 'Europol Programming Document 2019-2021'.
[20] Information obtained from a representative of Europol via phone interview (held on 17 July 2020).

The private party respondents to the survey provided a very different picture, reporting on the 'rare (in less than 10% of cases)' take down of online content. This view, however, was expressed by one respondent only, which does not seem representative enough.

The study aimed to understand how the number of removals as a result of a referral compares to the number of take-downs carried out proactively (i.e. voluntary take-down, not dependent on the prior receipt of a referral). Whilst no quantifiable evidence could be gathered, it seems that **the approach to, and thus the rate of, proactive take-down depends on a variety of factors**, including the business model and social responsibility rules followed by the OSPs concerned. As a general rule, larger platforms would have a vested interest in proactively removing terrorist content[21]. It is noted that according to the one private party which responded to the survey, proactive take-down of online content 'never' happens.

The research suggests that **no statistical data are collected on the number of instances when private parties respond to referrals**. From Europol's side, this is certainly the case, as confirmed by the Europol representative[22]. The one private party respondent provided a number in its response to the survey, claiming that its organisation responds to referrals 'less than 50 times' a year. This seems to be an estimate, given that the stakeholder, when being asked about precise statistics, could not provide exact figures.

Qualitative findings

The EU IRU does not use an automated tool to monitor terrorist online content. Instead, the EU IRU staff **manually tracks branded terrorist content**. As a result of this manual processing, the EU IRU only flags **'clear-cut' cases to the OSPs**, which can then **review the content against their own terms of reference**. Under the current regulatory framework, the OSPs are not under a legal obligation to take online terrorist content down. Nevertheless, as the numbers above show, the receipt of referrals in most cases results in the removal of the online terrorist content[23].

According to the representative of Europol, the making of reliable and substantiated referrals with clear-cut terrorist content online which are shared with the concerned OSPs has also played a crucial role in **building trust with the OSPs** and improving their capacity to address terrorist abuse online. As a result, OSPs are becoming increasingly keen on cooperating with Europol. This enhanced cooperation manifests in, for example, regular Referral Action Days, which are also attended by the OSPs. Moreover, OSPs which could not be easily engaged in the past, now want to cooperate with Europol and take proactive measures against potential abuses before terrorist networks start using their platforms[24].

Under the current system, the OSPs **might transfer personal data to Europol, as a response to a referral.** Europol clarified that often, when sending a referral, the EU IRU receives an automatically generated response from the OSPs, confirming receipt. The EU IRU tries to isolate from these **automatically generated responses** those that provide **substantial feedback** for the EU IRU. The EU IRU only follows-up on these more substantial responses[25].

4.1.1.3 Possible challenges for and changes to the current practice

The box below provides a snapshot of how the stakeholders perceive the current practice and in particular, whether they see a need for change. It also outlines the key suggestions the stakeholders made for possible changes to the current practice.

[21] Information obtained from a representative of Europol via phone interview (held on 17 July 2020).
[22] Information obtained from a representative of Europol via phone interview (held on 17 July 2020).
[23] Information obtained from a representative of Europol via phone interview (held on 17 July 2020).
[24] Information obtained from a representative of Europol via phone interview (held on 17 July 2020).
[25] Information obtained from a representative of Europol via phone interview (held on 17 July 2020).

Box 3: Snapshot of views regarding the possible changes to the current practice

Possible challenges for the current practice:

- Some stakeholders reported on the 'partial suitability' of the system of referrals, for responding to referrals;
- The main shortcoming of the system is that it fails to address emerging operational needs, stemming from the increasing willingness of OSPs to share non-publicly available personal data with Europol outside the context of referrals;
- The current regulatory framework allowing for the system of 'proactive sharing' does not address these operational needs as:
    - OSPs point of view: this would entail significant analysis at their end, in particular the identification of the relevant jurisdiction of the respective national LEAs in order to allow for a targeted submission of the personal data to these national authorities. However, due to capacity issues, many OSPs are not in a position to carry out such thorough processing and would prefer sending bulk data to Europol.
    - Europol's point of view: under the current Europol Regulation, Europol can = only do limited processing of the personal data received from private parties, restricted to the identification of the national ENUs. Europol might face difficulties identifying the national ENUs concerned, purely on the basis of data received from the private parties, which can ultimately result in a loss of data. Moreover, if Europol identifies and transfers the personal data to the ENUs concerned with a request for resubmission, the latter are not always in a position to resubmit the data.

Possible changes to the current practice:

- There is a need to amend the Europol Regulation thereby allowing private parties and Europol to exchange personal data directly outside the context of referrals and under a system where Europol can carry out more extensive data processing operations, leading to the substantive analysis of the datasets received. It is also necessary to boost the human and technical capacity of Europol.

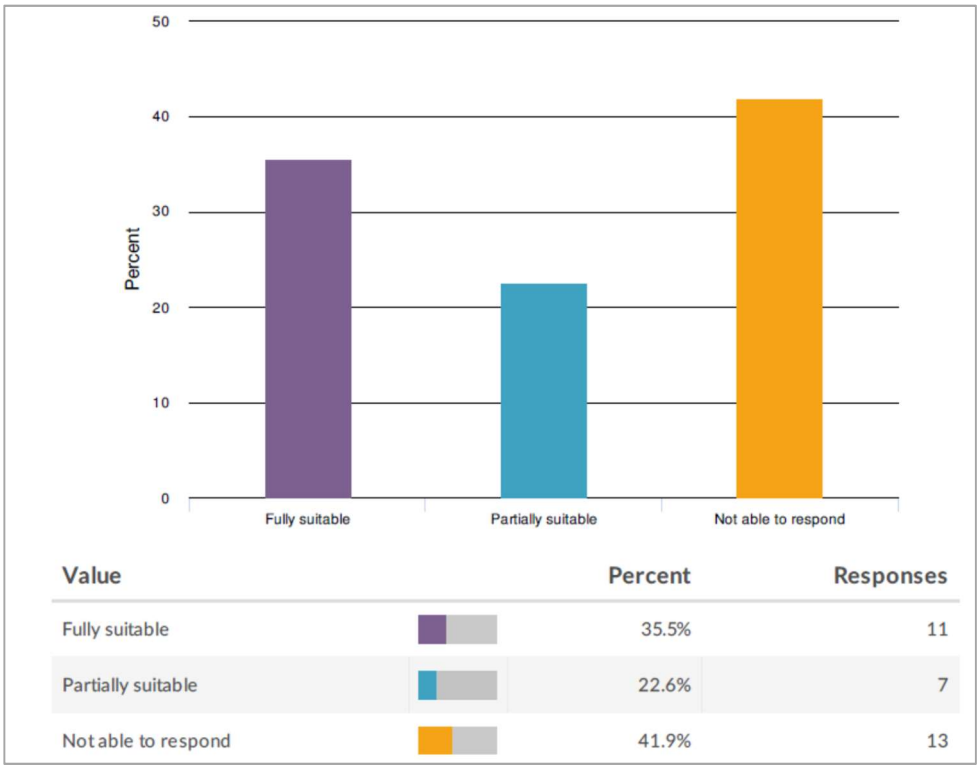
Possible challenges for the current practice

Based on the survey and the downloadable questionnaire, it was not possible to draw clear conclusions as to the suitability of the current system of referrals and responses to referrals. This is due to the fact that private parties, constituting the only stakeholder group with direct experience with the system (other than Europol), provided very limited input on the matter. The one private party who contributed to this part of the survey was not able to evaluate the system of referrals, and noted that the system of responding to referrals was 'fully suitable'.

Whilst the responses of the ENUs and the LEAs to the downloadable questionnaire, have to be read with the caveat that none of these organisations play a direct role in the system of referrals and responses to referrals, the responses provided by these organisations have hinted towards the existence of some shortcomings.

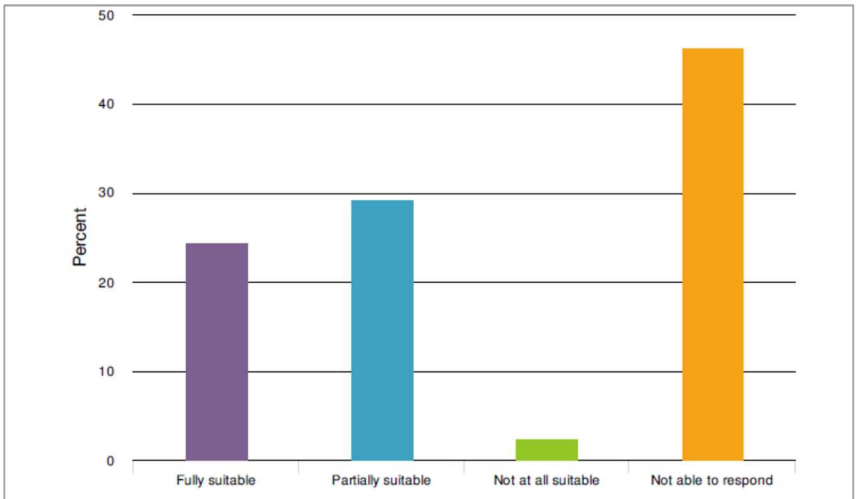
In the case of both stakeholder types, the majority of the respondents picked the answer option 'not able to respond' – echoing their lack of experience with the system. In the case of the ENUs, the majority of stakeholders who were able to respond reported on the 'partial suitability' of the system – both in connection with the system of referrals and responses to referrals. In the case of the LEAs, the answers were slightly reversed, with the majority of the respondents reporting on the full suitability of the system. These numbers, however, were somewhat counterbalanced by the relatively high number of respondents reporting on the partial suitability of the system of referrals. The views of the LEAs and ENUs in connection with the system of referrals are presented in the visuals below.

Figure 6: Suitability of the system of referrals – LEAs' views



Value	Percent	Responses
Fully suitable	35.5%	11
Partially suitable	22.6%	7
Not able to respond	41.9%	13

Figure 7: Suitability of the system – ENUs' views



Value	Percent	Responses
Fully suitable	24.4%	10
Partially suitable	29.3%	12
Not at all suitable	2.4%	1
Not able to respond	46.3%	19

The national IRUs were also asked to evaluate the system, given that they regularly interact with the EU IRU. For example, seven Member States' national IRUs have access to the tools used by the EU IRU

while sending referrals to the OSPs. Moreover, the EU IRU and the national IRUs may interact in the context of joint operations and while engaging OSPs, for example in the context of Referral Action Days. As an example, in October 2018, the EU IRU organised the 11th joint Referral Action Day together with the national IRUs of six Member States (Belgium, France, Germany, Italy, the Netherlands and the United Kingdom[26]). The EU IRU and the national IRUs identified several hundreds of suspected terrorist propaganda, which was then shared with the OSP concerned (Telegram), which attended part of the Referral Action Day[27].

The national IRUs, also **expressed some criticism towards the current practice**. Out of the seven stakeholders who did not pick the answer option 'not able to respond' (three responses, 30%), six (60%) evaluated the system as being only 'partially suitable' whilst one (10%) referred to the full suitability of the system. The national IRUs provided similar responses, while being asked about the suitability of the current system of responding to referrals to address serious cross-border crimes and terrorism: five (55.6%) stakeholders noted that they were 'not able to respond', four (44.4%) found the system 'partially suitable' and one (11.1%) referred to the full suitability of the system.

An interview with the EU IRU sought to clarify the underlying reasons behind the opinions pointing towards the partial suitability of the system. The interviewee explained that during the past five years the EU IRU has established a **trust-based, solid relationship with the OSPs**. Building on this experience, the **OSPs would be increasingly willing to share personal data with the EU IRU, proactively, thus outside the context of the referral system**. Whilst Europol would see an added value in receiving more personal data from the private parties, the current Europol Regulation sets clear limits for the data processing activities of Europol in connection with proactively shared data.

As explained in details under *Section 4.2.2 - Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing)* – under the current system, upon receipt of proactively shared personal data by the private parties, Europol may only process the personal data with the sole purpose of identifying the national ENU to whom Europol should transfer the data further. The national ENU may then decide to send the personal data back to Europol. As presented under *Section 4.2.2 - Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing)* - resubmissions do not always happen. Thus, even if the OSPs would attempt to send personal data to Europol proactively, there is no guarantee that the information would ultimately reach Europol[28].

It also creates a difficulty as **it might not be obvious for Europol who the national ENU is based on the data shared by the private parties**. This is due to the fact that in the context of proactive sharing, Europol can only process the data received from the private parties. There is no possibility for Europol to re-contact the private party and request more information or explanation[29].

The aforementioned issues are particularly problematic when seen together with the **capacity constraints faced by some OSPs,** which might not have the human resources and time to provide Europol with information specific to a given Member State. This would entail an analysis from their end. OSPs would rather send bulk data to a hub, which can do the necessary processing itself[30].

Possible changes to the current system

According to the representative of Europol, to tackle the challenges mentioned above, there is a need to reconsider the rules applicable for the proactive sharing of personal data, as set out in the Europol

[26] In October 2018, the United Kingdom was an EU Member State.
[27] Europol, 'Referral Action Day with six EU Member States and Telegram', available at: https://www.europol.europa.eu/newsroom/news/referral-action-day-six-eu-member-states-and-telegram.
[28] Information obtained from a representative of Europol via phone interview (held on 17 July 2020).
[29] Information obtained from a representative of Europol via phone interview (held on 17 July 2020).
[30] Information obtained from a representative of Europol via phone interview (held on 17 July 2020).

Regulation. These amendments should loosen the rules that currently limit Europol's data processing activities in connection with the personal data that are proactively shared with Europol by the private parties, and possibly allow for Europol to exchange personal data directly with private parties. To match the new roles foreseen by these more robust data processing activities, there is a need to consolidate Europol's capacity, both in terms of human resources and technical capacity[31].

4.2 INDIRECT EXCHANGES OF PERSONAL DATA

4.2.1 Europol receiving personal data from private parties via an intermediary

4.2.1.1 The concept of Europol receiving personal data from private parties via an intermediary

As also described under *Section 2: Background to the direct and indirect exchanges of personal data,* Article 26(1) of the Europol Regulation sets out the most traditional way for Europol to receive personal data from private parties. As per the said provision, Europol may process personal data obtained from private parties on the condition that they are received via an intermediary (usually the national competent authorities). It is important to note that the relevant competent authority, acting as an intermediary, is more than just a 'hub' under this scheme, because the intermediary takes the decision on whether to transfer the data to Europol or not. Indeed, in many, if not most cases, the national competent authorities decide not to share the data with Europol (see below). If the said authority transfers the personal data to Europol, it becomes a data owner, implying that the authority takes full responsibility for the personal data sets.

The box below provides an illustrative example of the practice.

Box 4: Example of Europol receiving personal data from private parties via an intermediary

In a concrete case, which began in the United States of America, a private party, the National Centre for Missing and Exploited Children (NCMEC) received a report of a suspected child abuse case via its CyberTipline. Upon examination of the report and completing it with some additional information of relevance for law enforcement purposes, NCMEC sent the information to the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Liaison Office at Europol in the Hague. The HSI Liaison Officer coordinated with Europol's European Cybercrime Centre (EC3). EC3 immediately cross-checked the information and produced an intelligence package, which was then sent to the Romanian authorities, where the suspect was based. The case led to the arrest of the Romanian suspect[32].

4.2.1.2 Overview of the current practice

The box below provides a snapshot of the main characteristics of the current practice.

Box 5: Main characteristics of the practice of Europol receiving personal data from private parties via an intermediary

Quantitative findings:

- As a general rule, no statistical data are collected by the stakeholders concerned on the practice. Compared to the other forms of exchanges, this 'traditional' way of transfer seems to be the one most used and Europol receives most of the personal data obtained from private parties via intermediaries;

[31] Information obtained from a representative of Europol via phone interview (held on 17 July 2020).
[32] Europol, 'International police action leads to rescue of 22-month old Romanian sex abuse victim', 25 February 2015, available at: https://www.europol.europa.eu/newsroom/news/international-police-action-leads-to-rescue-of-22-month-old-romanian-sex-abuse-victim.

- Estimated data suggest that Europol receives only a fraction ('minority') of the personal data that private parties transfer to the LEAs, even though this data relates or could relate to serious crime affecting two or more Member States, terrorism or other forms of crime which affect the common interest of the Union.

Qualitative findings in connection with personal data being transferred by the private parties to the national LEAs:

- As a general rule, private parties do not transfer personal data voluntarily to LEAs. The transfer of personal data from the private parties to the LEAs typically happens in the context of investigations, when responding to requests received from the national LEAs, or else stems from compliance with regulatory obligations requiring the private parties to transfer personal data to the national LEAs;
- Private parties tend to cooperate with the national LEAs of the country in which they are established, rather than with national LEAs of other countries;
- Multiple factors play a role for private parties' tendency to cooperate with the national LEAs of the country in which they are established, and not so much with LEAs of other countries, such as compliance with regulatory obligations and previous experience with LEAs in the form of public private partnerships stand out;
- The speed of the transfers of personal data from the private parties to the LEAs depends on what is meant under transfer: the preparation of datasets might take longer, but the actual/technical transfer of datasets happens very quickly;
- Private parties do not share personal data with the LEAs with the intention of sharing these further with Europol.

Qualitative findings in connection with personal data being transferred by the national LEAs to the national ENUs:

- When LEAs transfer the personal data obtained from the private parties further to the national ENUs, the speed of the transfer depends on the case, in particular the urgency of the case or the time needed to prepare the file to be transferred to the national ENU;
- In many cases, LEAs refrain from sharing personal data with the national ENUs, because of their lack of competence to act on the case (e.g. no legal basis to initiate an investigation; no ongoing investigation or no crime is identified), even though these data could relate to serious and organised crime or terrorism affecting another country;
- Once the personal data are transferred to the ENUs, the LEAs do not have clear visibility over the steps taken by the ENUs.

Qualitative findings in connection with personal data being transferred by the ENUs to Europol:

- Not all ENUs pass the personal data obtained from private parties (through the LEAs) on to Europol;
- When ENUs do not transfer the data further, this is mainly due to legal reasons (e.g. no legal reason to initiate an investigation; minor infringement; no suspect; etc.).

Quantitative findings

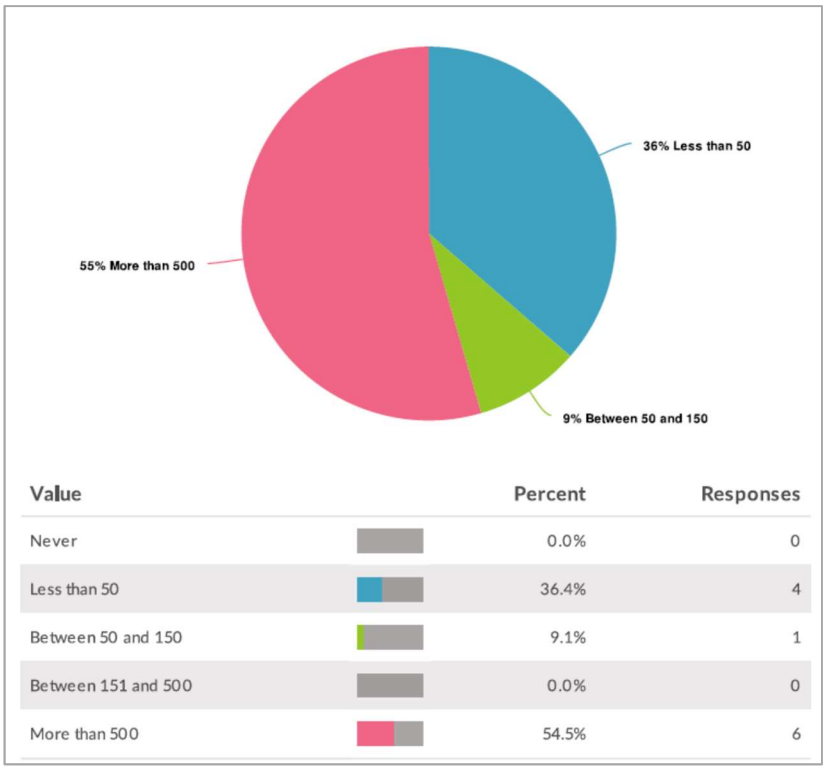
Whilst it was **not possible to obtain precise statistical data** on the number of instances when private parties share personal data with national competent authorities, when LEAs transfer the personal data obtained from private parties to the ENUs or when the ENUs transfer the personal data received from the LEAs further to Europol, the study clearly indicates that these **transfers take place on a regular basis**. Also, if compared to other forms of transfers, this channel seems to be the **most frequently used**.

The survey targeting private parties revealed some quantitative information on the matter. Twelve responses were provided to the question on the frequency of cases when **private parties see the need** to transfer personal data to national LEAs:

- Half of the responses (six responses, 50%) suggest that private parties **see the need for the transfer to national LEAs in 'more than 500 cases' a year**.
- Four responses (33.3%) come from private parties which see such a need 'less than 50 times' a year, whereas one response (8.3%) reported on the need being seen 'between 151-500 times' a year and 'zero times' a year was reported by one response also (8.3%).

When asked about the **number of actual transfers**, the responses to this same survey provided a very similar picture thereby showing that in a majority of the cases actual transfers take place 'more than 500 times' a year. The visual below provides an overview of the responses received from the private parties.

Figure 8: Number of personal data transfers from private parties to LEAs



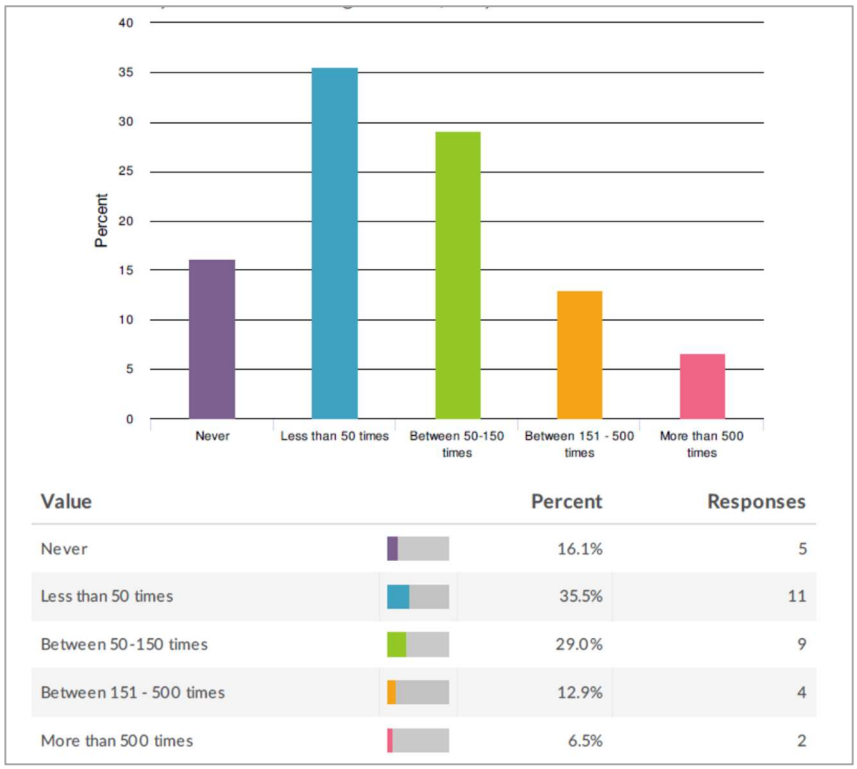
Value	Percent	Responses
Never	0.0%	0
Less than 50	36.4%	4
Between 50 and 150	9.1%	1
Between 151 and 500	0.0%	0
More than 500	54.5%	6

As only two private parties could provide statistical data on the matter via the survey, it seems that **statistical data, as a general rule, are not collected in practice**.

The interviews carried out with six private parties confirmed that statistical data collection is rare. Only one respondent could report on very precise numbers of transfers, which was recorded by the system used for sharing personal data with Europol through the intermediary.
All interviewees, however, provided an **estimate of the number of transfers**. These estimates show a **heterogeneous picture**. The private parties that typically transfer the highest number of personal data to the LEAs act because they are subject to a legal obligation to do so. The others, who are not subject to such obligations, tend to transfer personal data to the LEAs less frequently. It is noted that the difference in numbers between the two groups is considerable. As an example, the only private party which had precise statistical data on the number of transfers reported 193,742 transfers in 2018. Another private party representing the second group of stakeholders, who are not under the legal obligation of transferring personal data, reported less than 50 transfers a year.

The **national LEAs**, which often constitute the first intermediary in the transfers of personal data between private parties and Europol, were asked to provide information on the **number of cases when they transfer personal data received from the private parties to the ENUs**. The highest number of responses suggests that on a yearly basis, the LEAs make such transfers 'less than 50 times' (11 responses, 35.5%). This and the rest of the responses are presented in the visual below.

Figure 9: Number of personal data transfers (as obtained from private parties) from the LEAs to the ENUs



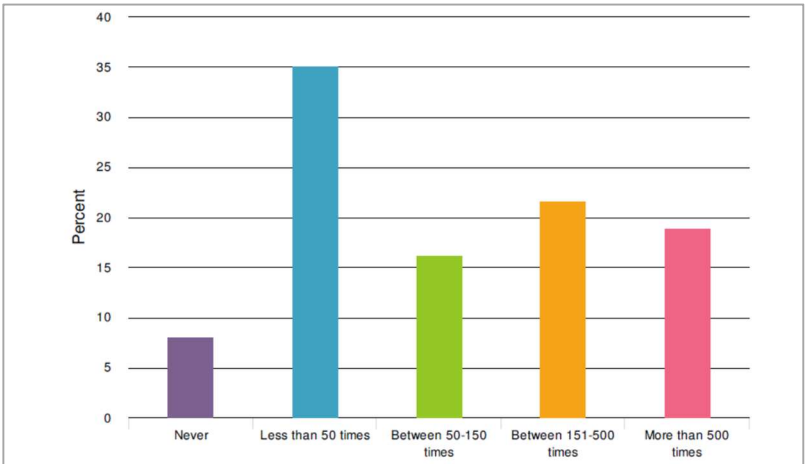
Value	Percent	Responses
Never	16.1%	5
Less than 50 times	35.5%	11
Between 50-150 times	29.0%	9
Between 151 - 500 times	12.9%	4
More than 500 times	6.5%	2

These numbers, if compared to the number of transfers of personal data made by private parties, suggest that **only a fraction ('minority') of all datasets sent by the private parties are forwarded further by the LEAs**. Possible reasons for this, and the possible consequences of these missed transfers, are provided below.

The interviews carried out with the LEAs confirmed that they do not collect **statistical data on the matter**. Two interviewees noted though that their respective organisation collects data on the number of times they send information to the ENUs. These statistics, however, do not disaggregate the numbers based on the type of data covered by these transfers. In other words, these statistics do not single out cases in which the transfer contained personal data.

The **ENUs**, which always constitute the last intermediary (making the **actual transfer of personal data to Europol**), reported **numbers similar to the LEAs** when asked about the number of transfers of personal data received from LEAs to Europol. These are presented in the visual below.

Figure 10: Number of personal data transfers (as obtained from private parties) from the ENUs to Europol



Value	Percent	Responses
Never	8.1%	3
Less than 50 times	35.1%	13
Between 50-150 times	16.2%	6
Between 151-500 times	21.6%	8
More than 500 times	18.9%	7

The interviews with the ENUs **echoed the findings of the interviews carried out with the LEAs**, reiterating that statistical data collection on the number of transfers that contain personal data does not happen. Out of the four interviewees, two noted that the ENUs do collect some statistical data e.g. on the number of transfers towards Europol, or the number of requests for information received; these, however, do not single out transfers that contained personal data.

Qualitative findings

Personal data being transferred by the private parties to the national LEAs

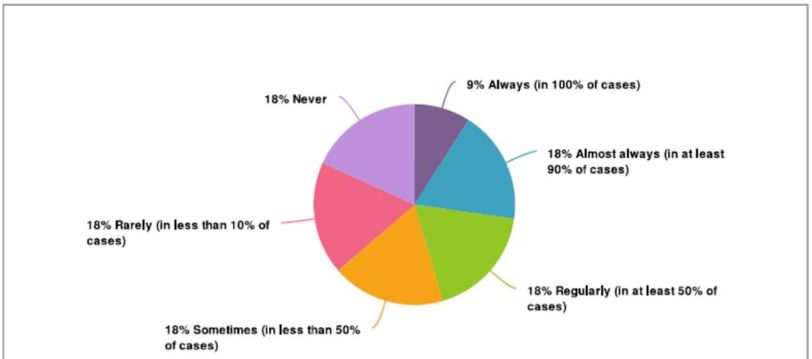
The survey, the interviews and the workshop revealed that private parties, as a general rule, **do not transfer personal data voluntarily to the intermediaries**. The transfers mainly happen as:

- Private parties receive a **request** from the national LEAs, typically in the context of investigations to transfer personal data to them. In these cases, private parties are typically under a legal obligation of responding to the LEA's requests;
- Private parties might be under a **reporting obligation** towards the LEAs, as imposed by the applicable regulatory frameworks.

The survey did not provide a clear-cut picture on the matter, but the interviews and the workshop clarified this point with the stakeholders, as set out below.

The 11 responses provided by the private parties to a related question in the survey suggested that **voluntary sharing is not a general rule**. As a matter of fact, only one response (9.1%) indicated that voluntary sharing happens 'always (in 100% cases)'. The remaining responses are provided in the visual below.

Figure 11: Voluntary transfer of personal data to national LEAs



Value	Percent	Responses
Always (in 100% of cases)	9.1%	1
Almost always (in at least 90% of cases)	18.2%	2
Regularly (in at least 50% of cases)	18.2%	2
Sometimes (in less than 50% of cases)	18.2%	2
Rarely (in less than 10% of cases)	18.2%	2
Never	18.2%	2

The six interviewed private parties confirmed that voluntary sharing does not happen on a regular basis. It is noted that the majority of these interviewees (four) are under the legal obligation of **sending reports and/or notifications** to the national LEAs, provided that the threshold set (e.g. suspicion of a crime) in the applicable legislation is met. All four organisations also had experience with the transfers of personal data to national LEAs as a **response to requests**. The interviewees explained that these requests are typically sent to them in the context of investigations. Depending on the type of personal data sought, these requests might be accompanied by judicial authorisations or similar. The interviewees explained that upon receipt of the authorities' requests they respond, as this is a legal obligation for them. The two other organisations which are not under the regulatory obligation to share personal data with the national LEAs through notifications or reports, clarified that they typically share personal data with national LEAs upon receipt of a request.

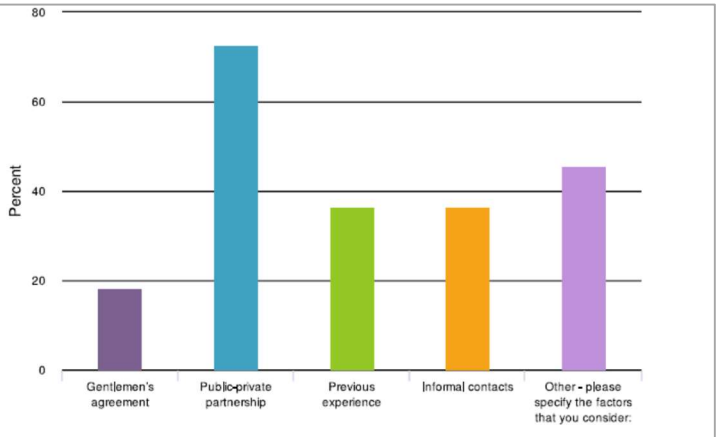
During the workshop, **reasons preventing the private parties from sharing personal data with the LEAs** were clarified. Two private party representatives noted that the current regulatory framework might prevent the private parties from sharing multi-jurisdictional datasets with all the LEAs concerned. It is understood that this is due to the fact that applicable legislation specifies which LEAs the private parties should be turning to. Once the data are shared, it is up to the LEAs to transfer the data further to other LEAs concerned. This might result in data losses, in particular in cases, where the LEAs decide not to transfer the data on to the other LEAs concerned.

The survey suggests that as a general rule, **private parties transfer personal data to the LEAs of the country where they operate – thus to the national LEAs**. Out of the 11 responses, seven (64%) indicate cooperation with national LEAs, whereas in four cases (36.4%) the responses suggest cooperation with organisations other than the national LEAs. The latter seems to be the case when the private parties are being contacted with requests by foreign LEAs (i.e. LEAs other than national LEAs). In addition, one private party in its response referred to cooperation with foreign LEAs, while describing its cooperation with European LEAs. This is due to the fact that the given private party is not Europe-based.

The finding that private parties typically cooperate with the LEAs of the country where they operate was also confirmed by the LEAs via the downloadable questionnaire. The large majority of the 32 responses provided to a related question (28 responses, 87.5%) indicates that cooperation happens this way.

The private parties' responses to a multiple-choice question in the survey indicates that **multiple factors and mainly the existence of public-private partnerships** (eight responses (72.7%))**, play a role in picking the national LEA** they cooperate with. The second most numerous hits (five responses, 45.5%) indicate that 'other reasons' might also play a role (in particular, the existence of statutory rules, indicating that private parties might be directed to certain authorities by law (four responses). The private parties' views are also presented in the visual below.

Figure 12: Basis of cooperation between private parties and the LEAs



Value	Percent	Responses
Gentlemen's agreement	18.2%	2
Public-private partnership	72.7%	8
Previous experience	36.4%	4
Informal contacts	36.4%	4
Being referred to by another organisation	0.0%	0
Other - please specify the factors that you consider:	45.5%	5

One interviewee confirmed that regulatory factors play a role in the selection of the national LEAs, as applicable legislation might specifically provide for the LEA to be contacted in the context of the exchanges of personal data.

During the workshop, compliance with regulatory obligation(s) was also referred to as a factor playing a role in the selection of the LEAs.

The survey also sought to understand the speed of transfer of personal data from **the private parties to the LEAs**. Nine private parties responded to the relevant question of the survey. The 11 responses indicate that many transfers typically happen 'within a day' (four responses, 44%) and even 'within an hour' (two responses, 22.2%). However, several other transfers happen only 'within a week' (two responses, 22.2%) or 'within a month' (one response, 11.1%) after tracing the potential criminal activity.

The interviewees further clarified, while commenting on the speed of the transfer, that there is a difference between the time needed for preparing the datasets and the actual (digital) transfer of the personal data. The actual transfer of personal data happens very quickly, as such processes are often

digitalised, and the private parties often use some systems provided by the LEAs. However, the time spent preparing the datasets impacts the speed with which the data is transferred. The interviewees provided some examples of factors impacting the time needed for preparing the datasets. Two interviewees explained that they might have to respect some deadlines set by applicable legislation, or the requests for information while preparing the files. When preparing datasets for notification/reporting purposes, the complexity of the case, including identifying the data which is relevant for the specific jurisdiction, might be the main factor determining the speed. One interviewee also mentioned that in cases when they transfer data to LEAs which are based in countries other than where the private party operates, and in particular when these are based in remote locations like the Far East or the Middle East, the transfers might take longer. This is the case as they have to ensure that data protection rules are complied with, that the data are encrypted and that the transfers can happen through secure channels.

The ENUs and the LEAs did not provide further insights into this particular aspect of the current practice.

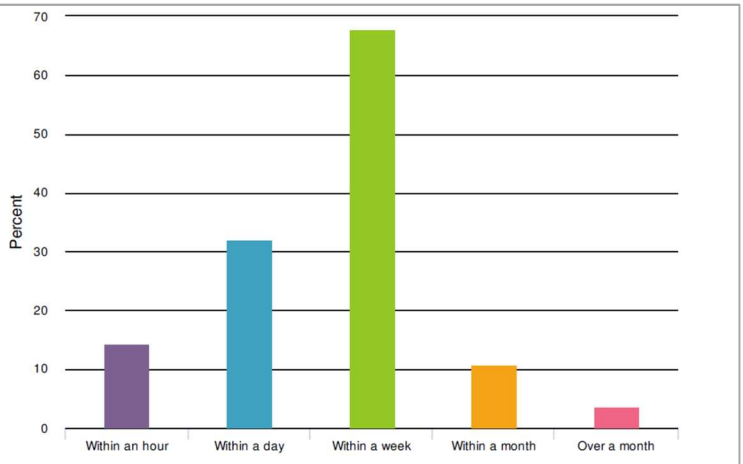
As a final point, the interviews with the private parties revealed that the **private parties do not share personal data with the LEAs with the intention of sharing these with Europol**. This was confirmed by the LEAs as well, who were systematically asked during the interviews whether while being contacted by the private parties, they are specifically requested to transfer the personal data onward to Europol.

Personal data being transferred by the national LEAs to the national ENUs

As mentioned above, the LEAs do not always transfer the personal data received from the private parties to the national ENUs. But when they do, **the speed of the transfer seems to differ on a case-by-case basis**.

This derives from the responses received to a question of the downloadable questionnaire, asking stakeholders to indicate the speed of the transfer of personal data to the ENUs. The stakeholders provided multiple answers to the question, suggesting that there is no clear-cut rule on the matter. Whilst it might be true that the answer **depends on the case itself**, one answer option received a particularly high number of hits, which might suggest that as general rule, the transfer of the personal data takes place **'within a week'** (nineteen responses, 67.9%). The visual below also outlines the other answer options picked by the respondents.

Figure 13: Speed of personal data transfer (obtained from private parties) from the LEAs to the ENUs



Value	Percent	Responses
Within an hour	14.3%	4
Within a day	32.1%	9
Within a week	67.9%	19
Within a month	10.7%	3
Over a month	3.6%	1

The finding that the **speed of transfer depends on the case** was also confirmed by all seven LEAs targeted by the interviews. Two interviewees explained that when the LEA obtains personal data from the private parties in the context of responding to requests received from other Member States, the LEA would respect the deadlines provided in the request. When the request is urgent, they would transfer personal data within a day, or in extreme cases even within an hour. Outside the context of responding to requests, the LEAs might abide with the deadlines set by their hierarchy. The other interviewees also confirmed that the speed of transfer might depend on the urgency of the case, or the time needed for the preparation of the file. Regarding the latter point, one stakeholder explained that the added value of the LEA in the system is to pass on processed data to the ENUs. This entails the provision of some analysis around the raw personal datasets transferred to the LEAs by the private parties.

The downloadable questionnaire and the interviews also tried to understand the **potential reasons behind the non-transfer of personal data from the LEAs to the ENUs**. Based on the responses received it seems that **various reasons** might lie behind this finding. This derives from the fact that the stakeholders picked multiple answer options while responding to the question. The main reason for non-transferring seems to relate to the **LEA actually not being competent to act in connection with the case**. This can be due to multiple reasons:

- 'no legal basis to initiate investigations in the Member State' (15 responses, 55.6%),
- 'no on-going investigation in the Member State' (13 responses, 48.1%),
- 'no crime identified' (10 responses, 37%),
- 'no victims' (two responses, 7.4%),
- 'no suspect' (two responses, 7.4%),
- personal data hinting to 'minor infringements' (two responses, 7.4%).

LEAs might decide not to transfer the personal data further also when the case concerned by the personal data has 'no apparent trans-border aspect' (eight response, 29.6%). The stakeholders also reported on issues linked to a 'lack of internal resources' (six responses, 22.2%), the existence of 'regulatory

burdens' (e.g. data protection rules preventing transfer) (five responses, 18.5%) and the existence of 'administrative burdens' (one, 3.7%). Seven stakeholders (25.9%) also said that 'other' factors might also play a role in the non-transfer of personal data namely, the personal data does not fall within Europol's mandate, or there is no ongoing investigation. One stakeholder even indicated that all of the above reasons are valid reasons for the non-transfer of personal data to the ENU and ultimately the real reason behind the non-transfer depends on a case-by-case basis.

The interviews confirmed that **various reasons** might lie behind the non-transfer of personal data obtained from private parties to the ENUs. Many interviewees further articulated one aspect, namely that the information at hand must clearly suggest that the personal data relates to a criminal activity which would **fall under Europol's mandate**. Thus, the transfer should be relevant to 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 […]' [33]. This was also confirmed during the workshop where the participants (two LEAs) stated that the LEAs transfer the personal data received from the private parties further to Europol, **when they identify a suspicious criminal activity that falls under Europol's mandate**. These transfers, as a general rule, take place in the context of investigations. One stakeholder noted that intelligence, collected outside the context of investigations, might also be shared with Europol. Intelligence sharing, however, is rare as LEAs are typically not designed to process large volumes of intelligence, or else specialised intelligence services (other than the regular LEAs) are competent to gather intelligence. Another stakeholder noted that his Member State does not transfer intelligence to Europol. As a result of the above, it seems that in some Member States, a prerequisite for further data sharing is the launch of an investigation or to have an ongoing investigation. In the absence of legal grounds to launch or run an investigation, data sharing with Europol does not seem to take place. This supports the responses received through the downloadable questionnaire and the findings of the interviews.

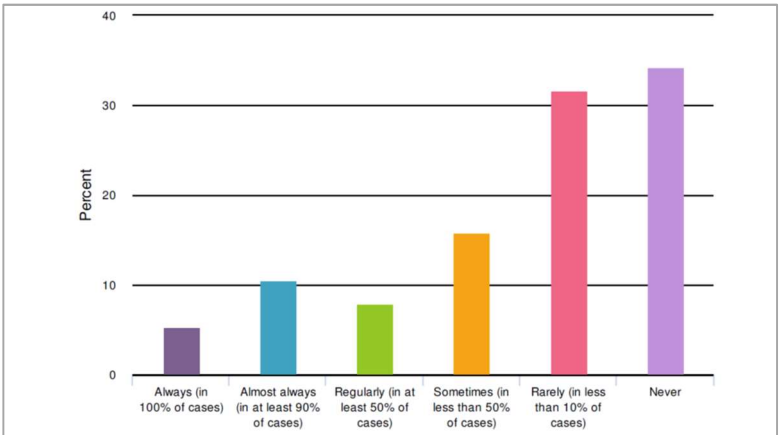
As a final element, the interviews clarified that once the LEAs transfer the data to the ENUs, they are not typically asked by the ENUs to clarify aspects of the file transferred. Moreover, as a general rule, LEAs are not informed of the fact that the ENUs transferred the personal data to Europol. This means that **once the personal data are transferred to the ENU, the LEAs do not have clear visibility over the steps taken by the ENUs**. One stakeholder noted that due to the fact that they have a liaison officer at the ENU, they can closely follow the steps taken by the ENU in relation to the transfers of personal data. Three interviewees also noted that sometimes they know, through indirect ways, that the personal data were transferred by the ENU to Europol. This happens when they receive additional follow-up requests from other Member States through the Europol channel, with respect to the case in the context of which the original transfer of personal data from the LEA to the ENU took place. One stakeholder noted that they take it for granted that the personal data transferred to the ENU are transferred onward to Europol. This finding was confirmed via the interviews carried out with ENUs as well, with one minor alteration, as one of the ENUs clarified that they always inform the LEAs of the cases when they do not transfer the data further to Europol.

Personal data being transferred by the ENUs to Europol

The downloadable questionnaire and the interviews aimed to explore whether or not the ENUs transfer the personal data on to Europol, once received from the LEAs. The downloadable questionnaire therefore, asked the ENUs to specify the frequency of cases when they decide not to transfer the personal data forward to Europol. Whilst a very limited number of stakeholders provided multiple answers to the question, it still seems to be clear that **the majority of the ENUs transfer the personal data to Europol; however, there are still a few ENUs which decide not to transfer personal to Europol**. This derives from the numbers presented in the visual below.

[33] Article 3(1) of the Europol Regulation.

Figure 14: Frequency of cases when personal data are not transferred further to Europol



Value	Percent	Responses
Always (in 100% of cases)	5.3%	2
Almost always (in at least 90% of cases)	10.5%	4
Regularly (in at least 50% of cases)	7.9%	3
Sometimes (in less than 50% of cases)	15.8%	6
Rarely (in less than 10% of cases)	31.6%	12
Never	34.2%	13

The downloadable questionnaire also gathered information on the **grounds for not transferring the personal data further**. As the respondents picked multiple answer options, it seems **that various grounds might justify the ENUs' decision of not transferring the personal data further**. As in the case of the LEAs, who were asked a very similar question in connection with their decision-making process, it seems that often **legal reasons lie behind the ENU's decisions**. These could be:

- 'no legal basis to initiate an investigation in the Member State' (14 responses, 43.8%),
- 'minor infringements' (eight, 25%),
- 'no suspects' (eight responses, 25%),
- 'no-on-going investigation in the Member State' (seven responses, 21.9%),
- 'no crime identified' (seven responses, 21.9%),
- 'no victims' (two responses, 6.3%).

Some hits also concerned the answer options 'no apparent trans-border aspect' (seven responses, 21.9%) and 'workload / lack of internal resources' (four responses, 12.5%). It is noted that 17 responses (53.1%) indicate the existence of some other reasons behind the decision. No information on what the category 'other' means could be retrieved from the downloadable questionnaire.

The interviews targeting four ENUs further explored the practices of the ENUs regarding the onward transfers of personal data received from the LEAs. One interviewee noted that the ENUs always transfer the personal data further to Europol. Two other interviewees altered this picture by stating that prior to submission they run a check through the file. This usually entails a quick check of whether or not the **transfer falls under Europol's mandate**.

4.2.1.3 Possible challenges for and changes to the current practice

The box below provides a snapshot of how the stakeholders perceive the current practice and in particular, whether they see a need for change. It also outlines the key suggestions the stakeholders made as to the possible change of the current practice.

Box 6: Snapshot of views regarding the possible changes to the current practice

Possible challenges for the current practice:

- Many stakeholders from all stakeholder groups (private parties, LEAs, and ENUs) consider the current system as not fully suitable to match their needs;
- According to the private parties consulted, the main shortcomings of the system are: the transfers of personal data being slow; requests received not being sufficiently clear; the follow-up by the LEAs not being sufficient; due to regulatory requirements, with which the LEAs have to comply, access to personal data held by private parties becoming increasingly difficult; private parties not being able to transfer multi-jurisdictional datasets to all LEAs concerned;
- According to the LEAs, the main shortcomings of the system are: the transfers of personal data by the private parties to the LEAs being slow; the LEAs having capacity issues while processing large amounts of data received from the private parties; some internal processes not being digitalised, resulting in the manual hand-over of files within the LEA's hierarchy;
- According to the ENUs, the main shortcomings of the system are: the transfers of personal data being slow; collaboration with some private parties being challenging; legal framework not providing enough grounds for private parties to share personal data with Europol.

Possible changes to the current practice:

- Regarding the possible changes to the current practice the private parties made the following suggestions:
  - Sharing personal data directly with Europol or else granting Europol direct access to personal data;
  - Adapting the data protection rules applicable to the exchanges of personal data within the same private party, with other private parties operating in the same sector and with a wider range of LEAs;
  - Europol, or a similar central authority, playing the role of a clearing house and obtaining personal data from the private parties centrally for the onward transfer of these datasets to the respective LEAs;
  - Providing a platform for the LEAs to exchange information;
  - Through PPPs providing a platform for a discussion on the more targeted use of the current system;
  - Review the current system to better utilise data analytical abilities, understand the capabilities of the infrastructure supporting the current practice and explore the impact the different crimes have on the current practice.

- Regarding the possible changes to the current practice, the LEAs made the following suggestions:
  - Awareness raising on the use of the practice to boost its use;
  - Designation of a single point of contact within the private parties responsible for the exchanges of personal data with LEAs;
  - Establishment of secure channels for the exchanges of personal data between the private parties and the LEAs;
  - Revision of applicable rules to allow private parties to share personal data with a wider group of LEAs;

- Revision of applicable legislation at the national level to push private parties to transfer personal data to the LEAs faster;
- Further digitalisation of internal processes surrounding the transfers of personal data;
- LEAs being allowed to exchange personal data among themselves.

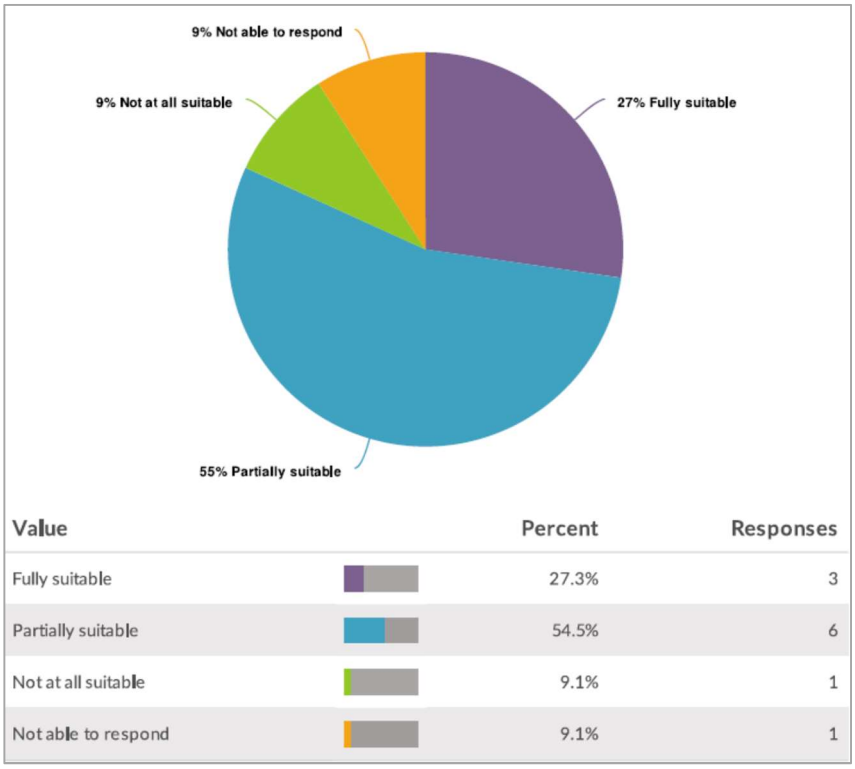
- Regarding the possible changes to the current practice, the ENUs made the following suggestions:
  - Grant the LEAs wider access to personal data collected by private parties;
  - Allow private parties to share personal data directly with Europol.

Possible challenges for the current practice

All stakeholder groups targeted by the downloadable questionnaires, the survey and the interviews were asked to evaluate the current system. Moreover, the workshop served as an opportunity to obtain some additional views from the stakeholders.

The responses received from the 11 **private parties** responding to the corresponding question of the survey suggest that **the current practice is not fully suitable to match their needs**. This derives from the responses presented in the visual below.

Figure 15: Suitability of the current practice – private parties' point of view



Value	Percent	Responses
Fully suitable	27.3%	3
Partially suitable	54.5%	6
Not at all suitable	9.1%	1
Not able to respond	9.1%	1

The LEAs' responses to the downloadable questionnaire indicate that many LEAs consider the system not fully suitable to match their needs. More or less the same number of responses relates to the suitability (14 responses, 41.2%) and the partial suitability (15 responses, 44.1%) of the system. One stakeholder (2.9%) evaluated the system as 'not at all suitable' and another (2.9%) was not able to respond.

The ENUs' responses to the downloadable questionnaire revealed that the majority rated the system as **only 'partially suitable'** (21 responses (48.8%). This is followed by seventeen responses (39.5%) which rated the system as 'fully suitable'. It is noted that six ENUs (14%) were 'not able to respond'.

Some of the ENUs (12 respondents) provided an explanation of why they evaluated the system in one way or another. The stakeholders referred to three main reasons:

- The system being too **slow**, which ultimately results in insufficient responses to criminal activities. One ENU stakeholder reiterated this issue during the workshop;
- **Collaboration** with some private parties being **difficult** – this depends on a case-by-case basis;
- Currently applicable legal framework **not** providing **enough grounds** for the private parties to **share personal data with Europol**.

The interviews and the workshop sought to better understand the underlying reasons behind the responses above.

All **private party** interviewees (six), even those who chose the answer option 'fully suitable' while responding to the survey, expressed some **concerns regarding the current practice**, for various reasons:

- The current system being **slow** was a concern reported by three interviewees. The interviewees mentioned that this is particularly problematic given that criminals act fast. The current lack of speed of the system results in missed opportunities for fighting criminals;
- The current system being **non-transparent** was reported by one stakeholder. The stakeholder noted that while responding to requests, they often lack information on the context of the request and have no visibility over the specific use of the personal data provided to the LEAs. More clarity would result in better results, as the private party could better tailor the transfer to the needs of the LEAs;
- One stakeholder explained that the system as such is suitable; however, the follow-up based on the information provided is not. Due to the **lack of follow-up** (e.g. financial investigations), criminals escape;
- Another stakeholder noted that due to the currently applicable data protection framework, **LEAs cannot always obtain personal data** from the private parties. This results in missed opportunities for fighting organised criminals.

During the workshop, two private parties noted that the **sharing of personal data with LEAs must be in line with the applicable legal framework**, including the GDPR. The GDPR to a certain extent has restricted the sharing of personal data, as for example private parties operating within the same sector are not allowed to exchange personal data among themselves, which might result in missed opportunities as the exchange of personal data between the private parties could result in the identification of suspicious criminal activities.

It was further noted that while private parties collect a lot of personal data, the **current legal framework does not allow the private parties to share multi-jurisdictional datasets with all the LEAs from the various jurisdictions**. Rather, the private parties only share the personal data with the respective LEAs with which the private parties have an obligation to share personal data. As a result, not all LEAs concerned might receive all relevant datasets.

Out of the seven **LEAs**, four reported on some shortcomings of the system for the following reasons:

- Two stakeholders noted that sometimes it **takes some time** for the private parties to respond to a request received from the LEAs, which ultimately results in a lengthy process;

- One stakeholder noted that shortcomings result from the **manual processing** of files by the LEA. Under the current system, they have to prepare all packages to be sent to Europol through the ENUs in **paper format** to be signed by their hierarchy. Once the file is signed, the file is digitalised and is sent forward to the ENUs;
- One stakeholder recalled that the **LEAs sometimes receive large files** from the private parties, which would subsequently have to be processed by the LEAs. This raises **capacity and capability issues** with the consequence that LEAs are not always able to analyse the entire datasets and therefore miss out on sharing relevant personal data with LEAs of other Member States or with Europol.

It is noted that the views of the four ENUs, which were subsequently interviewed, did not echo the critical views voiced by the majority of ENUs in the survey (nor the critical views of the private parties). The four interviewed ENUs considered the current practice fully suitable, even though one stakeholder noted that their national system has a shortcoming. This shortcoming stems from the fact that in the country concerned there are **no digitalised channels for the transfers of personal data** by the private parties to the LEAs. Instead, they have to transfer the personal data via normal postal services, which makes the system slow. Moreover, during the workshop, an ENU confirmed that there are delays ("bottlenecks") in the transfer of personal data being that the personal data is transferred from the private parties to the LEAs and the ENUs before it reaches Europol.

The results from the survey and some of the aforementioned views referring to missed opportunities indicate that there is an **operational need for changing the system**.

The box below illustrates some real-life examples, suggesting that there is an operational need to change the current practice.

Box 7: Examples illustrating operational needs for changing the current practice of Europol receiving personal data from private parties via an intermediary

One private party dealing with illicit online content explained that under the current regulatory framework they are legally prohibited from sharing personal data directly with Europol. As a matter of fact, they are under the legal obligation to channel personal data through the national authority, which would then be responsible for transferring the personal data to Europol for processing. The private party carries out activities which entail the transfer of large amounts of personal data to the national authority. Due to the amount of information shared with the intermediary, as well as the time it takes to prepare the information received from the private party for onward transmission to Europol, the onward transfer is slow, which hinders the main purpose of transferring information. To expedite the process and shorten the delays for information transfer, the private party indicated that it would be beneficial if there could be direct exchange of personal data between private parties and Europol.

Another stakeholder noted that private parties that investigate and collect evidence on criminal and terrorist activities in conflict areas, including war zones, typically have some working arrangements with national LEAs or international organisations for the sharing of personal data. Europol has concluded working arrangements with national LEAs, which agreed to receive personal data and information from private parties in order to transfer it to Europol. However, the conclusion of these working arrangements is perceived as complicated and cumbersome and they often rely on personal relationships between Europol staff and the persons responsible within the national LEAs. Moreover, under this system the onward transfer of personal data still depends on the discretionary powers of an intermediary. As a result, personal data containing information on criminal and terrorist activities might reach Europol late or not at all, although such datasets might be particularly useful to identify, investigate and prosecute terrorists or criminals.

Possible changes to the current practice

The stakeholders were also asked to provide some suggestions as to **how the current practice could be changed.**

From among the six **private parties** who were interviewed, five had suggestions regarding possible changes to the current practice. **Most of these opinions suggested a change to the applicable legislative framework**:

- One interviewee noted that there might be a need to transfer personal datasets **directly to a single, centralised authority** such as Europol. This authority could receive the information and send requests towards the private parties. As a result of this centralisation, law enforcement could move faster. The interviewees mentioned that the establishment of this would necessitate changes to the applicable EU regulatory framework;
- Another interviewee also suggested the possibility of transferring personal data without going through the national authority in order to speed up the process of transferring personal data. In the case of this interviewee, the national authority has direct access to this private party's database. Such access could be given to Europol. However, this might necessitate some change to the applicable EU regulatory framework;
- One interviewee recalled that one of the main obstacles for LEAs to access personal data is data protection. This shortcoming of the current system could be overcome by a **more flexible interpretation of data protection rules** by the national data protection authorities, thereby allowing wider access to personal data for law enforcement purposes. Alternatively, access rights should be **revised in the GDPR**. The same interviewee noted that **Europol, or a similar centralised organisation,** could potentially take the role of a **clearing house** and could obtain data directly from the private parties for their onward transfer to the LEAs;
- Another interviewee noted that the shortcomings of the current system would have to be tackled at multiple levels:
    - **Private parties** carrying out similar activities should be allowed to **exchange personal data among themselves**. Under the currently applicable regulatory and data protection frameworks, private parties are often prevented from sharing personal data freely even within their own organisation. This is an issue especially for large private parties, with activities in multiple countries;
    - Under the current rules, private parties who are subject to some regulatory obligations to notify or report suspicious criminal activities are often obliged to cooperate with a national authority specified in applicable legislation. The private party felt that sometimes there is a need to **cooperate with LEAs beyond those prescribed by laws**, which might entail cooperation with **LEAs of other countries**. Legislation should facilitate this;
    - It was also noted that under the current framework, **LEAs do not cooperate with each other enough**. Europol's role in this regard could be reinforced;
    - Part of the solution could be the **establishment of more PPPs**, involving peer organisations and/or governmental stakeholders from the EU countries. These could create a platform for sharing information based on trust and under strict confidentiality rules. LEAs could potentially bring their typologies or interests to the PPPs, whereas private parties could bring their data – be it bulk data or individualised data. By talking to each other, the LEAs and the private parties could come up with some systems allowing for a more efficient use of personal data and thus for more efficient ways of fighting criminals.
- Another stakeholder recalled that the current system pre-dates today's level of full-scale digitalisation and is not suitable for fighting crime and terrorism in the digital area. The **current system** needs to be **reviewed** and in order to do so, the nature and the impact of the different crimes need to be better understood. Moreover, there is a need to identify the shortcomings of

the current analytical and infrastructural capacities. To move these changes forward there has to be a champion at EU-level, which could potentially be Europol. The interviewee also noted that the currently applicable legal framework might have some shortcomings, which are abused by criminals. These shortcomings would be different per private party as often, the activities of the private parties are regulated by separate legislation.

During the workshop, one private party intervened in favour of a simplification of the legal framework for private parties to share personal data with Europol, including the simplification of the GDPR and the Anti-Money Laundering Directive.

During the workshop, the participants also commented on the possibility of granting the LEAs direct access to their datasets, as a possible solution to the issue caused by the private parties not being able to share data with some LEAs when their datasets concern multiple jurisdictions. However, the private parties did not consider this a suitable solution at this stage, given the limitations of the currently applicable data protection legal framework. During the workshop, one ENU suggested the possibility that the private parties share personal data directly with Europol when the personal data is within Europol's mandate in order to avoid the personal data being transferred through the intermediaries (i.e. the LEAs and the ENUs) before it reaches Europol. Europol could analyse the personal data received and when found to be significant, share it with the respective Member States.

LEAs provided suggestions regarding the potential change of this part of the current system both through the downloadable questionnaire and the interviews.

Out of the 13 responses provided to a relevant question in the downloadable questionnaire three reiterated the **need for awareness raising campaigns on the current practice**, thereby improving its use. One respondent suggested the **designation of a single contact point** within the private parties responsible for the exchanges of personal data between them and the LEAs. Another stakeholder provided a similar suggestion referring to an enhanced role data protection officers could play while exchanging personal data with LEAs. The same stakeholder noted exchanges could be facilitated by the **establishment of secure channels**. Moreover, the same stakeholder reiterated the importance of awareness raising, which could ultimately result in private parties sharing personal data voluntarily with LEAs. A different stakeholder suggested the revision of the regulatory framework, which currently obliges certain private parties to share personal data with specific institutions (e.g. financial institutions reporting to Financial Intelligence Units) in a way that **would extend this communication obligation to other LEAs**. The remaining stakeholders either noted that they had no suggestions or else provided a response, which without the necessary context, could not be interpreted.

The seven LEAs targeted by the interviews were in general satisfied with this part of the current system. However, two of the LEAs put forward concrete recommendations. One noted that under the current system the transfer of personal data is slow. To overcome this, **LEAs,** upon receipt of personal data of relevance in a cross-border context, should be able to **communicate with each other directl**y, thus without going through the ENU as an intermediary and Europol. The same interviewee referred to the **digitalisation of the system for the exchanges of personal data**. Another interviewee noted that legislation at national level could be adjusted thereby **obliging private parties to transfer the personal data faster**.

During the workshop, three participants (LEAs and ENUs) highlighted the important difference between information and intelligence sharing. The participants stated that LEAs are structured to process information on a case-by-case basis linked to an investigation and not to deal with massive amounts of intelligence. As LEAs are not necessarily structured to process intelligence, any change to the current transfer of personal data from private parties to Europol via the LEAs would need to establish whether personal data is shared by private parties either to serve investigative purposes or else to serve intelligence purposes.

As mentioned above, the ENUs were in general satisfied with this part of the current system. Consequently, most stakeholders did not have any suggestions for the possible change to the system. One stakeholder suggested that LEAs could be given **more access to the personal data collected by private parties**. Another stakeholder suggested that in order to avoid the slow transfer of personal data from private parties to Europol through the LEAs, **private parties could share personal data directly with Europol** when it falls within the mandate of the Agency. Europol could analyse and share the personal data with the respective Member States when the information is found to be significant.

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

4.2.2.1 The concept of proactive sharing

As also described under *Section 2: Background to the direct and indirect exchanges of personal data,* Article 26(1) of the Europol Regulation establishes the general rule that Europol shall only process personal data received from private parties on condition that it is received via a national unit, a contact point in a third country or in an international organisation with which Europol has an established cooperation through a cooperation agreement, or via an authority of a third country or an international organisation which is the subject of an adequacy decision by the European Commission or with which the EU has concluded an international agreement.

Article 26(2) of the Europol Regulation provides a procedure for cases, where **private parties nonetheless share personal data directly with Europol (outside of the context of referrals** as envisaged under Article 26(5)(c) of the Europol Regulation). When Europol receives personal data directly from private parties, **Europol may process** the personal data received **solely for the purpose of identifying the responsible ENU**, the contact point or authority concerned (for the purpose of this section, hereinafter: ENU). Once the ENU is identified, Europol shall immediately transfer the personal data to the respective entity. Europol shall delete the personal data received from the private parties within four months, unless the ENU resubmits the personal data through the established channel of communication.

The box below provides some illustrative examples of the practice.

Box 8: Examples of proactive sharing[34]

A payment service provider identified some illegal transactions, resulting in the withdrawal of cash approximately EUR 10 million from ATM machines located in 10 Member States. The payment service provider reached out to Europol in the context of proactive sharing and provided Europol with information about the locations of the ATM machines, the cards used for withdrawals, transaction IDs and time-stamps. Europol in the given case processed the data solely for the purpose of identifying the competent ENUs as foreseen in Article 26(2) of the Europol Regulation. In this case, Europol could identify the ENUs concerned without requesting further information from the payment service provider, because the bulk data sent by the private party contained reference to the location of the ATM machines. Europol, in line with the requirements of the Europol Regulation, immediately forwarded the personal data to the competent ENUs. However, Europol could not provide the whole intelligence picture to the ENUs concerned. In addition, Article 26(2) of the Europol Regulation prevented Europol from analysing the data further, e.g. to identify the movements of criminals withdrawing cash at ATMs across the EU, because the Agency is only allowed to process such information to identify the ENUs concerned. Furthermore, Europol could only inform the respective

[34] Information obtained via scoping interview with Europol representatives and via written contribution received on 21 August 2020.

ENUs of withdrawals from ATMs within their jurisdiction, and not about the withdrawals from ATMs outside their jurisdiction, so that data transmitted did not enable the ENUs to identify such movements themselves[35].

An Online Service Provider (OSP) identified repeated attempts by users to set up accounts with the purpose of disseminating content (video, audio, pdf, images) produced by the so-called "Islamic State" (IS) terrorist organisation. The content was branded (i.e. it displayed the logos and visuals of the terrorist organisation) and therefore could be easily detected and assessed as terrorist activity by the OSP. Because the content was inciting the online audiences to join the terrorist organisation (IS) and conduct terrorist attacks on western soil, the OSP turned to Europol with information about the user accounts (i.e. email addresses, IP addresses etc.). Although Europol processed the information, the nature of the data did not allow for a direct link to be drawn with a specific EU Member State and therefore the information could not be shared with any specific competent ENU. Europol would have to ask any ENU who would be willing to play the role of the intermediary (in this generic threat against the western countries) in order to receive and re-submit the data to Europol for further analysis in Europol's databases.

4.2.2.2 Overview of the current practice

The box below provides a snapshot of the main characteristics of the practice.

Box 9: Main characteristics of the practice of proactive sharing

Quantitative findings:

- Whilst no statistical data are collected on the practice; it seems that the practice is rarely used.

Qualitative findings in connection with private parties sharing personal data proactively with Europol:

- The private parties that participated in the study, did not have any experience with sharing personal data directly with Europol, which can be explained by the current legal framework. They could therefore not provide any input on this form of exchange of personal data with the Agency.

Qualitative findings in connection with the role of ENUs in the resubmission of personal data:

- The speed of resubmission to Europol depends on the case, including the amount of personal data that needs to be assessed before it is transferred to Europol; the time taken to consult with the LEAs;
- As a general rule, the ENUs consult the LEAs in the context of resubmissions, meaning that the ENUs do not tend to decide alone over the resubmission of personal data;
- There could be multiple reasons for ENUs not to resubmit the personal data to Europol (e.g. no legal basis to initiate an investigation, or no ongoing investigation), even though the personal data could possibly relate to serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.

Qualitative findings in connection with the role of LEAs in the resubmission of personal data:

- When being consulted in the context of resubmission, the LEAs typically transfer the personal data back to the ENUs;
- The speed of transfer to the ENUs depends on the urgency of the case and whether other authorities need to be consulted;

[35] Another point that could be mentioned here is that in the absence of a wider intelligence picture, the personal data relevant for the jurisdiction of an ENU may not meet national legal 'thresholds' to start an investigation.

- There could be multiple reasons for LEAs to advise their ENUs not to resubmit personal data to Europol e.g. no legal basis to initiate an investigation, or no ongoing investigation); even though these personal data could possibly relate to serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.

Quantitative findings

All consulted stakeholders confirmed that they **do not collect statistical data in connection with this form of exchange of personal data**.

Information obtained from **Europol**[36] confirms that Europol's current databases do not mark the following types of exchanges:

- Europol receiving personal data from private parties in the context of proactive sharing;
- Europol transferring personal data received directly from private parties to the identified ENUs.

While Europol did not provide precise data, Europol representatives stated that **private parties rarely share personal data directly with the Agency**.

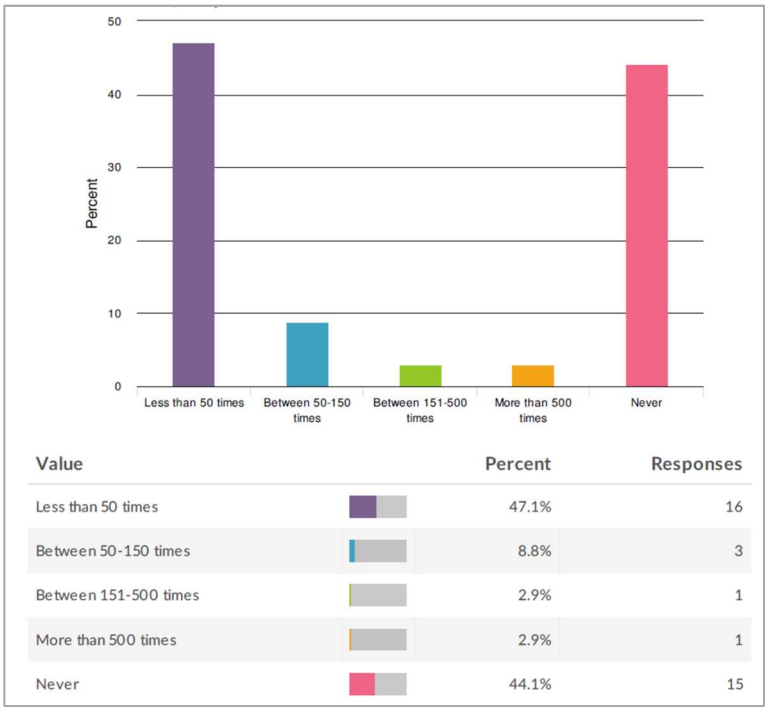
The rare use of the system has also been confirmed by the private parties, the ENUs and the LEAs, who were asked to quantify the number of exchanges, both via the survey / downloadable questionnaire and the interviews. Two private party respondents to the survey noted that such transfers 'never' take place.

During the interviews, which were held with six private parties in total, none of the interviewees referred to statistical data collection activities on the practice. As a matter of fact, all private parties targeted by the interviews clarified that they had **no practical experience** with the system of proactive sharing.

The downloadable questionnaire to the **ENUs** also sought to obtain information on the frequency of cases when **Europol sends** these organisations personal data obtained from private parties, **for resubmission**. These responses, which are presented in the visual below, suggest that these cases are rare.

[36] Information obtained from Europol on 23 April 2020, as a response to a request filed by the Research Team.

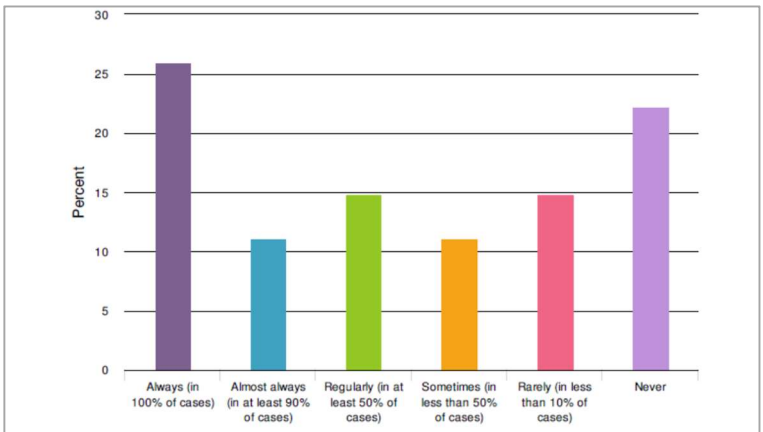
Figure 16: Frequency of Europol sending personal data to the ENUs for resubmission



Value	Percent	Responses
Less than 50 times	47.1%	16
Between 50-150 times	8.8%	3
Between 151-500 times	2.9%	1
More than 500 times	2.9%	1
Never	44.1%	15

When being asked about the **frequency of resubmissions to Europol**, 27 responses were provided by the respondents indicating that that ENUs **do not always resubmit the personal data received from Europol**. The responses of the ENUs are provided in the visual below.

Figure 17: Frequency of resubmission of personal data by ENUs to Europol



Value	Percent	Responses
Always (in 100% of cases)	25.9%	7
Almost always (in at least 90% of cases)	11.1%	3
Regularly (in at least 50% of cases)	14.8%	4
Sometimes (in less than 50% of cases)	11.1%	3
Rarely (in less than 10% of cases)	14.8%	4
Never	22.2%	6

The interviews held with four ENUs aimed to clarify the experience of this stakeholder group with the practice. Whilst these interviews targeted only a small number of interviewees (four), they revealed some important findings:

- Three of the respondents clarified that, contrary to what they had previously indicated in the downloadable questionnaire, they were **unaware of any cases when this system was used by their respective Member State**;
- The remaining one respondent, while noting limited experience with the system, indicated that the **quantitative data** provided in the downloadable questionnaire were her **own estimates**, and her Member State **does not collect statistical data on the matter**.

These responses suggest that some of the stakeholders, while responding to the downloadable questionnaire might have provided answers that do not fully reflect the reality. Nevertheless, the interviews seem to confirm that the system of **proactive sharing is rarely used at the moment**.

The **national LEAs** were also asked, via the downloadable questionnaire, to quantify the number of cases when **they are consulted on the resubmissions** of personal data to Europol by the national ENUs.

Out of the 28 responses provided to a related question in the questionnaire, 21 responses (75%) indicate that LEAs are **'never' consulted by the ENUs** in the context of the resubmission of personal data to Europol. Six responses (21.4%) indicated being consulted 'less than 50 times' a year and one response (3.6%) suggests that LEAs are consulted 'between 50-150 times' a year by the national ENUs in the context of resubmissions.

The responses received from the national LEAs were followed up via the interviews with seven interviewees. These interviews also targeted stakeholders who, via the downloadable questionnaire, reported on being consulted by the ENUs in the context of resubmissions. These interviews, revealed the following:

- Two respondents noted that LEAs **do not have good visibility over the origin of the requests passed on to them by the ENUs**, in particular, they are not informed of the fact that they are being consulted in the context of a resubmission request from Europol;
- Two respondents confirmed that their national LEAs **have already been consulted** in the context of resubmissions – both noted though that **no statistical data** on the matter are collected;
- Three respondents clarified that as opposed to previous responses given to the downloadable questionnaire, they **were not aware of any cases** when the national LEA was consulted by the ENUs in the context of resubmissions.

The responses of the seven selected stakeholders in addition to revealing some deviations from the responses provided to the downloadable questionnaire, confirm **that LEAs are not always consulted in the context of resubmissions**. Regarding this finding, one stakeholder interviewee even noted that under the national regulatory framework **ENUs have the discretionary power to resubmit the personal data to Europol** without prior consultation of the LEA. This suggests that it is also possible that this step of the resubmission process is skipped in some Member States.

Qualitative findings

Qualitative findings in connection with private parties sharing personal data proactively with Europol

The very low number of responses received from the **private parties** to the survey (two responses) on this question suggests that instead of proactively sharing personal data with Europol, private parties **tend to share personal data with national LEAs**[37].

The use of channels other than proactive sharing was confirmed by the interviewees.

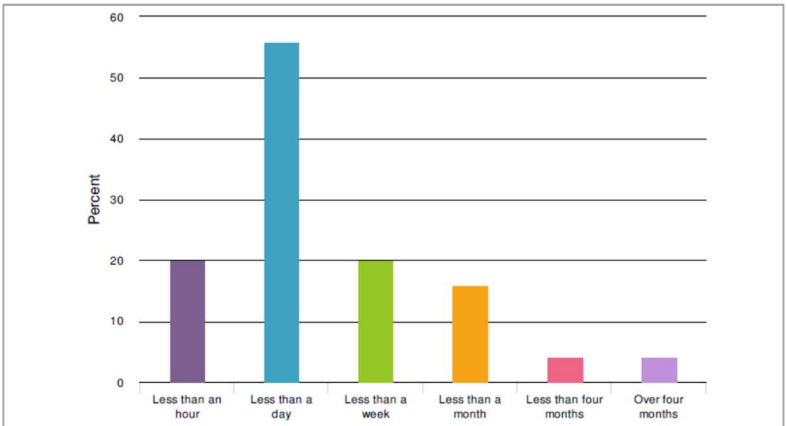
Qualitative findings in connection with the role of ENUs in the resubmission of personal data

Whilst the extent of their experience is not entirely clear (see above), **ENUs** provided some **insights** into the functioning of the system.

The downloadable questionnaire revealed some information about the **speed of resubmissions**. When being asked about the time needed for assessing whether or not the personal data received from Europol should be resubmitted, the stakeholder group provided 45 responses. Some stakeholders chose multiple answers, suggesting that the **speed depends on the case concerned**, including on the amount of personal data that needs to be assessed before it is resubmitted to Europol, and the time it takes to consult with the LEAs. The majority of the responses (14 responses, 56%) suggests that such a decision is taken within 'less than a day'. The visual below provides some further insights into the responses of the stakeholders.

[37] Moreover, LEAs tend to share personal data not proactively, but rather in reaction to a legal obligation, with the national LEA of the country in which they are established.

Figure 18: Speed of resubmission of personal data by the ENU to Europol



Value	Percent	Responses
Less than an hour	20.0%	5
Less than a day	56.0%	14
Less than a week	20.0%	5
Less than a month	16.0%	4
Less than four months	4.0%	1
Over four months	4.0%	1

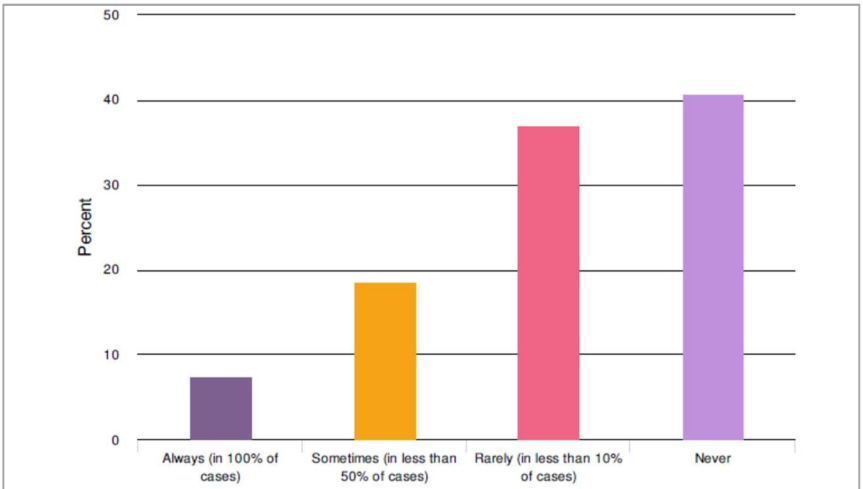
Based on the responses (35 responses) provided to the downloadable questionnaire, it seems that in a majority of Member States the **ENUs contact the national LEAs in the context of resubmissions**. In some Member States, however, such consultations do not take place. This derives from 22 (62.9%) responses referring to such consultations and 13 responses (37.1%) referring to the lack thereof.

It also seems that **these consultations do not systematically happen**. Only three responses out of the 21 (14.3% of responses) related to the answer option 'always (in 100% of cases)', thereby indicating that the consultation of LEAs in the context of resubmissions is mandatory. The largest numbers of responses related to the answer options of 'almost always (in at least 90% of cases)' (six responses, 28.6%) and 'regularly (in at least 50% of cases)' (six responses, 28.6%). Four responses (19%) suggest that such consultations 'sometimes (in less than 50% of cases') happen and two (9.5%) that they 'rarely (in less than 10% of cases)' happen.

According to the ENUs, **as a general rule, LEAs transfer the data back to them**. This is suggested by the fact that according to the ENUs, the LEAs 'never' or 'rarely' fail to resubmit personal data to the ENUs[38]. The visual below provides the aggregated responses of the stakeholders.

[38] It is noted that some stakeholders provided multiple answers to the question.

Figure 19: Frequency of cases when LEAs do not transfer the personal data back to the ENUs



Value	Percent	Responses
Always (in 100% of cases)	7.4%	2
Sometimes (in less than 50% of cases)	18.5%	5
Rarely (in less than 10% of cases)	37.0%	10
Never	40.7%	11

When asked about the **reasons for not being able to resubmit personal data** to Europol, the ENUs provided 57 responses. It should be noted that some stakeholders referred to multiple grounds for not resubmitting, thus the high number of responses. The highest number of responses (13 responses, 41.9%) relate to the answer option 'other', indicating that grounds other than the ones mentioned below tend to result in the lack of resubmission of personal data. The respondents did not specify what these other grounds are. The rest of the grounds mentioned by the respondents are:

- 'no on-going investigation in the country' (11 responses, 35.5%),
- 'no legal basis to initiate an investigation in the country' (eight responses, 25.8%),
- 'no suspect identified' (seven responses, 22.6%),
- 'no victims identified' (four responses, 12.9%),
- 'no crime identified' (four responses, 12.9%),
- 'no apparent cross-border aspect' (four responses, 12.9%),
- 'data concerns minor infringement' (three responses, 9.7%),
- 'workload / lack of resources to process data' (three responses, 9.7%).

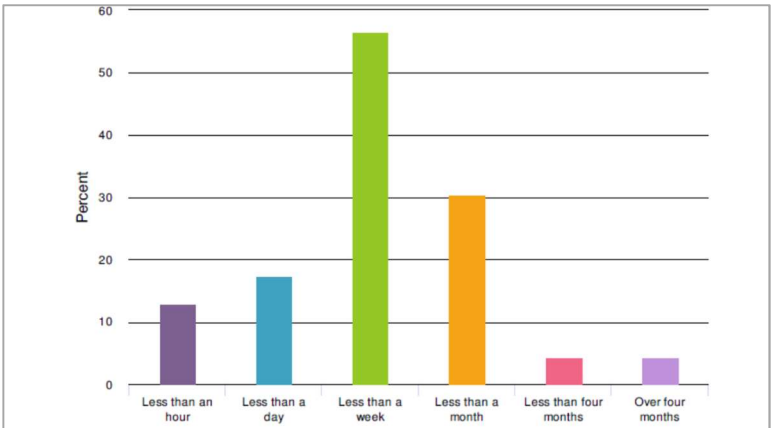
Notwithstanding the fact that several ENUs indicated in their responses to the questionnaire that they have experience with the resubmission of personal data, the interviews presented a different outcome. Only one ENU interviewee confirmed experience in connection with this practice. The interviewee clarified that in the context of resubmission of personal data, the ENU does not always reach out to and transfer the personal data to the LEAs.

Qualitative findings in connection with the role of LEAs in the resubmission of personal data

The LEAs' responses to the downloadable questionnaire reveal some details about the use of the system from their perspective.

The **speed** with which the LEAs reply to the ENUs in the context of resubmissions **seems to depend on the case**, namely on the urgency of the case and whether other authorities need to be consulted. This derives from the fact that some of the LEAs picked multiple answer options while responding to the downloadable questionnaire. As illustrated in the visual below, among the different scenarios, one referring to replies being submitted to ENUs in 'less than a week' stands out (13 responses, 56.6%).

Figure 20: Speed of response to requests received from ENUs in the context of resubmission



Value	Percent	Responses
Less than an hour	13.0%	3
Less than a day	17.4%	4
Less than a week	56.5%	13
Less than a month	30.4%	7
Less than four months	4.3%	1
Over four months	4.3%	1

LEAs were also asked to specify the **most frequently used grounds for advising the ENUs not to resubmit the personal data to Europol**. Based on the responses received it seems that LEAs use multiple grounds for providing such advice. The following two grounds seem to stand out:

- 'no on-going investigation in the country' (eight responses, 47.1%),
- 'no legal basis to initiate an investigation in the country' (seven responses, 41.2%).

These numbers are followed by:

- 'other' (five responses, 29.4%),
- 'no crime identified' (four responses, 23.5%),
- 'no apparent trans-border aspect' (four responses, 23.5%),
- 'workload/lack of resources to process to request' (one response, 5.9%).

The category 'other' revealed that some of the stakeholders had no experience with the concept of advising the ENUs in connection with the resubmissions. One respondent noted that in their experience it is rare for them to advise the ENUs not to resubmit personal data to Europol. Another stakeholder noted that the grounds are case-specific, thus the choice of the answer option 'other'. Yet another stakeholder seemed to be confused by the system, as the response noted that when private parties share personal data with Europol, their organisation would not have to transfer the personal data to Europol themselves.

As mentioned above, only two LEA representatives targeted by the interviews had experience with the practice of proactive sharing of personal data with Europol. One of the interviewees noted that **requests**

for resubmissions do not necessarily reach the national LEAs, as the ENUs may decide on the resubmission themselves. When such requests reach the national LEAs, they respond to a request received from the ENU, when there is a legal ground to do so. This is the only action that the LEAs take in the context of resubmissions, implying that they do not provide just simple advice to the ENUs. When there is a legal ground, they resubmit the personal data. The second LEA representative who had experience with the system noted that when the ENUs receive a request from Europol, be it in the context of resubmissions or otherwise, the **ENUs forward the requests to the LEAs**. The interviewee said that they very **rarely advise the ENU not to resubmit personal data to Europol**. The interviewee also confirmed that the speed of a response towards the ENU depends on the case in the context of which they were contacted. In urgent cases, they react quickly, whereas in complex cases, potentially involving multiple LEAs, their response is slower.

4.2.2.3 Possible challenges for and changes to the current practice

The box below provides a snapshot of how the stakeholders perceive the current practice of proactive sharing and in particular, whether they see a need for a change of the practice. It also outlines key suggestions the stakeholders made for possible changes to the current practice.

Box 10: Snapshot of views regarding the possible changes to the current practice

- Stemming from the rare use of the system in practice, and consequently from the lack of experience of the stakeholders, little information could be obtained about the main characteristics of the system;
- Some views could be gathered on the reasons behind the rare use of the system which seems to relate to: system being complex, its use being complicated in practice, as well as the exchange being slow;
- Ultimately the rare use of proactive sharing and the low resubmission rate might result in data losses and thus in missed opportunities;
- Operational needs and thus reasons for changing the system stem from these missed opportunities and from the fact that the 'traditional' way of Europol receiving personal data from private parties via an intermediary and the system of referrals have their shortcomings which might, among others, result in a need to enhance means for the proactive sharing of personal data with Europol;
- Possible changes would entail legislative changes, leading to the extended capacity of Europol to receive personal data directly from private parties and having the right to process it for all the purposes within its mandate;
- Any change to the current practice would have to be carefully considered, as it raises capacity issues for Europol to process data, including its ability to check that all data protection related safeguards are respected by the private parties while transferring personal data to Europol.

Possible challenges for the current practice

Potentially due to the limited experience of stakeholders with the current practice of proactive sharing, responses to the survey and the downloadable questionnaire suggest that the majority of the stakeholders have **no opinion about the suitability of the system** to respond to the current and future threats posed by serious cross-border crime, cybercrime and terrorism. Those stakeholders who did not choose the answer option 'not able to respond', provided a **mix of responses to the question asking about the suitability of the practice**.

The two private parties who responded to the survey noted that in their view, the current system is 'fully suitable'. Responses from the ENUs suggest that the system is only 'partially suitable' (11 responses, 31.4%). Eight responses (23.5%) relate to the answer option 'fully suitable'. Only one response (2.9%) captures the opinion that the system is 'not at all suitable'. The LEAs' opinions were equally

heterogeneous, though they reversed the top two categories of responses as follows: nine responses (31%) referred to the answer option 'fully suitable', and seven (24.1%) to the answer option 'partially suitable'.

The **interviews could not clarify the underlying reasons behind the responses above**, as many of the interviewees clarified during the interview that **they had very little experience, if any, with the system**. As a matter of fact, none of the private parties and ENUs could comment on the suitability of the system. Among the LEAs, one respondent noted that the system is only 'partially suitable' as the exchange of **personal data is slow** due to its set-up involving multiple actors.

Information obtained from a representative of Europol[39], suggest that the rare use of the mechanism provided under Article 26(2) of the Europol Regulation might result from the fact that the procedure in its current form is **complex and its use is complicated in practice**. Moreover, due to the complexity of the process, involving potentially multiple actors at the national level (ENUs and LEAs), even in cases when the resubmission happens, Europol might receive the personal data originating from the private parties **with a considerable delay**, which could ultimately render the data received obsolete or irrelevant. Instances **when data are not resubmitted** by the Member States to Europol might also cause some **data losses and thus result in missed opportunities**.

These potential data losses already hint towards an **operational need to change the current practice** as set out in Article 26(2) of the Europol Regulation, in order to allow Europol to exchange personal data directly with private parties.

The existence of potential operational needs for change was also highlighted by some of the private parties when interviewed about the system of Europol receiving personal data from the private parties through an intermediary and the system of referrals. Some stakeholders considered that a system under which they could share personal data with Europol directly, for the latter to process the datasets further, would be a potential solution to overcome the challenges of the current system of Europol receiving personal data from the private parties through an intermediary.

Due to the very limited use of the current system, it was not possible to identify real life examples highlighting shortcomings of the practice.

Possible changes to the current practice

The stakeholders targeted with the downloadable questionnaire / survey, the interviews and the workshop were systematically asked for suggestions as to how the current practice could be changed. The responses suggest that there seems to be a need for **enhancing Europol's capacity to directly exchange personal data with private parties**, and **to process the data** received directly from private parties. The stakeholders acknowledged that such a change can only be achieved **with a regulatory amendment** to the Europol Regulation.

Most of the responses touching upon the aforementioned aspects were provided by the ENUs. While responding to the downloadable questionnaire, 15 ENUs provided answers to the questions on how the current practice could be changed. Seven of these responses refer to the reinforcement of Europol's competences and/or the possible revision of the Europol Regulation. Two responses suggest that instead of reconsidering the system of proactive sharing, the relationship between private parties and the LEAs should be boosted, which could result in enhanced data sharing by the private parties with the LEAs. The remaining responses either provided unclear recommendations, or otherwise noted that the respondents did not have anything to add.

[39] Information obtained from Europol on 23 April 2020, as a response to a request filed by the Research Team.

A limited number of LEAs could also contribute to this question via the downloadable questionnaire. It is noted though that out of the 10 responses received only a few provided real recommendations as to how the system could be changed; the rest provided generalities (e.g. there is room for improvement) or otherwise reported on the lack of experience with the system. The few responses (four), however, echoed the observations made by the ENUs regarding the possible revision of the regulatory framework.

The private parties responding to the survey did not provide any recommendations as to how the current practice could be improved.

The interviews added very little to the views presented above. As a matter of fact, only the ENUs could contribute to this topic via the interviews. According to one interviewee, a change to the current practice might not result in increased exchanges of personal data with Europol, because private parties would always prefer to share personal data with their 'closest contacts', which are the national LEAs.

Moreover, one interviewee expressed some concerns regarding the capacity of Europol to process an increased inflow of personal data from private parties. Another stakeholder reiterated the need for the ENUs to be kept informed of all data transfers that happen between private parties and Europol.

The discussion during the workshop confirmed the views taken by ENUs (as seen above) that **Europol's mandate could be expanded** thereby allowing Europol to exchange personal data directly with private parties. This would ensure a central and coordinated response. However, this would require **additional resources for Europol** in order to be able to cope with the amount of personal data it would receive from private parties.

One EU-level stakeholder targeted by the interviews explained that **any change to the currently applicable regulatory framework would have to be carefully assessed** to ensure that data protection and other fundamental rights related **safeguards remain respected**. Regarding this point the interviewee recalled that under the current regulatory framework, Article 26(2) of the Europol Regulation constitutes a derogation from the rules set out in Article 26(1) of the Europol Regulation. The latter provision sets out the 'traditional' mechanism for the exchanges of personal data between private parties and Europol. The intermediaries involved in this 'traditional' way of transferring personal data from the private parties to Europol make sure that the data exchanges are compliant with applicable data protection safeguards, as set out in national legislation. The purpose limitation of Europol's data processing activities, as set out in Article 26(2) of the Europol Regulation, stems from the fact that Europol is not in a position to check whether private parties comply with their national data protection related obligations while transferring personal data to Europol. Any amendment to this purpose limitation would have to address this issue.

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

4.2.3.1 The concept of national law enforcement authorities sharing personal data with private parties through Europol

As described under *Section 2: Background to the direct and indirect exchanges of personal data*, this study also covers a **scenario**, which is not currently regulated by the Europol Regulation. This scenario reflects the operational need to obtain personal data from private parties, and the difficulties national LEAs face when trying to obtain personal data from private parties, in particular if these are based outside their jurisdiction. LEAs might fail to obtain personal data from private parties this way, or might risk receiving only partial data, or data with some delays. On the other hand, private parties might be hesitant to share personal data with LEAs, also because they are not sure about the authenticity of the request received from a national LEA from another country.

The scenario captures one of the possible solutions to overcome this issue. Under this scenario Europol would act as an intermediary between LEAs and private parties. LEAs would be able to exchange personal data with private parties via Europol. The scenario also factors in a role for the ENUs given that communication between the LEAs and Europol typically happens through this intermediary.

The study aimed to explore the extent to which the issues covered by the scenario exist. Furthermore, it aimed to map whether the suggested solution of Europol acting as an intermediary would be the best suggested approach to overcome the challenge.

Box 11: Example illustrating the scenario

The given case concerns the access of LEAs to a database called WHOIS. This database is maintained by domain name operators (registries) and resellers (registrars) and provides information on domain names, including information on the domain holders' names. The Internet Corporation for Assigned Names and Numbers (ICANN), which is an organisation that coordinates the maintenance of WHOIS and 'ensures its secure operation and stability'[40], requires the registries and registrars to maintain this database. Before the entry into force of the GDPR[41], LEAs could retrieve personal data (e.g. names of domain name holders) from the WHOIS database easily, as such information was publicly available. Due to the entry into force of the GDPR, LEAs are no longer able to directly access the personal data held by the registries and registrars. LEAs' access to the WHOIS data is subject to the conclusion of a formal legal procedure with the registries and registrars.

The procedure has led to substantial administrative burdens for the LEAs and to long delays in obtaining personal data from WHOIS. In the given case, it was considered, also with the involvement of EDPS[42], how the issues could be resolved and whether Europol could play a role as:

- A simple accreditor giving assurance to the private parties that the LEAs approaching them are genuine LEAs;
- An actor providing a common European platform for the LEAs to channel their requests through Europol to selected private parties;
- An information exchange facilitator, with direct access to the exchanged personal data and with the possibility of adding operational value to the information exchanged.

4.2.3.2 Existence of the challenge

The box below provides a short description of the challenge:

Box 12: Existence of the challenge in the context of national LEAs obtaining personal data from private parties

- When trying to obtain non-publicly available personal data from the private parties without judicial authorisation or similar, LEAs reported on the following obstacles:
  - Late response from the private parties;
  - Incomplete datasets received from the private parties;
  - No response from the private parties;
  - Requests being refused.
- During the interviews, the interviewees confirmed that these issues seem to concern cross-border cases;

[40] General Secretariat of the Council 'EU Lines To Take on WHOIS policy reform', 23 October 2018, available at: https://data.consilium.europa.eu/doc/document/ST-13443-2018-INIT/en/pdf.

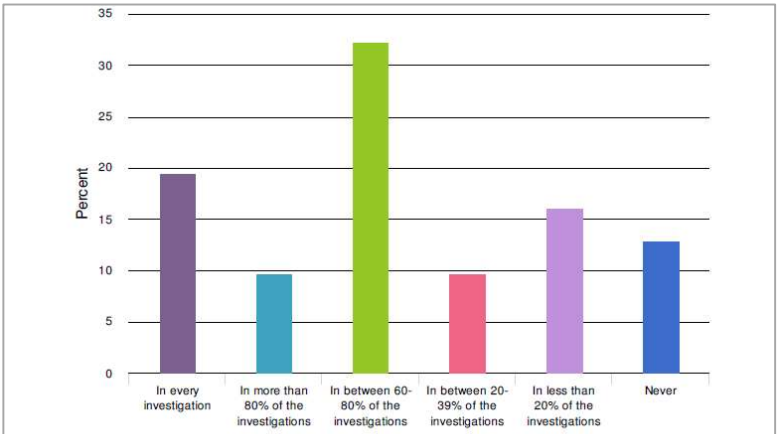
[41] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88, available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[42] EDPS, 'Europol's consultation on law enforcement access to WHOIS database', available at: https://edps.europa.eu/sites/edp/files/publication/18-09-07_letter_drewer_en.pdf

- Interviewees also confirmed that LEAs face difficulties when filing 'unofficial' requests with the private parties. Whilst the term 'unofficial' might mean different things depending on the jurisdiction concerned, it is understood that it typically covers the following scenarios: requests that are supposed to be filed with a judicial authorisation or similar, are being sent without such authorisation. Private parties can only address 'unofficial requests', when allowed by the applicable data protection framework.

The downloadable questionnaire, the survey and the interviews confirmed a growing need for LEAs to obtain personal data from private parties in their investigations, as illustrated in the visual below.

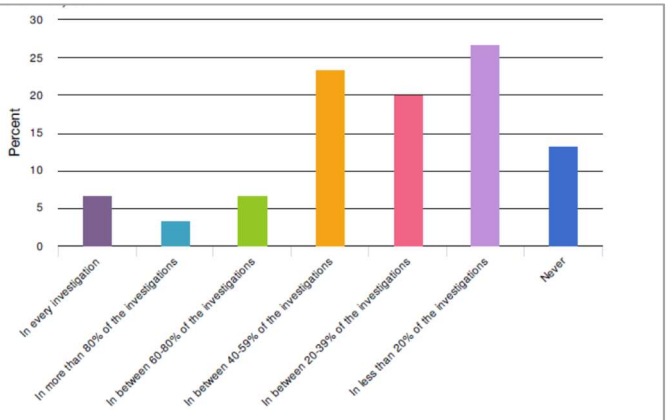
Figure 21: The need of LEAs to obtain personal data from private parties



Value	Percent	Responses
In every investigation	19.4%	6
In more than 80% of the investigations	9.7%	3
In between 60-80% of the investigations	32.3%	10
In between 20-39% of the investigations	9.7%	3
In less than 20% of the investigations	16.1%	5
Never	12.9%	4

The downloadable questionnaire, the survey and the interviews all confirmed that some LEAs face challenges while trying to obtain non-publicly available personal data from the private parties. The downloadable questionnaire targeting the LEAs revealed that most LEAs encounter difficulties – at least to a certain extent – while trying to obtain personal data from the private parties without judicial authorisation or similar. The LEAs experience is illustrated in the visual below.

Figure 22: Frequency of cases when LEAs face difficulties while obtaining personal data from private parties without judicial authorisation or similar



Value	Percent	Responses
In every investigation	6.7%	2
In more than 80% of the investigations	3.3%	1
In between 60-80% of the investigations	6.7%	2
In between 40-59% of the investigations	23.3%	7
In between 20-39% of the investigations	20.0%	6
In less than 20% of the investigations	26.7%	8
Never	13.3%	4

When asked about the **type of difficulties** that the LEAs face when obtaining personal data without a judicial authorisation, the majority of the stakeholders (17 responses, 58.6%) indicated that the **'information came too late'**, followed by 16 responses (55.2%) which indicated that the **'information was incomplete'**, another 13 responses (44.8%) indicated that they **'tried to obtain data, but did not receive a reply'** and a further 11 responses (37.9%) indicated that they **'tried to obtain data, but the request was refused'**. Ten responses (34.5%) referred to 'other' types of difficulties while the remaining responses indicated that they 'do not know who to contact' (one response, 3.4%) and they 'do not know they can contact the private party for data' (one response, 3.4%). It is noted that some stakeholders referred to the existence of multiple difficulties, while responding to the related question.

Only a limited number of **private parties** (two) responded to the relevant question of the survey asking about the **frequency of cases when they are being asked** by the LEAs without a judicial authorisation, warrant or similar, to provide them with non-publicly available personal data. The responses received from this small sample of stakeholders suggest that these cases either 'never' happen, or only happen 'less than 50 times' a year. These numbers seem to contradict the responses given by the LEAs. It is noted, however, that the sample responding to the question was small and thus the responses received might not be representative.

The interviews tried to clarify the views of the different stakeholder groups and gather additional information on the matter.

The interviews with the LEAs provided some context for the scenario as they clarified that **private parties are, as a general rule, under the legal obligation of responding to the national LEAs' request** for non-publicly available personal data. These requests are typically filed in the context of ongoing investigations and could be accompanied by judicial authorisation, warrant or similar, but this is not always the case. Five of the interviewees explained that the national legal framework clearly stipulates cases when the LEAs should require a **judicial authorisation, warrant or similar** when

asking for certain types of personal data from the private parties. For instance, a judicial authorisation is required when requesting personal data from the private parties that relate to the most intimate aspects of the data subject's life (example provided by one interviewee) or when accessing personal data stored on a mobile device (example provided by one interviewee). Moreover, different types of judicial authorisations might be required depending on the type of personal data being requested (personal data relating to a phone subscription or medical history, example provided by one interviewee).

The interviews, in addition to seeking some contextual information, tried to gather additional input from the LEAs regarding the difficulties they face. Three LEAs explained that the process of obtaining non-publicly available personal data from the private parties without judicial authorisation, a warrant or similar is less of a difficulty in the national context and more of an issue **in the cross-border context**. Making a request to a private party in a different jurisdiction creates difficulty, including practical issues such as finding the right contact details, utilising the right channels of communication and the manner in which personal data could be requested. This was also echoed by some of the participants during the workshop. The remaining interviewees either did not report on the existence of issues in connection with the process of obtaining non-publicly available personal data from private parties without a judicial authorisation or similar, or else noted that the only shortcoming to be mentioned is the fact that this process might be slow.

The context provided by the LEAs was also confirmed by the private parties. From among the private parties interviewed, only two had experience with this scenario. These were mainly private parties representing the financial and banking industry. Both interviewees confirmed that as a general rule, they **receive requests from the LEAs which are supported by judicial authorisation, warrant or similar**. Requests without such authorisation or similar are considered as unofficial and thus, as a general rule, are not addressed. Private parties can only exceptionally address unofficial requests when such action is in line with the legal framework covering the protection of personal data or else, when the circumstances necessitate the sharing of personal data without judicial authorisation. These latter cases could occur, for example, in the context of terrorism related activities. One of the interviewees also noted though that based on the data shared with them by the national LEAs in the context of the unofficial requests, they might start an internal investigation. These internal investigations might ultimately lead to the preparation of suspicious activity reports, which would then be submitted by the private parties to the national LEAs. Therefore, the LEAs might eventually obtain the information originally sought.

On the basis of the above it seems that the **challenge** of obtaining non-publicly available personal data from the private parties **exists** when:

- The LEAs **send an unofficial request for information to the private parties**;
- A request is filed in the context of an investigation, be it with or without a judicial authorisation, the LEAs as a general rule obtain personal data from the private parties. This is due to the fact that private parties seem to be under the legal obligation of responding to the requests received from the LEAs. Whilst this might be the case, stakeholders noted that information from the private parties as a response to a request filed without judicial authorisation or similar, **might come too late**, or **come in an incomplete form**. As referred to above, the stakeholders to the downloadable questionnaire also noted that it might happen that they do not receive the requested data sets or else their requests are refused. In line with the context provided by the stakeholders via the interviews, it is understood that such a scenario may occur when the request is unofficial.
- The LEAs request personal data from private parties in a cross-border context, and the request is not accompanied with a judicial authorisation or similar.

4.2.3.3 Possible solutions to the address the challenges

The box below provides a snapshot of the possible solutions that could be put in place to overcome the difficulties that the stakeholders currently face.

Box 13: Snapshot of views regarding the possible changes to the current practice

- Some stakeholders reported on the need to channel requests to and the responses from the private parties through Europol;
- Many stakeholders also considered a need for the exchange of good practices as a possible solution to overcome existing difficulties;
- The private parties were somewhat doubtful about the possible involvement of Europol in the exchanges of personal data between them and the national LEAs;
- Under the current regulatory framework (thus without changes to the Europol Regulation) the role that Europol can play as an intermediary is limited, as all of its processing activities would have to have a legal base in the Europol Regulation;
- The more data processing Europol would do, the higher the data protection and fundamental rights related safeguards should be, and the issue of liability would need to be addressed.

All data collection tools aimed to gather views on the possible solutions that could be used to address the main difficulties that the stakeholders currently face.

The LEAs, while completing the downloadable questionnaire, provided multiple suggestions on the matter. Most of the responses (19 responses, 67.9%) suggest that the difficulties linked to obtaining personal data from private parties without a judicial authorisation or similar, could be overcome if the LEAs could share best practices with each other. This was followed by 13 responses (46.4%) suggesting that Europol should maintain a platform for channelling requests between the national LEAs and the private parties. One response (3.6%) indicated that a third party, other than Europol (e.g. Interpol) could maintain a platform for channelling requests. Six responses (21.4%) referred to solutions 'other' than the above, indicating the importance of establishing and maintaining platforms for LEAs to channel requests.

The survey targeting the private parties registered two responses on the matter, both referring to the possible solution of 'private parties sharing best practices'.

The interviews tried to better understand the points of views of the different stakeholder groups in particular in connection with the possible solution of involving Europol in the exchanges of personal data between the private parties and the national LEAs in the role of an intermediary.

Three of the seven LEAs saw advantages in Europol channelling requests from national LEAs to private parties. Two of these LEAs indicated that the role of Europol would be especially helpful with cross-border cases including when the private party is established outside of the European Union. In these cases, Europol could play a central role in coordinating requests, help in identifying the right contacts and the manner in which a request for personal data shall be filed in the respective jurisdiction. Furthermore, another LEA mentioned that the role of Europol in these circumstances could expedite the procedure by gaining access to the personal data in a timely manner.

Another three LEAs indicated that they do not see any use for Europol's intermediary role in order to gain access to personal data from private parties as the national legal framework provides them with enough grounds to request personal data whether by means of a judicial authorisation or otherwise.

Out of the six private parties, three indicated that they did not have experience with the system and thus could not provide suggestions as to how the current obstacles could be removed.

The remaining three private parties recalled that their activities, including the activity of sharing personal data with the national LEAs, are currently regulated at national level. Some of these rules are set out in applicable data protection legislation. One interviewee expressed some concerns as to how Europol or any other third party could act as an intermediary for obtaining personal data from the private parties for the onward transfer of these datasets to the national LEAs, as this route would ultimately bypass the rules set by the national legislative frameworks. The remaining two recalled that in due regard to the applicable regulatory framework, they would only be able to respond to 'official' requests. From their point of view, the origin of the request is indifferent. Thus, they would treat requests filed directly by the LEAs and through Europol the same way.

The latter views were also confirmed by one of the EU-level stakeholders targeted by the interviews. This interviewee reiterated that from the private parties' point of view, it might not make a difference if they receive a request from Europol or from the national LEAs.

The same stakeholder noted that in case Europol's intermediary role is further explored as a possible solution, the following aspects would have to be further mapped:

- The precise role to be played by Europol ranging from being a simple certifier of the authenticity of requests filed by the national LEAs to the private parties, to being a data processor of data obtained from private parties;
- Depending on the role concerned, the extent of Europol's data processing activities would vary. The more extensive the data processing activities of Europol are, the more data protection concerns might arise, which would prompt the need for higher data protection standards for the individuals and clear justification for the processing activities.

A private party also recalled that any role to be played by Europol would have to have a legal basis in the Europol Regulation. Some of the roles that could potentially be foreseen for Europol might not have such a legal basis, thus - under the current Europol Regulation - Europol would not be able to play these roles.

The workshop also explored the possible involvement of Europol in the exchanges of personal data between the private parties and the LEAs. One participant stated that in their Member State, there is a centralised manner for LEAs to obtain personal data from private parties, including OSPs. This model could be utilised to centralise at a national level the requests from LEAs to private parties.

Furthermore, during the workshop the issue of liability was raised. If Europol were to be the main interlocutor between the LEAs and the private parties, the Europol Regulation would need to allow Europol to assume liability for the personal data that is shared.

5 CONCLUSIONS AND RECOMMENDATIONS

The conclusions and recommendations below are structured around the different systems used for the exchanges of personal data between the private parties and Europol.

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

The system of referrals and responses to referrals is a **widely used practice**. Since 2015, it has resulted in the removal of a large amount of terrorist content online and has led to the establishment of a solid working relationship between Europol and the OSPs. Building on this solid relationship, **OSPs would be increasingly willing to share personal data with Europol**, beyond the data contained in the referrals (thus personal data not limited to previously received referrals only). The **current system of sharing personal data does not sufficiently address these operational needs** as:

- Under the current rules, Europol would not be able to process these datasets for purposes other than the one set out in the current version of the Europol Regulation – allowing Europol to carry out data processing with the sole purpose of identifying the national ENU. As there is no obligation for the national ENUs to resubmit, the personal data shared by the OSPs might not reach Europol. Moreover, Europol faces difficulties in identifying the national ENUs, based purely on the data shared by the private parties, if these are not specific enough for this purpose. Under the current rules, Europol is not allowed to seek additional information from the private parties, and has to delete the data after four months, if it cannot identify the national ENU concerned based on the data at hand;
- From the OSPs' perspective proactive sharing can be burdensome and can 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.

To address the issue there is a **need to revise the rules of the Europol Regulation** applicable to the sharing of personal data. These rules should allow Europol to exchange personal data with OSPs for the purpose of analysis. The current limitations of Europol's legal regime should be lifted to allow for such analysis. Moreover, there is a need to boost the capacity of Europol (both technical and human resources) to cope with its extended role.

Europol receiving personal data from private parties via an intermediary

Europol typically receives personal data from the private parties through intermediaries i.e. LEAs and ENUs. Whilst this **'traditional' channel is commonly used**, stakeholders have reported on **some shortcomings which ultimately result in data losses and missed opportunities**. Private parties, due to the currently applicable EU regulatory framework, could be prevented from sharing certain datasets with the national LEAs. Moreover, in cases that concern multiple jurisdictions, the private parties might not be able to identify and share personal datasets with all LEAs concerned. LEAs and ENUs do not automatically transfer the data further to Europol. Whilst this might stem from legitimate, often legal reasons, the non-transfer might result in missed opportunities for Europol to fulfil its mandate. Moreover, judging from the involvement of multiple actors in the exchanges of personal data, the exchanges of personal data between private parties and Europol might be slow.

To address these issues, stakeholders provided the following recommendations:

- **Reinforcing Europol's ability to receive personal data directly from private parties, especially when the personal data relates to cross-border cases,** and to subsequently **process** the personal data received;

- Making adjustments to the regulatory framework, allowing private parties to **share personal data with the LEAs on more grounds** and potentially with **an extended group of LEAs**;
- Providing a **platform** for the private parties which operate within the same sector **to exchange personal data** among themselves, and for the private parties and the LEAs to intensify dialogues about the more targeted use of the current system;
- **Designating** within the private parties a **person to coordinate** the exchanges of personal data with the LEAs;
- **Raising awareness** of the current system of 'Europol receiving personal data from private parties via an intermediary', thereby reinforcing/intensifying its use.

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

The system of proactive sharing in its current form is **rarely used**, is perceived as being **complex** and overly **complicated**. When it is used, the system of resubmissions results in personal data reaching Europol with **a considerable delay**, which could ultimately render the data received obsolete or irrelevant.

Consequently, the current system is perceived to **result in data losses and missed investigative opportunities**.

According to the stakeholders consulted this necessitates **regulatory changes to the system**. There seems to be a need to reconsider the current purpose limitation restricting Europol's data processing activities to the sole purpose of identifying the ENU, which then might resubmit the personal data to Europol. This could ultimately result in an extended mandate for Europol to directly receive personal data from private parties. Stemming from the potentially extended mandate, there might be a need to provide Europol with the additional resources necessary to handle the anticipated increased volume of personal data received from the private parties. Moreover, data protection and fundamental rights related safeguards would have to be adjusted to the enhanced data processing activities of Europol.

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

The research confirmed a growing need for LEAs to obtain personal data from private parties in their investigations. The study also confirmed that **LEAs face challenges while trying to obtain non-publicly available personal data from the private parties.** These challenges occur when filing requests without a judicial authorisation or similar. Whilst many stakeholders **see a need for a change, views on the possible solutions are conflicting**. Some stakeholders have 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. As an alternative solution to the issue, some stakeholders recommended the establishment of platforms for exchanges of good practices between the LEAs.

ANNEXES

ANNEX 1 – BIBLIOGRAPHY

Council of the European Union, Europol's cooperation with strategic partners: strengths and possible inefficiencies in cooperation with Private Parties, July 2019

General Secretariat of the Council EU Lines To Take on WHOIS policy reform, October 2018

European Data Protection Supervisor, EDPS Opinion on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries, March 2018

European Data Protection Supervisor, EDPS Annual Report 2018

EDPS, Europol's consultation on law enforcement access to WHOIS database, September 2018

European Parliament, Joint Parliamentary Scrutiny Group on Europol, September 2019

European Parliament, Data exchanges: Strengthening Europol cooperation with non-EU countries, July 2018

European Parliament, Europol: The EU law enforcement cooperation agency, September 2019

Europol, SIRIUS EU Digital Evidence Situation Report 2019, 20 December 2019

Europol, Cryptocurrency experts meet at Europol to strengthen ties between law enforcement and private sector, June 2019

Europol, Europol and NTT Security team up to improve cybersecurity, June 2019

Europol, Europol Teams up with Industry Experts to Combat Phishing, March 2019

Europol, EU Internet Referral Unit - TRANSPARENCY REPORT 2017, September 2018

Europol, Europol's EU Internet Referral Unit partners with Belgium, France and the Netherlands to tackle online terrorist content, March 2018

Europol, The Jihadi Wolf Threat, June 2017

Europol, EU Internet Referral Unit – Year one report – Highlights, February 2016

Europol, International police action leads to rescue of 22-month old Romanian sex abuse victim', February 2015

Europol, Europol's strategic agreements with third countries, EU agencies and international organisations

Europol EU Internet Referral Unit – EU IRU

Europol, 'Europol Programming Document 2019-2021'

Gall F., Interoperable Law Enforcement Cooperation Challenges in the EU Area of Freedom, Security and Justice, February 2019

Keatinge T., Public-Private partnerships and Financial Crime: Advancing an inclusive model, December 2017

Maxwell N., Expanding the Capability of Financial Information Sharing Partnerships, March 2019

Statewatch News, Warnings over proposed new Europol partners in Middle East and North Africa, May 2018

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, OJ L 135, 24.5.2016, p. 53–114

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88, available at:

ANNEX 2 – SURVEY QUESTIONNAIRE TARGETING PRIVATE PARTIES

PROFILING QUESTIONS:

1. Are you replying as?

- Company / firm
- Business association
- Non-governmental organisation
- Other

If other, please specify the type of your organisation in the box below.

2. What is your organisation's main field of activity?

- Financial services
- Online content provider
- Internet service provider
- E-commerce
- Transportation industry
- Couriers and postal services
- Non-profit services
    - NGO dealing with battlefield information
    - NGO active in the fight against human trafficking
    - NGO active in the fight against child sexual abuse
    - NGO active in another field

If active in another field, please specify your organisation's main field of activity in the box below.

- Other

If other, please specify your organisation's main field of activity in the box below.

3. In which country is your organisation based / working from (not necessarily the same as where the headquarters are)?

- Austria
- Belgium
- Bulgaria
- Czech Republic
- Croatia
- Cyprus
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece

- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- United Kingdom
- Other

If other, please specify in the box below.

4. Please provide the name of your organisation and your position within the organisation in the box below.

5. If you are interested in being contacted for a follow-up interview, please provide your name and contact details in the box below.

6. Which type(s) of personal data exchanges does your organisation have experience with?

- Direct exchanges of personal data with Europol
- Indirect exchanges of personal data with Europol

7. Which type(s) of *direct* exchanges of personal data does your organisation have experience with?

- Sharing of personal data between Europol and private parties in the context of referrals
  - Europol transferring personal data to you as a private party via referrals
  - My organisation responding to a referral received from Europol
- Other forms of direct exchange (i.e. transfer is undoubtedly in the interest of the data subject, transfer is necessary in the interests of preventing the imminent perpetration of a crime)

8. Which type(s) of *indirect* exchanges of personal data does your organisation have experience with?

- Private parties sharing personal data with national law enforcement authorities
- Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing)

1. SHARING OF PERSONAL DATA BETWEEN EUROPOL AND PRIVATE PARTIES IN THE CONTEXT OF REFERRALS

1. a. Europol transferring (publicly available) personal data to you as a private party via referrals

9. On average, how many referrals does your organisation receive from Europol in a year?

- None
- Less than 50
- Between 50-150
- Between 151-500
- More than 500

If your organisation has precise data on the number of referrals received, please indicate these in the box below.

Reference period (please indicate the year(s) the data refer to)	Number of referrals (please provide numeric information)	Comment (free text, not mandatory)

10. How has the number of referrals received by your organisation from Europol evolved since the entry into force of the Europol Regulation (1 May 2017)?

- Increased
- Decreased
- Remained the same

11. How often does your organisation take down the content following the information received from Europol?

- Always (in 100% of cases)
- Almost always (in at least 90% of cases)
- Regularly (in at least 50% of cases)
- Sometimes (in less than 50% of cases)
- Rarely (in less than 10% of cases)
- Never

12. If the answer to the question above is 'sometimes', 'rarely', or 'never' it is because: Please select three options from the below list.

- The personal data received from Europol is limited / insufficient to justify the removal of the content
- There is a lack of internal resources to deal with data received
- There is uncertainty regarding the legal implications of action in the context of national regulatory framework
- Unclear deadline for taking the content down

- Lack of proper channel(s) to receive referrals in a coordinated manner
- Uncertainty about what specific action is expected to be taken
- Other reason

If other, please specify the reasons in the box below.

13. On average, how often does your organisation proactively take down online content – i.e. without responding to a referral - in a year?

- Never
- Less than 50 times
- Between 50-150 times
- Between 151-500 times
- More than 500 times

If your organisation has precise data on this, please indicate these in the box below.

Reference period (please indicate the year(s) the data refer to)	Number of cases when online content is proactively taken down (please provide numeric information)	Comment (free text, not mandatory)

14. How often do you inform Europol of cases when your organisation proactively takes down online content?

- Always (in 100% of cases)
- Almost always (in at least 90% of cases)
- Regularly (in at least 50% of cases)
- Sometimes (in less than 50% of cases)
- Rarely (in less than 10% of cases)
- Never

15. To what extent does your organisation consider the current practice of referrals (Europol transferring (publicly available) personal data to you as a private party via referrals) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

- Fully suitable
- Partially suitable
- Not at all suitable
- Not able to respond

Please explain your answer, based on your experience in the box below. In particular please provide concrete examples to cases where the personal data received from Europol was useful / not useful.

16. How could the current practice of referrals be improved?

1.b. Your organisation responding to a referral received from Europol

17. On average, how many responses to referrals does your organisation send back to Europol in a year?

- None
- Less than 50
- Between 50-150
- Between 151-500
- More than 500

If your organisation has precise data on the number of responses to referrals sent back to Europol, please indicate these in the box below.

Reference period (please indicate the year(s) the data refer to)	Number of responses to referrals (please provide numeric information)	Comment (free text, not mandatory)

18. How has the number of responses to referrals, as provided by your organisation to Europol, evolved since the entry into force of the Europol Regulation (1 May 2017)?

- Increased
- Decreased
- Remained the same

19. On average, how fast does your organisation respond to a referral received from Europol?

- Within an hour
- Within a day
- Within a week
- Within a month
- Over a month

20. In general, which crime(s) does your organisation's response to a referral relate to? Please select three options from the below list.

- Cybercrime
- Drug trafficking
- Facilitation of illegal immigration

- Organised property crime
- Trafficking in human beings
- Excise and MTIC[43] fraud
- Illicit firearms trafficking
- Environmental crime
- Criminal finances and money laundering
- Document fraud

21. How often has your organisation encountered difficulties in responding to a referral received from Europol?

    - Always (in 100% of cases)
    - Almost always (in at least 90% of cases)
    - Regularly (in at least 50% of cases)
    - Sometimes (in less than 50% of cases)
    - Rarely (in less than 10% of cases)
    - Never

22. What are the main obstacles to responding to referrals? Please select three options from the below list.

    - Regulatory burden (e.g. limitations posed by national data protection rules)
    - Administrative burden (procedure being complex / burdensome)
    - Lack of internal resources
    - Lack of contact person at Europol
    - Lack of proper channel / system for responding to referrals
    - Other obstacles

Please explain your answer, based on your experience in the box below.

23. To what extent does your organisation consider the current practice of responding to a referral received from Europol suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

    - Fully suitable
    - Partially suitable
    - Not at all suitable
    - Not able to respond

Please explain your answer, based on your experience and by including examples to cases where you think your response to a referral provided useful information to Europol.

24. How could the current practice of responding to a referral received from Europol be improved?

[43] Missing Trader Intra Community

2.a. Private parties sharing personal data with national law enforcement authorities

25. On average, how often does your organisation see the **need** for sharing personal data with national law enforcement authorities in a year?

- None
- Less than 50 times
- Between 50-150 times
- Between 151-500 times
- More than 500 times

If your organisation has precise data on the number of instances in which your organisation sees a **need** to transfer personal data to national law enforcement authorities, please indicate these in the box below.

Reference period (please indicate the year(s) the data refer to)	Number of instances where your organisation sees a **need** to transfer (please provide numeric information)	Comment (free text, not mandatory)

26. On average, how often does your organisation actually transfer personal data to national law enforcement authorities in a year?

- Never
- Less than 50 times
- Between 50-150 times
- Between 151-500 times
- More than 500 times

If your organisation has precise data on the number of transfers of personal data to national law enforcement authorities, please indicate these in the box below.

Reference period (please indicate the year(s) the data refer to)	Number of actual transfers (please provide numeric information)	Comment (free text, not mandatory)

27. How often does your organisation transfer such personal data proactively (i.e. on your own initiative and not as a response to a request from a national law enforcement authority)?

- Always (in 100% of cases)
- Almost always (in at least 90% of cases)
- Regularly (in at least 50% of cases)
- Sometimes (in less than 50% of cases)
- Rarely (in less than 10% of cases)
- Never

28. How has the number of transfers of personal data to national law enforcement authorities evolved since the entry into force of the Europol Regulation (1 May 2017)?

- Increased
- Decreased
- Remained the same

29. In general, which crime(s) are typically concerned by the transfer of personal data? Please select three options from the below list.

- Cybercrime
- Drug trafficking
- Facilitation of illegal immigration
- Organised property crime
- Trafficking in human beings
- Excise and MTIC[44] fraud
- Illicit firearms trafficking
- Environmental crime
- Criminal finances and money laundering
- Document fraud

30. Which law enforcement authorities does your organisation usually cooperate with for the transfer of personal data? Please select one option from the below list.

- National law enforcement authority in EU Member States (e.g. police bodies, customs, prosecution services)
- Contact point or authority in a third country outside the EU/ international organisation
- Other

If other, please specify the type of organisation in the box below

31. What is the basis of cooperation with this regular contact? Please select three options from the below list.

- Gentlemen's agreement
- Public-private partnership
- Previous experience
- Informal contacts
- Being referred to by another organisation
- Other

[44] Missing Trader Intra Community

If other, please specify the factors that you consider in the box below:

32. Are the national law enforcement authorities that your organisation usually cooperates with from the same country where you are based / working from (not necessarily the same as where the headquarters are)?

- Yes
- No

33. If not, in which country(ies) is/are the national law enforcement authorities based? Please select up to three options, reflecting countries where the national law enforcement authorities are most frequently based.

- Austria
- Belgium
- Bulgaria
- Czech Republic
- Croatia
- Cyprus
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- United Kingdom
- Other

If other, please specify the relevant country(ies) in the box below.

34. What are the reasons for cooperating with a national law enforcement authority that is based in a country other than the one where your organisation is based / working from? For instance, victims

or suspects concerned are from the country where the national law enforcement authority is established.

35. If your organisation needs to identify the relevant national law enforcement authorities (within the EU or beyond), how long does this take on average?

- An hour
- A day
- A week
- A month
- Over a month

36. On average, how quickly does your organisation transfer personal data to a relevant national law enforcement authority after tracing a potential criminal activity?

- Within an hour
- Within a day
- Within a week
- Within a month
- Over a month

37. How often has your organisation encountered obstacles while trying to transfer personal data to national law enforcement authorities?

- Always (in 100% of cases)
- Almost always (in at least 90% of cases)
- Regularly (in at least 50% of cases)
- Sometimes (in less than 50% of cases)
- Rarely (in less than 10% of cases)
- Never

38. What are the main obstacles for transferring personal data to national law enforcement authorities? Please select up to three main obstacles, which in your opinion are the most common ones.

- Difficulties in identifying the State concerned
- Several States being concerned by the personal data
- Not having contact in a State concerned
- Difficulties in identifying the national law enforcement authority concerned
- Regulatory burden (e.g. limitations posed by national data protection laws)
- Administrative burden (e.g. procedure being burdensome for my organisation)
- Lack of internal resources
- No platform available for transferring personal data
- Uncertain channel identified for the transfer of personal data
- Other

If other, please specify the reason(s) in the box below.

39. Has your organisation ever decided **not to** transfer personal data to national law enforcement authorities and instead decided to act differently?

- Yes
- No

40. If yes, how did your organisation proceed? Please select three options from the below list.

- Decided to transfer personal data directly to Europol (proactive sharing)
- Decided to contact or to seek advice from an umbrella organisation[45]
- Decided to seek advice from a national authority or Europol
- Decided not to transfer personal data at all
- Other

If other, please specify in the box below.

41. To what extent does your organisation consider the current practice of private parties sharing personal data with national law enforcement authorities suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

- Fully suitable
- Partially suitable
- Not at all suitable
- Not able to respond

Please explain your answer based on your experience in the box below. In particular, please provide concrete examples to cases where in your opinion you transferred data to a national law enforcement authority which would have been useful in the fight against cross-border crime, cybercrime and terrorism.

42. How could the current practice of private parties sharing personal data with national law enforcement authorities be improved?

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

43. On average, how often does your organisation share personal data directly with Europol (outside the context of referrals), in a year?

- Never
- Less than 50 times
- Between 50-150 times
- Between 151-500 times
- More than 500 times

[45] This term refers to a larger association, which coordinates the activities of its member organisations and works to protect their shared interests.

If your organisation has precise data on the number of cases, please provide these numbers in the box below.

Reference period (please indicate the year(s) the data refer to)	Number of transfers (please provide numeric information)	Comment (free text, not mandatory)

44. How has the number of proactive transfers of personal data (outside the context of referrals) to Europol evolved since the entry into force of the Europol Regulation (1 May 2017)?

- Increased
- Decreased
- Remained the same

45. In general, which crime/s are typically concerned by this transfer? Please select three options from the below list.

- Cybercrime
- Drug trafficking
- Facilitation of illegal immigration
- Organised property crime
- Trafficking in human beings
- Excise and MTIC[46] fraud
- Illicit firearms trafficking
- Environmental crime
- Criminal finances and money laundering
- Document fraud

46. For which reasons does your organisation proactively share personal data with Europol (outside the context of referrals)?

Please specify the reasons in the box below:

47. How often is your organisation informed by Europol that they could not process the personal data directly?

- Always (in 100% of cases)
- Almost always (in at least 90% of cases)
- Regularly (in at least 50% of cases)
- Sometimes (in less than 50% of cases)

[46] Missing Trader Intra Community

- Rarely (in less than 10% of cases)
- Never

48. Has your organisation ever decided not to transfer personal data directly to Europol at the first place and instead decided to act differently?

    - Yes
    - No

49. If yes, how did your organisation proceed?

    - Decided to transfer personal data through an intermediary (e.g. national law enforcement authority, such as police bodies, customs or prosecution offices)
    - Decided not to transfer personal data at all
    - Other

If other, please specify in the box below.

50. To what extent does your organisation consider the current practice of sharing personal data directly with Europol outside the context of referrals (proactive sharing) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

    - Fully suitable
    - Partially suitable
    - Not at all suitable
    - Not able to respond

Please explain your answer based on your experience in the box below. In particular, please provide concrete examples to cases where in your opinion you transferred data to Europol, which would have been useful in the fight against cross-border crime, cybercrime and terrorism.

51. How could the current practice of sharing personal data directly with Europol outside the context of referrals (proactive sharing) be improved?

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

52. On average, how often is your organisation requested – without receiving a judicial order or similar - to provide non-public personal data to national law enforcement authorities in a year?

- Never
- Less than 50 times
- Between 50-150 times
- Between 151-500 times
- More than 500 times

53. How often does your organisation decide **not to** provide personal data to national law enforcement authorities following this request?

- Always (in 100% of cases) decides not to
- Almost always (in at least 90% of cases) decides not to
- Regularly (in at least 50% of cases) decides not to
- Sometimes (in less than 50% of cases) decides not to
- Rarely (in less than 10% of cases) decides not to
- It never decides not to

54. What are the reasons for not providing personal data to a request filed by national law enforcement authorities? Please select up to three reasons, which in your opinion are the most common ones.

- Authentication of sender
- Request is too wide
- Request does not comply with internal procedures (e.g. sent to the wrong unit)
- Request is unclear
- Request is incomplete
- Organisation is not the right addressee
- Organisation does not have the data requested
- Other

If other, please indicate this reason(s) in the box below.

55. How would you suggest addressing the issue? Please select one option from the below list.

- Sharing best practices among private parties
- Europol to maintain a platform for channelling the request
- Third party (e.g. Interpol) to maintain a platform for channelling the request
- Other

If other, please complete the box below

ANNEX 3 – DOWNLOADABLE QUESTIONNAIRE TARGETING THE ENUS

PROFILING QUESTIONS:

1. Are you replying as? Please select the one, which is relevant.

   ☐ Member of Europol National Unit
   ☐ Liaison Officer
   ☐ Contact point in a third country
   ☐ Contact point in an international organisation
   ☐ Authority in a third country
   ☐ Authority in an international organisation
   ☐ National law enforcement authority[47]: Police
   ☐ National law enforcement authority: Prosecution office
   ☐ National law enforcement authority: Customs
   ☐ National law enforcement authority: Internal Referral Unit (IRU)
   ☐ Other national competent authority: national data protection authority
   ☐ Other

If other, please specify the type of your organisation in the box below.

2. What is your (not your organisation's) main field of activity? Please select up to three options from the below list. Fight against:

   ☐ Cybercrime
   ☐ Drug trafficking
   ☐ Facilitation of illegal immigration
   ☐ Organised property crime
   ☐ Trafficking in human beings
   ☐ Excise and MTIC[48] fraud
   ☐ Illicit firearms trafficking
   ☐ Environmental crime
   ☐ Criminal finances and money laundering
   ☐ Document fraud
   ☐ Other

If other, please specify your main field(s) of activity in the box below.

3. Which country is your organisation based in / does your organisation represent (this latter category being applicable to liaison officers)?

   ☐ Austria
   ☐ Belgium

[47] Law enforcement authority in charge of the prevention, investigation, detection or prosecution of criminal offences.
[48] Missing Trader Intra Community

☐ Bulgaria
☐ Czech Republic
☐ Croatia
☐ Cyprus
☐ Denmark
☐ Estonia
☐ Finland
☐ France
☐ Germany
☐ Greece
☐ Hungary
☐ Ireland
☐ Italy
☐ Latvia
☐ Lithuania
☐ Luxembourg
☐ Malta
☐ Netherlands
☐ Poland
☐ Portugal
☐ Romania
☐ Slovakia
☐ Slovenia
☐ Spain
☐ Sweden
☐ United Kingdom
☐Other

If other, please specify in the box below.

4. Please provide the name of your organisation and your position in the box below.

5. If you are interested in being contacted for a follow-up interview, please provide your name and contact details in the box below.

6. Which type(s) of personal data exchanges does your organisation have experience with /knowledge of?

☐ Direct exchanges of personal data between private parties and Europol
☐ Indirect exchanges of personal data between private parties and Europol

7. Which type(s) of *direct* exchanges of personal data does your organisation have experience with / knowledge of?

☐ Sharing of personal data between Europol and private parties in the context of referrals:
☐ Europol transferring personal data to a private party via referrals
☐ Private party responding to a referral received from Europol
☐ Other forms of direct exchange (i.e. transfer is undoubtedly in the interest of the data subject, transfer is necessary in the interests of preventing the imminent perpetration of a crime)

8. Which type(s) of *indirect* exchanges of personal data between Europol and private parties does your organisation have experience with / knowledge of?

☐ Private parties sharing personal data with national law enforcement authorities
☐ Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing)

1. SHARING OF PERSONAL DATA BETWEEN EUROPOL AND PRIVATE PARTIES IN THE CONTEXT OF REFERRALS

1.a. Europol transferring (publicly available) personal data to a private party via referrals

9. To what extent does your organisation consider the current practice of referrals (Europol transferring (publicly available) personal data to a private party via referrals) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

☐ Fully suitable
☐ Partially suitable
☐ Not at all suitable
☐ Not able to respond

Please explain your answer in the box below.

10. How could the current practice of referrals at the EU level be improved?

1.b. Private party responding to a referral received from Europol

11. To what extent does your organisation consider the current practice of responding to referrals (i.e. private party responding to a referral received from Europol) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

☐ Fully suitable
☐ Partially suitable
☐ Not at all suitable
☐ Not able to respond

Please explain your answer in the box below.

12. How could the current practice of responding to referrals be improved?

2.a. Private parties sharing personal data with national law enforcement authorities

13. On average, how often does your organisation transfer the personal data received from national law enforcement authorities to Europol in a year?

☐ Never
☐ Less than 50 times
☐ Between 50-150 times
☐ Between 151-500 times
☐ More than 500 times

If your organisation has precise data on the number of transfers of personal data to Europol, please indicate these in the box below.

Reference period (please indicate the year(s) the data refer to)	Number of transfers (please provide numeric information)	Comment (free text, not mandatory)

14. How has the number of transfers of personal data from private parties to Europol carried out by your organisation in this context Europol evolved since the entry into force of the Europol Regulation (1 May 2017)?

☐ Increased
☐ Decreased
☐ Remained the same

15. On average, how quickly does your organisation transfer personal data received from a national law enforcement authority to Europol?

☐ Within an hour
☐ Within a day

☐ Within a week
☐ Within a month
☐ Over a month

16. How often does your organisation NOT transfer the personal data obtained from private parties (through national law enforcement authorities) to Europol, even though the data may relate to another Member State or a third country?

☐ Always (in 100% of cases)
☐ Almost always (in at least 90% of cases)
☐ Regularly (in at least 50% of cases)
☐ Sometimes (in less than 50% of cases)
☐ Rarely (in less than 10% of cases)
☐ Never

17. What are the most frequent reasons for not transferring personal data obtained from private parties (through national law enforcement authorities) to Europol? Please select up to three reasons, which in your opinion are the most frequent.

☐ No on-going investigation in your Member State
☐ No legal basis to initiate an investigation in your Member State
☐ No victims
☐ No suspects
☐ No crime identified
☐ Minor infringement
☐ No apparent transborder aspect
☐ Workload/Lack of internal resources
☐ Other

If other, please specify the reason(s) in the box below:

18. To what extent does your organisation consider the current practice of private parties sharing personal data with national law enforcement authorities suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

☐ Fully suitable
☐ Partially suitable
☐ Not at all suitable
☐ Not able to respond

Please explain your answer based on your experience in the box below.

19. How could the current practice of private parties sharing personal data with national law enforcement authorities be improved?

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

20. On average, how often does Europol send your organisation (as representative of the Member State concerned) personal data it had received from a private party for resubmission, in a year?

☐ Never
☐ Less than 50 times
☐ Between 50-150 times
☐ Between 151-500 times
☐ More than 500 times

If your organisation has precise data on the number of cases when Europol sent your organisation personal data that it had received from a private party, please provide these numbers in the box below.

Reference period (please indicate the year(s) the data refer to)	Number of transfers (please provide numeric information)	Comment (free text, not mandatory)

21. How long does it take for your organisation on average to assess whether to resubmit entirely or partially the personal data?

☐ Less than an hour
☐ Less than a day
☐ Less than a week
☐ Less than a month
☐ Less than four months
☐ Over four months

22. On average, how often does your organisation resubmit personal data to Europol ?

☐ Always (in 100% of cases)
☐ Almost always (in at least 90% of cases)
☐ Regularly (in at least 50% of cases)
☐ Sometimes (in less than 50% of cases)
☐ Rarely (in less than 10% of cases)
☐ Never

If your organisation has precise data on the number of resubmissions, please provide these numbers in the box below.

Reference period (please indicate the year(s) the data refer to)	Number of resubmissions (please provide numeric information)	Comment (free text, not mandatory)

23. How has the number of resubmissions of personal data to Europol in this context evolved since the entry into force of the Europol Regulation (1 May 2017)?

☐ Increased
☐ Decreased
☐ Remained the same

24. What are the most frequent reasons for NOT resubmitting personal data to Europol? Please select up to three reasons, which in your opinion are the most frequent.

☐ No on-going investigation in my State
☐ No legal basis to initiate an investigation in my State
☐ No victims
☐ No suspects
☐ No crime identified
☐ Minor infringement
☐ No apparent transborder aspect
☐ Workload / Lack of resources to process the request
☐ Other

If other, please specify the reasons in the box below.

25. As a general rule, does the resubmission of personal data entail consultation of other national law enforcement authorities?

☐ Yes
☐ No

26. If yes, how often does your organisation have to consult other national law enforcement authorities in relation to the resubmission of personal data?

☐ Always (in 100% of cases)
☐ Almost always (in at least 90% of cases)
☐ Regularly (in at least 50% of cases)
☐ Sometimes (in less than 50% of cases)
☐ Rarely (in less than 10% of cases)

27. How often does it happen that national law enforcement authorities do not transfer back to your organisation the personal data and thus your organisation is no longer in a position to resubmit personal data to Europol?

☐ Always (in 100% of cases)
☐ Almost always (in at least 90% of cases)
☐ Regularly (in at least 50% of cases)
☐ Sometimes (in less than 50% of cases)
☐ Rarely (in less than 10% of cases)
☐ Never

28. To what extent does your organisation consider the current practice of private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

☐ Fully suitable
☐ Partially suitable
☐ Not at all suitable
☐ Not able to respond

Please explain your answer based on your experience in the box below.

29. How could the current practice of private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) be improved?

ANNEX 4 – DOWNLOADABLE QUESTIONNAIRE TARGETING THE LEAS

PROFILING QUESTIONS:

1. Are you replying as? Please select the one, which is relevant.

   ☐ Member of Europol National Unit
   ☐ Liaison Officer
   ☐ Contact point in a third country
   ☐ Contact point in an international organisation
   ☐ Authority in a third country
   ☐ Authority in an international organisation
   ☐ National law enforcement authority[49]: Police
   ☐ National law enforcement authority: Prosecution office
   ☐ National law enforcement authority: Customs
   ☐ National law enforcement authority: Internal Referral Unit (IRU)
   ☐ Other national competent authority: national data protection authority
   ☐ Other

If other, please specify the type of your organisation in the box below.

2. What is your (not your organisation's) main field of activity? Please select up to three options from the below list. Fight against:

   ☐ Cybercrime
   ☐ Drug trafficking
   ☐ Facilitation of illegal immigration
   ☐ Organised property crime
   ☐ Trafficking in human beings
   ☐ Excise and MTIC[50] fraud
   ☐ Illicit firearms trafficking
   ☐ Environmental crime
   ☐ Criminal finances and money laundering
   ☐ Document fraud
   ☐ Other

If other, please specify your main field(s) of activity in the box below.

3. Which country is your organisation based in / does your organisation represent (this latter category being applicable to liaison officers)?

[49] Law enforcement authority in charge of the prevention, investigation, detection or prosecution of criminal offences.
[50] Missing Trader Intra Community

☐ Austria
☐ Belgium
☐ Bulgaria
☐ Czech Republic
☐ Croatia
☐ Cyprus
☐ Denmark
☐ Estonia
☐ Finland
☐ France
☐ Germany
☐ Greece
☐ Hungary
☐ Ireland
☐ Italy
☐ Latvia
☐ Lithuania
☐ Luxembourg
☐ Malta
☐ Netherlands
☐ Poland
☐ Portugal
☐ Romania
☐ Slovakia
☐ Slovenia
☐ Spain
☐ Sweden
☐ United Kingdom
☐ Other

If other, please specify in the box below.

4. Please provide the name of your organisation and your position in the box below.

5. If you are interested in being contacted for a follow-up interview, please provide your name and contact details in the box below.

6. Which type(s) of personal data exchanges does your organisation have experience with /knowledge of?

☐ Direct exchanges of personal data between private parties and Europol

☐ Indirect exchanges of personal data between private parties and Europol

7. Which type(s) of *direct* exchanges of personal data does your organisation have experience with / knowledge of?

☐ Sharing of personal data between Europol and private parties in the context of referrals:
☐ Europol transferring personal data to a private party via referrals
☐ Private party responding to a referral received from Europol
☐ Other forms of direct exchange (i.e. transfer is undoubtedly in the interest of the data subject, transfer is necessary in the interests of preventing the imminent perpetration of a crime)

8. Which type(s) of *indirect* exchanges of personal data between Europol and private parties does your organisation have experience with / knowledge of?

☐ Private parties sharing personal data with national law enforcement authorities
☐ Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing)

1. SHARING OF PERSONAL DATA BETWEEN EUROPOL AND PRIVATE PARTIES IN THE CONTEXT OF REFERRALS

1. a. Europol transferring (publicly available) personal data to a private party via referrals

9. To what extent does your organisation consider the current practice of referrals (Europol transferring (publicly available) personal data to a private party via referrals) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

☐ Fully suitable
☐ Partially suitable
☐ Not at all suitable
☐ Not able to respond

Please explain your answer in the box below.

10. How could the current practice of referrals at the EU level be improved?

2.a. Private parties sharing personal data with national law enforcement authorities

11. On average, how often does your organisation transfer the personal data obtained from private parties to Europol National Unit, contact point, or authority in a third country or international organisation, in a year?

☐ Never
☐ Less than 50 times
☐ Between 50-150 times
☐ Between 151-500 times

☐ More than 500 times

If your organisation has precise data on the number of transfers of personal data to Europol National Unit, contact point, or authority in a third country or international organisation, please indicate these in the box below.

Reference period (please indicate the year(s) the data refer to)	Number of transfers (please provide numeric information)	Comment (free text, not mandatory)

12. How has the number of transfers of personal data to Europol National Unit, contact point, or authority in a third country or international organisation evolved since the entry into force of the Europol Regulation (1 May 2017)?

    ☐ Increased
    ☐ Decreased
    ☐ Remained the same

13. Is/are the private party/-ies that typically transfer the personal data to your organisation established in the same country as where you are competent to act?

    ☐ Yes
    ☐ No

14. If not, in which country/-ies is/are the private party/-ies based / working (not the same as having headquarters in a country)? Please select up to three countries where the private parties that typically transfer personal data are established.

    ☐ Austria
    ☐ Belgium
    ☐ Bulgaria
    ☐ Czech Republic
    ☐ Croatia
    ☐ Cyprus
    ☐ Denmark
    ☐ Estonia
    ☐ Finland
    ☐ France
    ☐ Germany
    ☐ Greece
    ☐ Hungary
    ☐ Ireland

☐ Italy
☐ Latvia
☐ Lithuania
☐ Luxembourg
☐ Malta
☐ Netherlands
☐ Poland
☐ Portugal
☐ Romania
☐ Slovakia
☐ Slovenia
☐ Spain
☐ Sweden
☐ United Kingdom
☐ Other

If other, please specify in the box below.

15. What are the reasons for cooperating with a private party that is established in another country? For instance, private party established in another country having information about your country's nationals.

16. On average, how quickly does your organisation transfer personal data obtained from a private party to Europol National Unit, contact point, or authority in a third country or international organisation?

☐ Within an hour
☐ Within a day
☐ Within a week
☐ Within a month
☐ Over a month

17. How often does your organisation NOT transfer the personal data obtained from private parties to Europol National Unit, contact point, or authority in a third country or international organisation, even though the data may relate to, or be linked to another Member State or a third country?

☐ Always (in 100% of cases)
☐ Almost always (in at least 90% of cases)
☐ Regularly (in at least 50% of cases)
☐ Sometimes (in less than 50% of cases)
☐ Rarely (in less than 10% of cases)
☐ Never

18. What are the most frequent reasons for not transferring personal data obtained from private parties to Europol National Unit, contact point, or authority in a third country or international organisation? Please select up to three reasons, which in your opinion are the most frequent.

☐ No on-going investigation in your Member State
☐ No legal basis to initiate an investigation in your Member State
☐ No victims
☐ No suspects
☐ No crime identified
☐ Minor infringement
☐ No apparent transborder aspect
☐ Lack of internal resources
☐ Regulatory burden (e.g. national laws obliging national law enforcement authorities to investigate cases first before transferring personal data further, restrictions posed by national data protection rules)
☐ Administrative burden (e.g. procedure being burdensome for my organisation)
☐ Other

If other, please specify the reason(s) in the box below.

19. To what extent does your organisation consider the current practice of private parties sharing personal data with national law enforcement authorities suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

☐ Fully suitable
☐ Partially suitable
☐ Not at all suitable
☐ Not able to respond

Please explain your answer based on your experience in the box below.

20. How could the current practice of private parties sharing personal data with national law enforcement authorities be improved?

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

21. In the context of your national regulatory framework, is your organisation consulted on the resubmission of personal data to Europol by ENU, contact point/authority in a third country or international organisation?

☐ Yes
☐ No
☐ It depends on the circumstances

If the answer is 'it depends', please specify these circumstances in the box below.

22. How often does the ENU, contact point/authority in a third country or international organisation consult your organisation (as representative of the Member State concerned) on the resubmission of personal data it had received from Europol in a year?

☐ Never
☐ Less than 50 times
☐ Between 50-150 times
☐ Between 151-500 times
☐ More than 500 times

If your organisation has precise data on this, please provide these numbers in the box below.

Reference period (please indicate the year(s) the data refer to)	Number of consultations (please provide numeric information)	Comment (free text, not mandatory)

23. How has the number of consultations on the resubmission of personal data to Europol evolved since the entry into force of the Europol Regulation (1 May 2017)?

☐ Increased
☐ Decreased
☐ Remained the same

24. On average, how long does it take for your organisation to reply to the ENU's/ contact point/ authority request or contact?

☐ Less than an hour
☐ Less than a day
☐ Less than a week
☐ Less than a month
☐ Less than four months
☐ Over four months

25. What are the most frequent reasons for advising the ENUs (contact points/authorities in third countries or international organisations) not to resubmit the personal data, which Europol received from directly from private parties? Please select up to three reasons, which in your opinion are the most frequent.

☐ No on-going investigation in my Member State
☐ No legal basis to initiate an investigation in my Member State

☐ No victims
☐ No suspects
☐ No crime identified
☐ Minor infringement
☐ No apparent transborder aspect
☐ Workload / Lack of resources to process the request
☐ Other

If other, please specify the reasons in the box below.

26. To what extent does your organisation consider the current practice of private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

☐ Fully suitable
☐ Partially suitable
☐ Not at all suitable
☐ Not able to respond

Please explain your answer based on your experience in the box below.

27. How could the current practice of private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) be improved?

2.c. National law enforcement authorities for sharing personal data with private parties via Europol

28. How often would your organisation need to obtain - without judicial authorisation - non-public personal data from private parties that are known to be available in a year?

☐ In every investigation
☐ In more than 80% of the investigations
☐ In between 60-80% of the investigations
☐ In between 40-59% of the investigations
☐ In between 20-39% of the investigations
☐ In less than 20% of the investigations
☐ Never

29. How often does your organisation face difficulties in obtaining - without judicial authorisation - non-public personal data from private parties that are known to be available in a year?

☐ In every investigation
☐ In more than 80% of the investigations

☐ In between 60-80% of the investigations
☐ In between 40-59% of the investigations
☐ In between 20-39% of the investigations
☐ In less than 20% of the investigations
☐ Never

30. What difficulties does your organisation typically face while obtaining - without judicial authorisation - non-public personal data from private parties? Please select up to three reasons, which in your opinion are the most frequent.

☐ My organisation has tried to obtain data in the past, but request was refused
☐ My organisation has tried to obtain data in the past, but did not receive a reply
☐ My organisation does not know who to contact
☐ My organisation does not know that they can contact the private party for data
☐ Information came too late
☐ Information received was incomplete
☐ Other

If other, please complete the box below.

31. What has your organisation tried doing to resolve the issue?

32. How would you suggest overcoming the issue? Please select up to one option from the below list.

☐ Sharing best practices among national competent authorities in charge of law enforcement
☐ Europol to maintain a platform for channelling the request
☐ Third party (e.g. Interpol) to maintain a platform for channelling the request
☐ Other

If other, please complete the box below.

ANNEX 5 – DOWNLOADABLE QUESTIONNAIRE TARGETING THE NATIONAL IRUS

PROFILING QUESTIONS:

1. Are you replying as? Please select the one, which is relevant.

   ☐ Member of Europol National Unit
   ☐ Liaison Officer
   ☐ Contact point in a third country
   ☐ Contact point in an international organisation
   ☐ Authority in a third country
   ☐ Authority in an international organisation
   ☐ National law enforcement authority[51]: Police
   ☐ National law enforcement authority: Prosecution office
   ☐ National law enforcement authority: Customs
   ☐ National law enforcement authority: Internal Referral Unit (IRU)
   ☐ Other national competent authority: national data protection authority
   ☐ Other

If other, please specify the type of your organisation in the box below.

2. What is your (not your organisation's) main field of activity? Please select up to three options from the below list. Fight against:
   ☐ Cybercrime
   ☐ Drug trafficking
   ☐ Facilitation of illegal immigration
   ☐ Organised property crime
   ☐ Trafficking in human beings
   ☐ Excise and MTIC[52] fraud
   ☐ Illicit firearms trafficking
   ☐ Environmental crime
   ☐ Criminal finances and money laundering
   ☐ Document fraud
   ☐ Other

If other, please specify your main field(s) of activity in the box below.

3. Which country is your organisation based in / does your organisation represent (this latter category being applicable to liaison officers)?

   ☐ Austria
   ☐ Belgium
   ☐ Bulgaria

[51] Law enforcement authority in charge of the prevention, investigation, detection or prosecution of criminal offences.
[52] Missing Trader Intra Community

☐ Czech Republic
☐ Croatia
☐ Cyprus
☐ Denmark
☐ Estonia
☐ Finland
☐ France
☐ Germany
☐ Greece
☐ Hungary
☐ Ireland
☐ Italy
☐ Latvia
☐ Lithuania
☐ Luxembourg
☐ Malta
☐ Netherlands
☐ Poland
☐ Portugal
☐ Romania
☐ Slovakia
☐ Slovenia
☐ Spain
☐ Sweden
☐ United Kingdom
☐ Other

If other, please specify in the box below.

4. Please provide the name of your organisation and your position in the box below.

5. If you are interested in being contacted for a follow-up interview, please provide your name and contact details in the box below.

6. Which type(s) of personal data exchanges does your organisation have experience with /knowledge of?

☐ Direct exchanges of personal data between private parties and Europol
☐ Indirect exchanges of personal data between private parties and Europol

7. Which type(s) of *direct* exchanges of personal data does your organisation have experience with / knowledge of?

☐ Sharing of personal data between Europol and private parties in the context of referrals:
☐ Europol transferring personal data to a private party via referrals
☐ Private party responding to a referral received from Europol
☐ Other forms of direct exchange (i.e. transfer is undoubtedly in the interest of the data subject, transfer is necessary in the interests of preventing the imminent perpetration of a crime)

8. Which type(s) of *indirect* exchanges of personal data between Europol and private parties does your organisation have experience with / knowledge of?

☐ Private parties sharing personal data with national law enforcement authorities
☐ Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing)

1. SHARING OF PERSONAL DATA BETWEEN EUROPOL AND PRIVATE PARTIES IN THE CONTEXT OF REFERRALS

1.a. Europol transferring (publicly available) personal data to a private party via referrals

2. On average, how many referrals does your organisation send to private parties in a year?
☐ None
☐ Less than 50
☐ Between 50-150
☐ Between 151-500
☐ More than 500

If your organisation has precise data on the number of referrals sent, please indicate these in the box below.

Reference period (please indicate the year(s) the data refer to)	Number of referrals (please provide numeric information)	Comment (free text, not mandatory)

3. How has the number of referrals sent by your organisation evolved since the establishment of your organisation?

☐ Increased
☐ Decreased
☐ Remained the same

4. In general, which crime/s are typically concerned by the referrals sent by your organisation to private parties? Please select up to three options from the below list.

☐ Cybercrime
☐ Drug trafficking
☐ Facilitation of illegal immigration
☐ Organised property crime
☐ Trafficking in human beings
☐ Excise and MTIC[53] fraud
☐ Illicit firearms trafficking
☐ Environmental crime
☐ Criminal finances and money laundering
☐ Document fraud

5. To what extent does your organisation consider the current practice of referrals (Europol transferring (publicly available) personal data to a private party via referrals) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

☐ Fully suitable
☐ Partially suitable
☐ Not at all suitable
☐ Not able to respond

Please explain your answer in the box below.

6. How could the current practice of referrals at the EU level be improved?

7. On average, how many responses to referrals does your organisation receive from private parties in a year?

☐ None
☐ Less than 50
☐ Between 50-150
☐ Between 151-500
☐ More than 500

If your organisation has precise data on the number of responses to referrals received, please indicate these in the box below. Please indicate to which period the numbers refer.

Reference period (please indicate the year(s) the data refer to)	Number of responses to referrals received (please provide numeric information)	Comment (free text, not mandatory)

[53] Missing Trader Intra Community

8. How has the number of responses to referrals received evolved since the establishment of your organisation?

   ☐ Increased
   ☐ Decreased
   ☐ Remained the same

9. On average, how fast does your organisation receive responses to a referral from private parties?

   ☐ Within an hour
   ☐ Within a day
   ☐ Within a week
   ☐ Within a month
   ☐ Over a month

10. In general, which crime(s) are typically concerned by the responses to a referral received from private parties? Please select up to three options from the below list.

    ☐ Cybercrime
    ☐ Drug trafficking
    ☐ Facilitation of illegal immigration
    ☐ Organised property crime
    ☐ Trafficking in human beings
    ☐ Excise and MTIC[54] fraud
    ☐ Illicit firearms trafficking
    ☐ Environmental crime
    ☐ Criminal finances and money laundering
    ☐ Document fraud

11. To what extent does your organisation consider the current practice of responding to referrals (i.e. private party responding to a referral received from Europol) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

    ☐ Fully suitable
    ☐ Partially suitable
    ☐ Not at all suitable
    ☐ Not able to respond

[54] Missing Trader Intra Community

Please explain your answer in the box below.

12. How could the current practice of responding to referrals be improved?

2.a. Private parties sharing personal data with national law enforcement authorities

13. To what extent does your organisation consider the current practice of private parties sharing personal data with national law enforcement authorities suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

    ☐ Fully suitable
    ☐ Partially suitable
    ☐ Not at all suitable
    ☐ Not able to respond

Please explain your answer based on your experience in the box below.

14. How could the current practice of private parties sharing personal data with national law enforcement authorities be improved?

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

15. To what extent does your organisation consider the current practice of private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

    ☐ Fully suitable
    ☐ Partially suitable
    ☐ Not at all suitable
    ☐ Not able to respond

Please explain your answer based on your experience in the box below.

16. How could the current practice of private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) be improved?

ANNEX 6 – DOWNLOADABLE QUESTIONNAIRE TARGETING THE NATIONAL DATA PROTECTION AUTHORITIES

PROFILING QUESTIONS:

1. Are you replying as? Please select the one, which is relevant.

☐Member of Europol National Unit
☐Liaison Officer
☐Contact point in a third country
☐Contact point in an international organisation
☐Authority in a third country
☐Authority in an international organisation
☐National law enforcement authority[55]: Police
☐National law enforcement authority: Prosecution office
☐National law enforcement authority: Customs
☐National law enforcement authority: Internal Referral Unit (IRU)
☐Other national competent authority: national data protection authority
☐Other

If other, please specify the type of your organisation in the box below.

2. What is your (not your organisation's) main field of activity? Please select up to three options from the below list. Fight against:

☐Cybercrime
☐Drug trafficking
☐Facilitation of illegal immigration
☐Organised property crime
☐Trafficking in human beings
☐Excise and MTIC[56] fraud
☐Illicit firearms trafficking
☐Environmental crime
☐Criminal finances and money laundering
☐Document fraud
☐Other

If other, please specify your main field(s) of activity in the box below.

[55] Law enforcement authority in charge of the prevention, investigation, detection or prosecution of criminal offences.
[56] Missing Trader Intra Community

3. Which country is your organisation based in / does your organisation represent (this latter category being applicable to liaison officers)?

☐Austria
☐Belgium
☐Bulgaria
☐Czech Republic
☐Croatia
☐Cyprus
☐Denmark
☐Estonia
☐Finland
☐France
☐Germany
☐Greece
☐Hungary
☐Ireland
☐Italy
☐Latvia
☐Lithuania
☐Luxembourg
☐Malta
☐Netherlands
☐Poland
☐Portugal
☐Romania
☐Slovakia
☐Slovenia
☐Spain
☐Sweden
☐United Kingdom
☐Other

If other, please specify in the box below.

4. Please provide the name of your organisation and your position in the box below.

5. If you are interested in being contacted for a follow-up interview, please provide your name and contact details in the box below.

6. Which type(s) of personal data exchanges does your organisation have experience with /knowledge of?

☐Direct exchanges of personal data between private parties and Europol
☐Indirect exchanges of personal data between private parties and Europol

7. Which type(s) of *direct* exchanges of personal data does your organisation have experience with / knowledge of?

☐Sharing of personal data between Europol and private parties in the context of referrals:
☐Europol transferring personal data to a private party via referrals
☐Private party responding to a referral received from Europol
☐Other forms of direct exchange (i.e. transfer is undoubtedly in the interest of the data subject, transfer is necessary in the interests of preventing the imminent perpetration of a crime)

8. Which type(s) of *indirect* exchanges of personal data between Europol and private parties does your organisation have experience with / knowledge of?

☐Private parties sharing personal data with national law enforcement authorities
☐Private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing)

1. SHARING OF PERSONAL DATA BETWEEN EUROPOL AND PRIVATE PARTIES IN THE CONTEXT OF REFERRALS

1.a. Europol transferring (publicly available) personal data to a private party via referrals

2. To what extent does your organisation consider the current practice of referrals (Europol transferring (publicly available) personal data to a private party via referrals) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

☐Fully suitable
☐Partially suitable
☐Not at all suitable
☐Not able to respond

Please explain your answer in the box below.

3. How could the current practice of referrals at the EU level be improved?

1.b. Private party responding to a referral received from Europol

4. On average, how often does your organisation receive questions from private parties in relation to the data protection aspects of responding to a referral received from Europol in a year?

☐Never
☐Less than 50 times
☐Between 50-150 times
☐Between 151-500 times
☐More than 500 times

5. What have been the main data protection issues raised by these requests?

6. On average, how long does it take for your organisation to respond to a request?

☐Within an hour
☐Within a day
☐Within a week
☐Within a month
☐Over a month

7. Would in your opinion less restrictive national data protection rules result in an increase of response to referrals?

☐Yes
☐No

Please explain your answer in the box below.

8. To what extent does your organisation consider the current practice of responding to referrals (i.e. private party responding to a referral received from Europol) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

☐Fully suitable
☐Partially suitable
☐Not at all suitable
☐Not able to respond

Please explain your answer in the box below.

9. How could the current practice of responding to referrals be improved?

2.a. Private parties sharing personal data with national law enforcement authorities

10. How often does your organisation receive requests in relation to data protection issues linked to private parties sharing personal data with national law enforcement authorities?

☐Never
☐Less than 50 times
☐Between 51-150 times
☐Between 151-500 times
☐More than 500 times

11. What have been the main data protection issues raised by these requests?

12. How long does it take for your organisation to respond to a request?

☐Within an hour
☐Within a day
☐Within a week
☐Within a month
☐Over a month

13. Would in your opinion less restrictive national data protection rules result in an increase of transfers?

☐Yes
☐No

Please explain your answer in the box below.

14. To what extent does your organisation consider the current practice of private parties sharing personal data with national law enforcement authorities suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

☐Fully suitable
☐Partially suitable
☐Not at all suitable
☐Not able to respond

Please explain your answer based on your experience in the box below.

15. How could the current practice of private parties sharing personal data with national law enforcement authorities be improved?

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

16. To what extent does your organisation consider the current practice of private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) suitable as a response to current and possible future threats posed by serious cross-border crime, cybercrime and terrorism?

☐Fully suitable
☐Partially suitable
☐Not at all suitable
☐Not able to respond

Please explain your answer based on your experience in the box below.

17. How could the current practice of private parties sharing personal data directly with Europol outside the context of referrals (proactive sharing) be improved?
