Council of the European Union

Brussels, 15 December 2020
(OR. en)

13908/20
ADD 1

SIRIS 96
ENFOPOL 344
COPEN 379
SCHENGEN 11
IXIM 135
CODEX 6

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2020) 543 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation.

Delegations will find attached document SWD(2020) 543 final.

Encl.: SWD(2020) 543 final

EUROPEAN
COMMISSION

Brussels, 9.12.2020
SWD(2020) 543 final

PART 1/2

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

{COM(2020) 796 final} - {SEC(2020) 545 final} - {SWD(2020) 544 final}

Table of contents

List of Tables

Glossary

Term or acronym	*Meaning or definition*
COSI	Standing Committee on Internal Security
EC3	European Cybercrime Centre
ECTC	European Counter Terrorism Centre
EDPS	European Data Protection Supervisor
EIS	European Information System
ENISA	EU Agency for Criminal Justice Cooperation
EPPO	European Public Prosecutor Office
ETIAS	European Travel Information and Authorisation System
eu-LISA	EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
FIUs	Financial Intelligence Units
FIU.net	a decentralised and sophisticated computer network supporting the Financial Intelligence Units in the EU
ICANN	Internet Cooperation for Assigned Names and Numbers
IPC3	Intellectual Property Crime Coordinated Coalition
JIT	Joint Investigation Team
JPSG	Joint Parliamentary Scrutiny Group
NCMEC	National Centre for Missing and Exploited Children
OLAF	European Anti-Fraud Office
QUEST	Querying Europol Systems
SIENA	Secure Information Exchange Network Application
SIS	Schengen Information System
SOCTA	Serious and Organised Threat Assessment
TCO	Terrorist Content Online
TFEU	Treaty on the Functioning of the European Union

1. POLITICAL AND LEGAL CONTEXT

1.1 Political context

As set out in the EU Security Union Strategy[1], Europe faces a security landscape in flux, with evolving and increasingly complex security threats. Criminals exploit the advantages that the digital transformation and new technologies[2] bring about, including the inter-connectivity and blurring of the boundaries between the physical and digital world.[3] The COVID-19 crisis adds to this, as criminals have quickly seized opportunities to exploit the crisis by adapting their modes of operation or developing new criminal activities.[4] Beyond the short-term impact on security, the COVID-19 crisis will shape the serious and organised crime landscape in the EU in mid- and long-term.[5]

These threats spread across borders, cutting across a variety of crimes that they facilitate, and manifest themselves in poly-criminal organised crime groups[6] that engage in a wide range of criminal activities. As action at national level alone does not suffice to address these transnational security challenges, Member States' law enforcement authorities have increasingly made use of the support and expertise that Europol[7], the EU agency for law enforcement cooperation, offers to counter serious crime and terrorism. Since the entry into application of the 2016 Europol Regulation[8], the operational importance of the agency's tasks has changed substantially.

The threat environment changes the support Member States need and expect from Europol to keep citizens safe, in a way that was not foreseeable when the co-legislators negotiated the current Europol mandate. For example, the December 2019 Council Conclusions acknowledge "*the urgent operational need for Europol to request and receive data directly from private parties*", calling on the Commission to consider adapting the schedule for the review of the Europol Regulation "*in view of the need for European law enforcement to address ongoing technological developments*".[9] Indeed, there is a pressing social need to counter serious crimes prepared or committed using

---

1 COM(2020) 605 final (24.7.2020).

2 In July 2020, French and Dutch law enforcement and judicial authorities, alongside Europol and Eurojust, presented the joint investigation to dismantle EncroChat, an encrypted phone network used by criminal networks involved in violent attacks, corruption, attempted murders and large-scale drug transports (https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe).

3 The integration of digital systems in many criminal activities and the expansion of the online trade in illicit goods and services is transforming serious and organised crime. See Europol, Serious and Organised Threat Assessments 2017.

4 www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis. This is notably the case on cybercrime, fraud, counterfeiting and organised property crime.

5 https://www.europol.europa.eu/publications-documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu.

6 More than 5 000 organised crime groups were under investigation in Europe in 2017 – a 50% rise compared to 2013. 45% of the organised crime groups were involved in more than one criminal activity. The share of these polycriminal groups increased sharply. Organised crime groups often engage in more than one criminal activity. They are highly flexible and able to shift from one criminal activity to another. Europol, Serious and Organised Threat Assessments 2017.

7 Europol was established in 1995 on the basis of the Europol Convention.

8 Regulation (EU) 2016/794 (11.5.2016).

9 https://www.consilium.europa.eu/media/41586/st14755-en19.pdf. Regulation (EU) 2016/794 foresees an evaluation assessing the impact, effectiveness and efficiency of Europol by May 2022.

cross-border services offered by private parties,[10] notably cybercrimes.

While these threats are persistent and tenacious, access by law enforcement to the necessary data is an increasing challenge. [11] The growth in cybercrime and cyber-enabled crimes has a direct impact on citizens, with most people in the EU (55 %) concerned about their data being accessed by criminals and fraudsters.[12] Cybercriminals have been among the most adept at exploiting the COVID-19 pandemic, making the impact of the pandemic on cybercrime the most striking when compared to other criminal activities.[13] The e-evidence package[14], once adopted, will deliver an effective tool for national authorities to improve access to the relevant digital evidence and investigate these crimes. Beyond this initiative, there might be other important situations where further EU-level support is necessary to counter the threats posed by cybercrime and cyber-enabled crimes effectively, notably when private parties seek to report such crimes.

In response to pressing operational needs, and calls by the co-legislators for stronger support from Europol, the Commission Work Programme for 2020 announced a legislative initiative to "*strengthen the Europol mandate in order to reinforce operational police cooperation*".[15] This is also a key action of the EU Security Union Strategy. Consequently, **this impact assessment focuses on policy options to strengthen the Europol mandate**. In line with the call by the Political Guidelines[16] to "*leave no stone unturned when it comes to protecting our citizens*", this impact assessment addresses those areas where stakeholders ask for reinforced support from Europol.

Table 1 (p. 12) provides an overview of the problems addressed in this impact assessment, their drivers and how they link to the objectives. *Table 3* (p. 41) provides an overview of the link between the objectives and policy options addressed in this impact assessment. *Table 4* (p. 82) lists the preferred policy options that result from the assessment.

1.2 Europol as EU agency for law enforcement cooperation

Europol, the European Union Agency for Law Enforcement Cooperation, is the **centrepiece for EU-level support** to Member States in countering serious crime and terrorism. The agency offers support and expertise to national law enforcement authorities in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.

---

10 The term 'private parties' refers to organisations with a legal personality other than public authorities. This includes, but is not limited to, undertakings established under civil law, even if they are owned or controlled by a public authority.

11 Europol Internet Organised Crime Threat Assessment 2019.

12 European Union Agency for Fundamental Rights: Your rights matter: Security concerns and experiences, Fundamental Rights Survey (2020).

13 Europol Report: Catching the virus: cybercrime, disinformation and the COVID-19 pandemic (3.4.2020).

14 COM(2018) 225 final (17.4.2018) and COM(2018) 226 final (17.4.2018).

15 COM(2020) 37 final (29.1.2020). Given the need to reinforce Europol, as also expressed in the Council's call on the Commission to consider adapting the schedule for the review of the implementation of the Europol Regulation, the Commission therefore decided to strengthen the Europol mandate ahead of the evaluation of the impact, effectiveness and efficiency of the agency and its working practices as foreseen under the Europol Regulation by May 2022.

16 Political Guidelines: https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

Member States rely on the information sharing capabilities that Europol as the **EU criminal information hub** provides. The backbone of this is Europol's Secure Information Exchange Network Application (SIENA), which connects Europol's liaison officers, analysts and experts, law enforcement agencies in all Member States, as well as a growing number of third countries. The Europol Information System (EIS) is Europol's central criminal information and intelligence database used by Europol officials, Member State liaison officers, and seconded national experts stationed at Europol headquarters, as well as staff in law enforcement authorities in the Member States.

Member States also make use of the support Europol offers for **operational coordination**, especially in large-scale operations involving several countries. Europol's Operational Centre is the hub for the exchange of data among Europol, Member States and third countries on criminal activity. All of Europol's operational and information technology services are available to Member States. In addition, a mobile office can be deployed for on-the-spot support operations in Member States, thus providing a live connection to Europol's databases and platforms.

National law enforcement authorities also use Europol's analytical products in support of their investigations. Europol's **operational analysis** supports criminal investigations and criminal intelligence operations. Europol applies a range of data processing methods and techniques to perform operational analysis on suspects, convicted persons and persons where there are factual indications or reasonable grounds to believe they will commit criminal offences, and where necessary also on contacts and associates. Europol's **strategic analysis** products aim to give an insight and better understanding of crime and criminal trends in general, helping decision-makers identify priorities in the fight against organised crime and terrorism.

Europol offers a variety of **forensic analysis tools** to assist national law enforcement authorities, such as the Universal Forensic Extraction Device as a stand-alone mobile forensic kit that can extract data from 95 % of all mobile phones.

Europol's specialised centres provide tailor-made operational support and expertise to counter organised crime, cybercrime and terrorism. For example, the **European Cybercrime Centre** (EC3) strengthens the law enforcement response to cybercrime in the EU and thus helps protect European citizens, businesses and governments from online crime. EC3 offers its advanced digital forensics tools and platforms to investigations and operations in Member States, thus enabling a collective EU response to cybercrimes. The **European Counter Terrorism Centre** (ECTC) provides operational support to Member States in investigations following terrorist attacks. It cross-checks operational data against the data Europol already has, quickly bringing financial leads to light, and analyses all available investigative details to assist in compiling a structured picture of the terrorist network. The ECTC is now part of almost every major counter-terrorism investigation in the EU. Beyond the specialised centres, a number of thematic initiatives support law enforcement on crime-specific activities. For example, the **Intellectual Property Crime Coordinated Coalition (**IPC3) provides operational and technical support to law-enforcement agencies and other partners in the EU and beyond by facilitating and coordinating cross-border investigations, and monitoring and reporting online crime trends and emerging *modi operandi*. It also contributes to raising public awareness of intellectual property crimes and provides training to law enforcement in how to combat it.

Since the entry into application of the Europol Regulation, the **operational importance**

of the support provided by the agency has changed substantially.[17]

1.3 Legal context: the Europol Regulation

Europol operates on the basis of Regulation (EU) 2016/794 ('Europol Regulation').[18] Europol's mission is to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy, fulfilling its Treaty-based objective set out in Article 88(1) TFEU. The Europol Regulation entered into force on 13 June 2016 and took effect in all Member States on 1 May 2017.

The Europol Regulation pursues the following objectives:

- Europol should be a **hub for information exchange** in the Union. Information collected, stored, processed, analysed and exchanged by Europol includes criminal intelligence which relates to information about crime or criminal activities falling within the scope of Europol's objectives, obtained with a view to establishing whether concrete criminal acts have been committed or may be committed in the future.[19]
- Europol should increase the level of its **support to Member States**, so as to enhance mutual cooperation and the sharing of information.[20]
- To improve Europol's effectiveness in providing accurate crime analyses to the competent authorities of the Member States, it should use **new technologies to process data**. Europol should be able to swiftly detect links between investigations and common *modi operandi* across different criminal groups, to check cross-matches of data and to have a clear overview of trends, while guaranteeing a high level of protection of personal data for individuals. Therefore, Europol databases should be structured in such a way as to allow Europol to choose the most efficient IT structure.[21]
- Europol should also be able to act as a **service provider**, in particular by providing a secure network for the exchange of data, such as the secure information exchange network application (SIENA), aimed at facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations.[22]
- In order to ensure a **high level of data protection**, the purpose of processing operations and access rights as well as specific additional safeguards should be laid down. In particular, the principles of necessity and proportionality should be observed with regard to the processing of personal data.[23]
- Serious crime and terrorism often have links beyond the territory of the Union. Europol should therefore be able to exchange personal data with authorities of **third countries** to the extent necessary for the accomplishment of its tasks.[24]

---

17 See annex 4 for the increased operational support by Europol.

18 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.

19 Recital 12 of Regulation (EU) 2016/794.

20 Recital 13 of Regulation (EU) 2016/794.

21 Recital 24 of Regulation (EU) 2016/794.

22 Recital 24 of Regulation (EU) 2016/794.

23 Recital 24 of Regulation (EU) 2016/794.

24 Recital 32 of Regulation (EU) 2016/794.

The level of **data protection** at Europol is a crucial aspect for the work and success of the agency. Europol rightly claims to have one of the most robust data protection frameworks in the world of law enforcement, which has turned into an asset in the cooperation with national law enforcement authorities and is an important reason for the agency's success. For Europol to fulfil its mandate effectively and successfully, it is essential that all data processing by Europol and through its infrastructure takes place with the highest level of data protection. First, providing the highest level of data protection is necessary for citizens to have trust in the work of Europol. Second, Member States likewise demand that Europol processes data with the highest data protection standards, as they need to be confident that Europol provides for data security and confidentiality before they share their data with the agency, and ensure the legal sustainability of the criminal investigations.

Chapter VI of the Europol Regulation on *General data protection safeguards* provides a **comprehensive set of detailed safeguards** to guarantee a robust and high level data protection, transparency and liability to the day-to-day operations of the agency. It consists of a series of general and specific data protection principles, measures, obligations, responsibilities, requirements, limitations, data subject rights and external independent supervision.

The **European Data Protection Supervisor** (EDPS)[25] is responsible for the external supervision of all of Europol's data processing operations. Any new type of processing operation by the agency shall be subject to prior consultation by the EDPS.[26] The **Europol Cooperation Board**,[27] composed of a representative of a national supervisory authority[28] of each Member State and of the EDPS, may issue opinions, guidelines, recommendations and best practices related to data protection matters to Europol. A **Joint Parliamentary Scrutiny Group** (JPSG),[29] consisting of representatives of the European Parliament together with national parliaments, politically monitors Europol's activities in fulfilling its mission, including as regards the impact of those activities on the Fundamental Rights and freedoms of natural persons. Within Europol, the Data Protection Function, which is headed by Europol's Data Protection Officer (DPO[30]) and which acts with functional independence, works closely with Europol staff, offering advice and guidance in line with best practices on the processing of personal data.

The Europol Regulation sets out general **data protection principles** that require the agency to process personal data fairly and lawfully in a manner that ensures appropriate security, to collect data for specified, explicit and legitimate purposes and not further process the data in a manner incompatible with those purposes. According to these principles, personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed, accurate and kept up to date and in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed.[31] The Europol Regulation also foresees a system to assess the reliability of the source and accuracy of information processed at Europol, either received by a Member State or from a Union body, third country, international organisation or private party, or retrieved from publically available

25 Article 43 of Regulation (EU) 2016/794.
26 Article 39 of Regulation (EU) 2016/794.
27 Article 45 of Regulation (EU) 2016/794.
28 Article 42 of Regulation (EU) 2016/794.
29 Article 51 of Regulation (EU) 2016/794.
30 Article 41 of Regulation (EU) 2016/794.
31 Article 28 of Regulation (EU) 2016/794.

sources.[32]

The Europol Regulation limits the processing of personal data by the agency to data related to **specific categories of data subjects** listed in annex II of the Regulation (i.e. persons related to a crime for which Europol is competent).[33] However, there is a lack of legal clarity in the Europol Regulation in that respect, as the Regulation does not set out explicitly how the agency can comply with this requirement when processing personal data to meet its objectives and fulfil its tasks.[34]

Special requirements are set in the Europol Regulation as regards the processing of **special categories of personal data**. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data or data concerning a person's health or sex life is prohibited, unless it is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives and if those data supplement other personal data processed by Europol.[35]

Moreover, the Europol Regulation provides for time limits for the **storage and erasure of personal data**. Europol shall store personal data only for as long as is necessary and proportionate for the purposes for which the data are processed and in any event review the need for continued storage no later than three years after the start of initial processing of personal data. Europol may decide on the continued storage of personal data until the following review, which shall take place after another period of three years, if continued storage is still necessary for the performance of Europol's tasks. The reasons for the continued storage shall be justified and recorded. If no decision is taken on the continued storage of personal data, that data shall be erased automatically after three years.[36]

Furthermore, the Europol Regulation provides a series of **safeguards focused specifically on the data subjects**. Europol shall communicate a personal data breach to the data subject without undue delay (data breach notification).[37] The data subject has the right to obtain information on whether personal data relating to him or her are processed by Europol (right of access),[38] to request Europol to rectify personal data concerning him or her held by Europol if they are incorrect or to complete or update them, as well as to erase such data if they are no longer required for the purposes for which they are collected or are further processed (right of rectification, erasure and restriction).[39]

As set out in more detail in chapter 2, **all problems addressed in this impact assessment have newly emerged** since the adoption of the Europol Regulation in 2016. They are all driven by the way criminals exploit the advantages which the digital transformation and new technologies bring about. It was not an objective of the Europol Regulation to address these problems.

---

32 Article 29 of Regulation (EU) 2016/794.

33 Article 18(5) of Regulation (EU) 2016/794 limits the processing of personal data by Europol to the categories of data subjects listed in annex II of that Regulation. The categories of data subjects cover: (1) suspects, (2) convicted persons, (3) persons regarding whom there are factual indications or reasonable grounds to believe that they will commit, (4) persons who might be called on to testify in investigations or in subsequent criminal proceedings, (5) victims, (6) contacts and associates of a criminal, and (7) persons who can provide information on a crime.

34 For more details see annex 4 on past performance of Regulation (EU) 2016/794. This points is addressed in problem II on the big data challenge and in the related objective and policy options.

35 Article 30 of Regulation (EU) 2016/794.

36 Article 31 of Regulation (EU) 2016/794.

37 Article 35 of Regulation (EU) 2016/794.

38 Article 36 of Regulation (EU) 2016/794.

39 Article 37 of Regulation (EU) 2016/794.

1.4 Ensuring full compliance with Fundamental Rights

Given the importance of the processing of personal data for the work of law enforcement in general, and for the support provided by Europol in particular, this impact assessment puts a particular focus on the need to ensure full compliance with **Fundamental Rights** as enshrined in the Charter of Fundamental Rights, and notably the rights to the **protection of personal data**[40] and to respect for private life.[41]

As almost all problems, objectives and policy options addressed in this impact assessment involve the processing of personal data, any resulting limitation on the exercise of Fundamental Rights must be limited to what is strictly necessary and proportionate. The **thorough consideration of Fundamental Rights** in this impact assessment, and notably of the rights to the protection of personal data and to respect for private life, is based on a detailed assessment of policy options in terms of their limitations on the exercise of Fundamental Rights set out in annex 5.

The assessment of Fundamental Rights in annex 5 applies the Commission's Operational guidance on taking account of Fundamental Rights in Commission impact assessments,[42] the handbook by the Fundamental Rights Agency on Applying the Charter of Fundamental Rights,[43] and – for the first time in a Commission impact assessment – the toolkits[44] provided by the European Data Protection Supervisor on assessing necessity and proportionality. Based on this guidance, **annex 5 on Fundamental Rights**:

- describes the policy options discarded at an early stage due to their serious adverse impact on Fundamental Rights;
- sets out a step-by-step assessment of necessity and proportionality;
- outlines the rejected policy options if a less intrusive but equally effective option is available; and
- provides for a complete list of detailed safeguards for those policy options where a limitation on the exercise of Fundamental Rights is necessary, also due to the absence of a less intrusive but equally effective option.

Moreover, chapter 8 of this impact assessment provides an assessment of the **accumulated impact** of the preferred policy options on Fundamental Rights.

1.5 Other relevant EU initiatives

This impact assessment takes account of a wide range of relevant Commission initiatives that have been adopted or launched since the entry into force of the Europol Regulation.

As regards lack of effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals (see problem I as identified in chapter 2), the assessment of options to strengthen this cooperation takes account of the initiatives for the removal of **terrorist content online**[45] and to improve

---

40 Article 8 of the Charter of Fundamental Rights of the European Union (hereinafter, 'the Charter').
41 Article 7 of the Charter.
42 SEC(2011) 567 final (6.5.2011).
43 European Union Agency for Fundamental Rights: Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level (2018).
44 European Data Protection Supervisor: Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit (11.4.2017); European Data Protection Supervisor: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019).
45 COM(2018) 640 final (12.9.2018).

cross-border access to **electronic evidence** (e-evidence).[46] Once adopted, the e-evidence package will provide national law enforcement and judicial authorities with European Production Orders and European Preservation Orders to obtain digital evidence from service providers for criminal investigations, irrespective of the location of the establishment of the provider or the storage of the information.

As regards gaps on innovation and research relevant for law enforcement (see problem III as identified in chapter 2), the assessment of options to close this gap takes account of **EU security-related funding** under Horizon 2020,[47] the Internal Security Fund,[48] the proposed Horizon Europe[49] and the proposed Digital Europe programme.[50] It also takes account of the European strategy for data[51] and the White Paper on Artificial Intelligence[52] as the first pillars of the new digital strategy of the Commission, as well as the on-going work in preparation of governance of common European data spaces.[53]

As regards limits in the sharing of third-country sourced information on suspects and criminals (see annex 6), the assessment of options to strengthen this information sharing takes account of the on-going work towards the interoperability[54] of EU information systems for security, border and migration management and the **EU legal framework on large scale IT systems**. This includes existing or planned EU information systems, namely the Schengen Information System,[55] the EU Entry/Exit System,[56] the European Travel Information and Authorisation System,[57] and the proposed upgrading of the Visa Information System.[58]

This impact assessment takes full account of the relevant **EU data protection legislation**. As set out in chapter 2, this impact assessment is based on the assumption that as part of the legislative initiative to strengthen the Europol mandate, the Regulation[59] on the processing of personal data by EU institutions, bodies, offices and agencies will become fully applicable to Europol. This impact assessment also takes inspiration from the Data Protection Law Enforcement Directive.[60] Moreover, in the context of Europol's cooperation with private parties, this impact assessment takes account of the General Data Protection Regulation.[61]

The impact assessment also takes account of Europol's cooperation with **other Union bodies**, notably the European Public Prosecutor's Office[62], Eurojust[63] as the EU agency

---

46 COM(2018) 225 final and COM(2018) 226 final (17.4.2018) ("e-evidence package").
47 Regulation (EU) No 1291/2013 (11.12.2013).
48 Regulation (EU) No 513/2014 (16.4.2014). See also the Commission proposal for the Internal Security Fund for the next multiannual financial framework (COM(2018) 472 final (13.6.2018)).
49 COM(2018) 435 final (7.6.2018).
50 COM(2018) 434 final (6.6.2018).
51 COM(2020) 66 final (19.2.2020).
52 COM(2020) 65 final (19.2.2020).
53 Inception impact assessment for a legislative framework for the governance of common European data spaces (Ref. Ares(2020)3480073 - 02/07/2020).
54 Regulation (EU) 2019/818.
55 Regulation (EU) 2018/1862
56 Regulation (EU) 2017/2226 (30.11.2017).
57 Regulation (EU) 2018/1240 (12.9.2018).
58 COM(2018) 302 final (16.5.2018).
59 Regulation (EU) 2018/1725.
60 Directive (EU) 2016/680.
61 Regulation (EU) 2016/679.
62 Council Regulation (EU) 2017/1939 (12.10.2017).
63 Regulation (EU) 2018/1727 (14.11.2018).

for criminal justice cooperation, ENISA as the European Agency for Cyber Security[64] and the European Anti-Fraud Office (OLAF).[65]

64 Regulation (EU) 2019/881 (17.4.2019).
65 Regulation (EU, Euratom) No 883/2013 (11.9.2013).

problems	specific drivers	specific objectives
Problem I: lack of effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals	➢ criminals increasingly abuse cross-border services of private parties, who hold ever more personal data relevant for criminal investigations ➢ private parties do not have a central point of contact in case of unclear/multiple jurisdiction ➢ national authorities cannot effectively analyse multi-jurisdictional or non-attributable data sets through national or intergovernmental cooperation ➢ national law enforcement authorities face difficulties in transmitting requests containing personal data to private parties outside their jurisdiction • restrictions in the Europol Regulation: Europol cannot: effectively exchange personal data with private parties or serve as a channel to transmit Member States' requests to private parties.	***Objective I***: enabling effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals
Problem II: big data challenge for law enforcement authorities	➢ criminals and terrorist use information and communications technology ➢ analysis of large and complex datasets requires specific data processing ➢ restrictions in the Europol Regulation: lack of legal clarity and no consideration of the processing requirements of large and complex datasets	***Objective II***: enabling law enforcement to analyse large and complex datasets to detect cross-border links
Problem III: gaps on innovation and research relevant for law enforcement	➢ criminals quickly adapt to use new technologies to their criminals ends ➢ not all Member States are well equipped to exploit fully the advantages of new technologies for law enforcement ➢ restrictions in the Europol Regulation: no explicit role on innovation and research and no legal ground for data processing for innovation	***Objective III***: enabling Member States to use new technologies for law enforcement

Table 1: Link between problems, drivers and objectives

2. PROBLEM DEFINITION

This impact assessment addresses **three problems** that all bear on evolving security threats, and the consequential changes they bring about in Member States' operational needs to effectively address these threats. They all relate to the fact that criminals exploit the opportunities offered by the digital transformation and new technologies. All three issues constitute **major problems**, due to their impact on security, and as reflected by strong calls by the co-legislators for action. All three aspects raise **important policy choices** that require a detailed assessment of the problem drivers, the related objectives, available policy options and their impact. Therefore, this impact assessment **addresses these three core issues separately**:

1) lack of effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals;
2) big data challenge for law enforcement authorities;
3) gaps in innovation and research relevant for law enforcement.

All three problems have emerged since the adoption of the Europol Regulation in 2016.

The inception impact assessment[66] preceding this impact assessment identified a number of additional problems and objectives. When preparing this impact assessment, it became clear that several of these aspects do not raise important policy choices. They therefore do not need to be addressed in this impact assessment.

This includes aspects related the **clarification of already existing tasks of Europol**.[67]

This also includes aspects of **legal clarification,**[68] such as the clarification that Europol can act **as service provider** for crime-related bilateral exchanges between Member States using Europol's infrastructure.[69] In these cases, Europol does not have access to the personal data exchanged between Member States through Europol's infrastructure and cannot ensure compliance with the requirement related to the specific categories of data subjects in annex II of the Europol Regulation.[70] Such a clarification would address part of the issues raised by the European Data Protection Supervisor in the December 2019 Decision relating to the technical administration of FIU.net.[71]

---

66 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12387-Strengthening-of-Europol-s-mandate.

67 For example with regard to the coordination of investigations in so-called "high-value targets", Europol's role in Schengen evaluations, the threat assessment analysis that Europol provides to support the Commission and the Member States in carrying out risk assessment, or Europol staff actively assisting on the ground in the territory of the Member States.

68 For example with regard to the involvement of national analysts in processing at Europol, the use of Europol information in national court proceedings, or Europol staff giving evidence before a national court in judicial proceedings.

69 According to Article 8(4) of Regulation (EU) 2016/794, Member States may use Europol's infrastructure for exchanges also covering crimes falling outside the scope of the objectives of Europol. In these cases, Europol acts as data processor rather than as data controller.

70 For more details, see annex 4 on Past performance of Regulation (EU) 2016/794.

71 FIU.net is a decentralised and sophisticated computer network supporting the Financial Intelligence Units (FIUs) in the EU in their fight against money laundering and the financing of terrorism. In the related Decision, the EDPS concluded that the technical administration of FIU.net by Europol was in breach of the Europol Regulation (see the EDPS Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing (23.7.2020)). However, the legal clarification would not address the main aspect of the EDPS Decision, namely the fact that Europol cannot process administrative data that is not related to

There are **three additional aspects** that are considered politically relevant as they respond to calls by the co-legislators for a reinforced role of Europol, even though they raise less of a policy choice notably due to legal constraints related to all three aspects:

1) **Europol's ability to provide frontline officers (police officers and border guards) with the result of the analysis of third-countries sourced information on suspects and criminals**, where it is legally questionable whether it would be possible for Europol to issue 'discreet check' alerts in the Schengen Information System, as such alerts require a coercive measure by national authorities in case of a 'hit'. Issuing such alerts is therefore a prerogative of national authorities. At the same time, the information that third countries share with the EU about criminals and terrorists is increasingly relevant for EU internal security. As the EU criminal information hub, Europol holds valuable information it received from third countries on suspects and criminals, and it makes this information available to Member States through the Europol Information System.[72] In November 2018, the co-legislators already took the policy choice to give Europol access to alerts in the Schengen Information System.[73] Moreover, in September 2018, the co-legislators took the policy choice to enable Europol to enter third-country sourced information into the watchlist of the European Travel Information and Authorisation System (ETIAS) for third-country nationals exempt from the requirement to be in possession of a visa when crossing the EU external borders.[74] The watchlist will support Member States in assessing whether a person applying for a travel authorisation poses a security risk. Building on these policy choices taken by the co-legislators, annex 6 assesses the **policy option of introducing a new alert category in the Schengen Information System exclusively for Europol**, reflecting Europol's role and competences, as well as the necessary safeguards.

2) **Europol's cooperation with third countries**, where the requirement of essential equivalence as set by the Court of Justice of the EU in its case law[75] applies to any structural transfer of personal data to third countries. The Europol Regulation already provides for all legal grounds foreseen under EU law for the transfer of personal data to third countries.[76] The requirement of essential equivalence will apply to any such transfer, irrespective of any changes to the related provisions in the Europol Regulation.[77]

3) **Europol's capacity to request the initiation of criminal investigations**, where the material scope of the related provision in the Europol Regulation[78] is determined by the Article 88(1) TFEU, which leaves no scope to extend that material scope beyond

---

any crime.

72 In 2019, Europol accepted almost 12 000 operational contributions from third countries. In 2019, there were over 700 000 objects recorded in the Europol Information System that stem from Europol's analysis of data it received from third countries.

73 Regulation (EU) 2018/1862.

74 Regulation (EU) 2018/1240.

75 Opinion 1/15, *EU-Canada PNR Agreement*, EU:C:2017:592 (26.7.2017); judgment of 6 October 2015, *Schrems*, C- 362/14, EU:C:2015:650; judgement of 16 July 2020, C- 311/18, *Schrems II*, EU:C:2020:559.

76 Regulation (EU) 2016/794 sets outs three ways to establish a structural cooperation with a third countries that would provide legal grounds based on which Europol could lawfully transfer personal data to authorities of that third countries: (1) a Commission adequacy decision adopted in accordance with Article 36 of Directive (EU) 2016/680; (2) an international agreement concluded by the Union pursuant to Article 218 TFEU; (3) an authorisation by the Europol Management Board, in agreement with the EDPS, based on a self-assessment that adequate safeguards for the protection of privacy and fundamental rights exist.

77 Europol can receive personal data from third countries, but cannot always share personal data with third countries in an effective manner (see problem definition in Annex 7).

78 Article 6 of Regulation (EU) 2016/794.

Europol's ability to request the initiation of investigations with regard to serious crimes affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.

These three aspects do not involve real policy choices. However, given the relevance of these three issues as reflected in calls by the co-legislators, and for reasons of completeness, all three aspects are thoroughly analysed in separate annexes to this impact assessment.[79]

Finally, two important aspects deserve mentioning. First, in terms of ensuring the **highest level of data protection** at Europol, there is strong support among stakeholders for making the Regulation[80] on the processing of personal data by EU institutions, bodies, offices and agencies directly applicable to Europol's data protection regime, complemented with more specific safeguards on data protection in the Europol Regulation where needed. This would further strengthen Europol's data protection regime and streamline the rules on supervision. This alignment will be based on a comparison between Chapter IX of Regulation (EU) 2018/1725 and the data protection provisions in the Europol Regulation, with the aim to assess in detail which provisions of Chapter IX can become directly applicable to the data processing by Europol and which ones should be included in the Europol Regulation. This aspect will not be further addressed in the impact assessment. Instead, it is assumed that this alignment would be part of the legislative initiative to strengthen Europol's legal mandate, **ensuring that Europol's legal regime continues to provide for the highest level of data protection**.[81]

Second, the **European Public Prosecutor's Office** (EPPO)[82] is mandated to launch investigations on crimes against the EU budget. While the EPPO Regulation anticipates Europol's support and cooperation[83], the current Europol Regulation does not explicitly reflect these obligations. The investigations and prosecutions by the EPPO – once operational – will require information and support from Europol. This will close information gaps that could otherwise hamper the ability of the EPPO to initiate and conduct criminal investigations for crimes falling under its jurisdiction. There is a need to align the mandate of Europol with the mandate of the EPPO.[84] This could be done by way of setting out, in the Europol Regulation, all obligations on Europol that flow from the

79 See annex 6, annex 7 and annex 8.

80 Regulation (EU) 2018/1725.

81 Article 98 of Regulation (EU) 2018/1725 foresees a review of Union legal acts by April 2022. Based on that review, the Commission may submit a legislative proposal to apply the Regulation to Europol. Aligning Europol's data protection regime with EU data protection law as part of the review of the Europol Regulation would anticipate the alignment foreseen by Regulation (EU) 2018/1725.

82 The EPPO was established by Council Regulation (EU) 2017/1939 (12.10.2017).

83 Article 24(1) of Council Regulation (EU) 2017/1939 (12.10.2017) provides that the agencies of the Union shall without undue delay report to the EPPO any criminal conduct in respect of which it could exercise its competence. Article 43(2) provides that the EPPO shall be able to obtain any relevant information falling within its competence that is stored in databases and registers of the agencies of the Union. Article 102 provides for the possibility of the EPPO to obtain, where necessary for the purpose of its investigations and at its request, any relevant information held by Europol, concerning any offence within its competence, and to ask Europol to provide analytical support to a specific investigation conducted by the EPPO.

84 The consultation showed that Member States support regulating the relationship between Europol and the EPPO. Member States called for amending Europol Regulation as far as necessary to mirror the EPPO legal basis, avoiding an imbalance between the two Regulations. At the same time, they stressed the importance of keeping Europol core principles applicable (i.e. *data ownership principle*). In the same line, 57, 5% of the responses on the targeted consultation by way of questionnaire (see annex 10) indicate that Europol's cooperation with the EPPO should be regulated in more detail, in order for the two organisations to work well together in the future.

EPPO Regulation, taking account of the specific processing requirements and conditions in the Europol Regulation. This would include Europol's obligation to: a) report relevant suspected cases to the EPPO; b) actively support[85] the investigations and prosecutions of the EPPO; and c) provide any relevant information requested by the EPPO.

This would foster the overall cooperation between the EPPO, Europol, Eurojust and OLAF, as far as the Europol Regulation is concerned, seeking to strengthen their cooperation in line with their respective mandates and competences.[86] It would therefore respond to the call in the July 2020 European Parliament Resolution[87] urging *"the EU agencies, in particular Europol, Eurojust and OLAF, to cooperate ever more closely with national authorities in order to detect fraud more effectively."* It would also be in line with the July 2020 Security Union Strategy[88] recognising that in the context of a strong European security ecosystem *"EU relevant authorities at EU level (such as OLAF, Europol, Eurojust and the European Public Prosecutor's Office) should also cooperate more closely and improve the exchange of information."*

In addition, the replies in targeted consultation by way of questionnaire (see Annex 11) very much supported regulating the relationship with the EPPO. Member States were also supportive to regulating the role of Europol in supporting the EPPO, as resulted from the Workshop on the revision of the Europol Regulation (see Annex 2). Furthermore, during the technical workshop on Europol and the EPPO, the participants provided overall positive feedback on aligning Europol's mandate with the EPPO, and clarifying and detailing their cooperation. Discussions on technical aspects of such an intervention focused on the 'double reporting' issue (Europol and Member States are both obliged to report cases of crimes against the EU budget, so-called 'PIF crimes', to the EPPO), the handling of information provided by Europol ('data ownership principle'), the possibility of an indirect access by the EPPO to Europol's information on the basis of a hit/no hit system (similarly to Eurojust and European Anti-Fraud Office OLAF), and the administrative and logistical costs to Europol, which would derive from the enhancement of the Agency's cooperation with the EPPO.

2.1 Lack of effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals

2.1.1 What is the problem?

Criminals increasingly abuse the cross-border services of private parties to carry out

---

85 Europol launched on 5 June 2020 the new European Financial and Economic Crime Centre (EFECC), which will enhance the operational support provided to the EU Member States and EU bodies in the fields of financial and economic crime and promote the systematic use of financial investigations.

86 There is also scope to strengthen Europol's cooperation with OLAF to detect fraud, corruption and any other illegal activity affecting the financial interests of the Union, in line with the rules on the transmission of personal data to Union bodies that are applicable to Europol under Regulation (EU) 2016/794. This would not affect the existing provisions in the Europol Regulation on cooperation with Eurojust, notably the provision on access by Eurojust to information stored by Europol (Article 21 of Regulation (EU) 2016/794). It would also not affect the cooperation between Europol and customs authorities, nor the cooperation between Europol and tax administrations through Eurofisc.

87 European Parliament resolution of 10 July 2020 on protection of the European Union's financial interests - combating fraud - annual report 2018 (2019/2128(INI)). https://www.europarl.europa.eu/doceo/document/TA-9-2020-0192_EN.html

88 COM(2020) 605 final (24.7.2020)

illegal activities. This includes internet-based services, but also financial services, as well as classical telecom services. In their 2019 Council Conclusions, the Member States have recognised "*the ever faster developments of modern technologies, and the ensuing increase in serious criminal offences committed online, in the dark web or with the help of those technologies*".[89] For example, sex offenders abuse children and share pictures and videos world-wide using platforms on both the surface web and the dark web.[90] Terrorists use the internet to recruit new volunteers and to teach them how to plan and carry out attacks.[91] Cyber criminals profit from the digitalisation of our societies using phishing and social engineering to commit other types of cybercrime such as online scams, ransomware attacks or payment fraud.[92]

As a result, private parties hold increasing amounts of personal data relevant for criminal investigations.[93] The internet has created a public space that is in private hands, making it difficult for law enforcement to perform their tasks of enforcing rules that apply online as they do offline. Member States have acknowledged this in their 2019 Council Conclusions, which note that "*private parties play a growing role in preventing and countering cyber-enabled crimes as they are often in possession of significant amounts of personal data relevant for law enforcement operations…"*.[94] As a result of the borderless nature of the internet, and the possibilities for operating anonymously therein, these data sets are often non-attributable (i.e. the relevant jurisdiction is unclear) or multi-jurisdictional (i.e. the data sets contain information relevant to many jurisdictions). Indeed, private parties may hold significant amounts of personal data on criminal activities, where victims, perpetrators, the digital infrastructure in which the personal data is stored, and the service provider running the infrastructure are all under different national legal frameworks, within the EU and beyond.

National authorities cannot effectively analyse multi-jurisdictional or non-attributable data sets through national solutions. If national law enforcement authorities obtain large data sets not targeted to their jurisdiction, it is very time consuming and resource intensive to sift through the data in order to identify the data relevant for the respective jurisdiction. By way of example, the US National Centre for Missing and Exploited Children (NCMEC) shared over 300 000 referrals of Child Sexual Abuse Material in 2019. There will be many cases where at least some law enforcement authorities lack the necessary resources to sift through such large amounts of data. Alternatively, if the national law enforcement authorities obtain smaller data sets targeted to their respective jurisdiction, they risk missing the holistic intelligence picture. By way of example, if criminals attack ATMs across Europe, but the law enforcement authorities only obtain data sets on attacks under their jurisdiction, they can miss out on important intelligence such as travelling patterns, or modus operandi.[95]

---

89 Council Conclusions on Europol's cooperation with Private Parties, Document 14745/19, 2 December 2019.

90 Europol Report, Exploiting Isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic, 19 June 2020.

91 Europol Press Release, Terrorist 'how-to' guides - focus of latest Europol Referral Action Day, 3 July 2020.

92 Europol Press Release, COVID-19 sparks upward trend in cybercrime, 5 October 2020.

93 77. 46 % of the responses on the targeted consultation by way of questionnaire (see annex 11) indicated that the role of private parties in preventing and countering cyber-enabled crimes is growing, as they are often in possession of significant amounts of personal data relevant for law enforcement operations.

94 Council Conclusions on Europol's cooperation with Private Parties, Document 14745/19, 2 December 2019; Stakeholders have also confirmed this assessment in the online survey.

95 Europol, Preventing Physical ATM Attacks, 2019.

Furthermore, Member States cannot effectively address these problems by way of intergovernmental cooperation. In theory, this could be achieved by contractual agreements by which the Member States, in which the private parties are established or have a legal representative, receive the personal data from the private parties under their jurisdiction and share it in a targeted manner with the Member States concerned or in an untargeted manner with all other 26 Member States. However, from a practical point of view, this could involve disproportionate resource implications for the Member States in which the private party is established. Those Member States might be unable or unwilling to invest in the resources necessary to analyse and dispatch data to 26 Member States, in particular if there are no indications that the criminal activity falls under their jurisdiction. In addition, national law enforcement authorities will face legal difficulties in sharing personal data in situations, where the criminal activity has no link to the jurisdiction of the Member State other than the fact that the private party holding the data is established under its jurisdiction.

Moreover, it is very time consuming and challenging for national law enforcement authorities to exchange information with private parties, in particular if the private parties are established in a different jurisdiction inside or outside the EU. Similarly private parties also face difficulties when receiving multiple requests from law enforcement authorities of other countries. This does not only lead to a significant administrative burden, but also poses problems in verifying whether the requesting authority is a legitimate law enforcement agency.[96] This creates liability risks for private parties, and the resulting procedures can lead to significant administrative burdens and long delays for law enforcement. This problem has been raised in relation to law enforcement's access to internet domain name registration data collected and stored by domain name registries and registrars (ICANN's WHOIS data base).[97] Private parties and law enforcement authorities may face similar problems when cooperating on removal orders and referrals under the proposed Regulation on preventing the dissemination of terrorist content online (hereafter: TCO Regulation).[98]

Therefore, Member States need an EU-level solution to address these challenges. Europol could play an increasingly important role in that regard. The Agency was set up to provide services which help Member States overcome the limitations of their national 'toolboxes', in particular by helping them to access relevant personal data held by other Member States. According to Article 88 (2) (a) TFEU, one of Europol's core tasks is the collection, storage, processing, analysis and exchange of information. The Agency already hosts the relevant data bases, against which information from private parties would have to be checked and analysed.

However, the Agency is very limited in the way it can support Member States when it comes to cooperating with private parties. Europol can receive personal data from private parties only via competent intermediaries (Member States' National Units, contact points of third countries or international organisations with which Europol can exchange personal data). In cases in which private parties proactively share personal data directly with Europol, the agency may process this data only to identify the responsible national

---

96 On private parties' ability to verify the authenticity of requests from competent authority, see also p. 6 of the of the Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (13.2.2019).

97 Letter from the EDPS to Europol dated 7 September 2018, Europol's consultation on law enforcement access to WHOIS database (https://edps.europa.eu/sites/edp/files/publication/18-09-07_letter_drewer_en.pdf).

98 Proposal for a Regulation on preventing the dissemination of terrorist content online, COM(2018) 640 final.

unit, transfer it to that national unit and then delete it. The national unit may then decide to resubmit the data. If Europol cannot identify the responsible national unit within four months, it will delete the data in question even if it is clearly relevant to its tasks.[99] Europol is prohibited from contacting private parties with requests for personal data.

The results of the consultation confirmed that the digitalisation of our societies has resulted in an increase in serious criminal offences committed online, on the dark web or with the help of such information technologies (cyber-enabled crimes). A large majority of participants agreed that the role of private parties in preventing and countering cyber-enabled crimes is growing as they are often in possession of significant amounts of personal data relevant for law enforcement operations.[100] The results of the consultation suggest that most participants agree that Europol would be best placed to provide the necessary services to Member States to improve cooperation with private parties. Many participants in the online survey noted that the current restrictions in Europol's mandate limit the effectiveness with which Europol can fulfil its task as the EU criminal information hub,[101] and that the lack of effective cooperation with private parties can:

- increase the risks of **delays** (e.g. where the identification of the Member State concerned is difficult and time-consuming),[102]
- increase the risk of **loss of information** (e.g. where Europol does not have enough information to identify the Member State concerned),[103]
- lead to a lack of **legal certainty** for private parties, when they submit personal data to Europol.[104]

The problems were also confirmed by a study into the current practice of direct and indirect exchanges of personal data between Europol and private parties.[105]

The study suggests that many stakeholders consider that the current legal framework

---

99 There are only three exceptions which allow Europol to transfer personal data directly to private parties, namely (i) if the transfer is undoubtedly in the interest of the data subject; (ii) if the transfer is absolutely necessary in the interest of preventing the imminent perpetration of a crime; or (iii) if the transfer concerns publicly available data and is strictly necessary for preventing and combatting internet-facilitated crimes (so-called referrals). Following such referrals of publicly available data, Europol may in connection therewith also receive personal data from private parties, if that private party declares it is legally allowed to transmit this data in accordance with the applicable law.

100 77. 46 % of the responses on the targeted consultation by way of questionnaire (see annex 11) indicated that the role of private parties in preventing and countering cyber-enabled crimes is growing, as they are often in possession of significant amounts of personal data relevant for law enforcement operations.

101 64.79 % of the participants of the targeted consultation by way of questionnaire (see annex 11) consider that the current restrictions on Europol's ability to exchange personal data with private parties limits Europol's capacity to effectively support Member States' investigations.

102 50.7 % of the participants of the targeted consultation by way of questionnaire (see annex 11) consider that the current restrictions on Europol's ability to exchange personal data with private parties result in a risk of delays (e.g. where the identification of the Member State concerned is difficult and time-consuming).

103 54.93 % of the participants of the targeted consultation by way of questionnaire (see annex 11) consider that the current restrictions on Europol's ability to exchange personal data with private parties result in a risk of loss of information (e.g. where Europol does not have enough information to identify the Member States concerned).

104 40.85 % of the participants of the targeted consultation by way of questionnaire (see annex 11) consider that the current restrictions on Europol's ability to exchange personal data with private parties result in a lack of legal certainty for private parties, when they submit data to Europol).

105 Milieu, 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 (not yet published) (see annex 4 for main findings).

limits Europol's ability to support Member States in effectively countering crimes prepared or committed with the help of cross-border services offered by private parties. While the system of referrals is functioning well, the current system of proactive sharing, as regulated by the European Regulation, is not suitable to address these operational needs. Therefore, many stakeholders would see benefits in enabling Europol to exchange personal data directly with private parties, outside the context of referrals.

In addition, a number of stakeholders have recommended the channeling of the requests and the responses through a dedicated platform, and many stakeholders suggested Europol in that regard. However, some others were doubtful about the intermediary role Europol might play between the private parties and the law enforcement agencies. As an alternative solution to the issue, some stakeholders recommended the establishment of platforms for the exchanges of good practices between the law enforcement agencies. The Home Affairs Ministers of the European Union reiterated in their October 2020 Declaration 'Ten points on the Future of Europol' the increasingly important role of private parties in fighting online and offline crime *"…because they possess information without which effective law enforcement is often impossible. This is especially true of online-service providers in the case of investigations into child sexual exploitation material, terrorism, financial or organised crime"*.[106]

2.1.2 What are the problem drivers?

In today's globalised societies, criminals move their goods, provide their 'services' and transfer their proceeds with ease between countries, regions and continents. In addition to new criminal opportunities, the digital transformation provides them with easy access to secure communication tools (such as EncroChat),[107] safe market places (such as the dark web),[108] and financial 'services' (such as money laundering).[109] Indeed, criminals increasingly abuse cross-border services of private parties to carry out illegal activities, and – as a consequence - private parties hold increasing amounts of personal data relevant for criminal investigations in several jurisdictions, which might be unrelated to the jurisdiction under which they are established. However, there is currently no effective cooperation between private parties and law enforcement authorities on the exchange of such data.

There are four problem drivers for the lack of effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals.

The *first problem driver* relates to the fact that **private parties do not have a contact point when they want to share multi-jurisdictional or non-attributable data sets with law enforcement**. Private parties will find it often difficult or even impossible to identify the jurisdictions, which would be in a position to investigate criminal activities on which they hold information.

The *second problem driver* relates to the fact that **national authorities cannot**

106 Declaration of the Home Affairs Ministers of the European Union, Ten points on the future of Europol, Berlin, 21 October 2020, (https://www.eu2020.de/blob/2408882/6dd454a9c78a5e600f065ac3a6f03d2e/10-22-pdf-virtbrotzeit-europol-en-data.pdf).

107 https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

108 https://www.europol.europa.eu/newsroom/news/international-sting-against-dark-web-vendors-leads-to-179-arrests.

109 https://www.europol.europa.eu/newsroom/news/20-arrests-in-qqaazz-multi-million-money-laundering-case.

effectively analyse multi-jurisdictional or non-attributable data sets through national or intergovernmental solutions, because it is very time consuming and resource intensive to sift through the data in order to identify the data relevant for the respective jurisdictions. Moreover, Member States of establishment will often not be in a position to analyse the data if there is no indication that the criminal activities are falling under their jurisdictions.

The *third problem driver* relates to the fact that it is **very time consuming and challenging for national law enforcement authorities to effectively exchange data with private parties**, in particular if the private parties are established in different jurisdictions inside or outside the EU. Similarly private parties face difficulties when receiving multiple requests from law enforcement authorities of other countries.

There is currently no EU-level solution that would provide Member States and private parties with an effective way to cooperate with each other in countering crimes prepared or committed by criminals abusing cross-border services offered by private parties. The *fourth problem driver* relates to **restrictions in the Europol Regulation**. The Agency is not able to support Member States in cooperating effectively with private parties:

1) Europol cannot be a **central point of contact for private parties**, which have identified criminal intelligence, but have troubles identifying the relevant jurisdictions concerned (hereafter also referred to as cases of **'non-attributable data sets'**). By way of example, the US National Center for Missing and Exploited Children (NCMEC) cannot share information related to child sexual abuse directly with Europol, which can therefore not analyse such data with a view to identifying the respective contact points or authorities concerned (here-after referred to as 'Member State concerned'[110]).
2) Europol cannot be a **central point of contact for private parties**, which have identified criminal intelligence relevant for multiple jurisdictions (hereafter also referred to '**multi-jurisdictional data sets'**) and which would like to share this intelligence with a single point of contact in order to provide a holistic picture of the criminal intelligence.
3) Europol cannot exchange information with a private party as a **follow-up** to that private party having shared personal data with the Agency in the first place, in order to notify that private party about the information missing for the Agency to establish the jurisdiction of the Member States concerned. For example, if an online service provider shares a video depicting child sexual abuse with Europol, but the data shared is insufficient for the Agency to identify the Member State concerned, the Agency cannot inform the online service provider of the missing information to enable it to decide whether to share additional information with the Agency that would enable it to identify the Member State concerned. This can lead to delays in identifying and transmitting the personal data to the Member State concerned.[111] This can also lead to the loss of data,[112] for example where

---

110 Under the current Europol Regulation (Article 26(1) Europol Regulation), Europol may process personal data only on the condition that they are received via national units of Member States, or by contact points and authorities of third countries and international organisations. In order to improve readability, this impact assessment will refer only to 'Member States concerned' as this is the most pertinent case in practice.

111 50.7 % of the participants of the targeted consultation by way of questionnaire (see annex 11) consider that the current restrictions on Europol's ability to exchange personal data with private parties result in a risk of delays (e.g. where the identification of the Member State concerned is difficult and time-consuming).

112 54.93% of the participants of the targeted consultation by way of questionnaire (see annex 11) consider that the current restrictions on Europol's ability to exchange personal data with private

Europol cannot identify the Member State concerned, or where the Member State decides not to resubmit the personal data to Europol, notably because there is no ground for opening an investigation under its jurisdiction, even though the personal data might be relevant for other Member States.

4) Europol cannot **proactively reach out to private parties** with a request for personal data, which would enable the Agency to enrich existing data and provide better analysis to Member States[113]. By way of example, Europol is not allowed to ask an online service provider for the registration data of an email-account, which is linked to criminal activities.[114]
5) Europol cannot be a **service provider** for Member States' law enforcement authorities sending requests containing personal data to private parties.[115] For example, Europol cannot act as an intermediary for requests from national police to internet domain name registries or registrars for access to domain name registration data, such as may be facilitated by the Internet Cooperation for Assigned Names and Numbers (ICANN).

Member States acknowledged these shortcomings in their 2019 Council Conclusions, noting that "…*the current legislative framework, especially Articles 17 and 26 of Regulation (EU) 2016/794, restrict the ability of Europol to process data obtained from private parties on the substance, insofar as they require the prior submission of the data by other channels, which can cause considerable delays and ultimately render such data obsolete or no longer relevant for investigation or analysis*." They further acknowledge that "*the current legislative framework may also cause a complete loss of relevant information, for instance where a Member State considers data obtained from a private party as irrelevant and therefore neither opens its own investigation nor establishes a ground for submission of that data to Europol, whereas Europol might have been able to establish, in accordance with its mandate, a link to one or more Member States if the data had been transmitted to it directly by the private party*."[116]

2.1.3 How will the problem evolve without intervention?

Without any intervention, the support that Member States could seek from Europol to facilitate the cooperation with private parties, notably to analyse non-attributable or multi-jurisdictional data sets with a view to identifying the Member States concerned, might be affected. As indicated in section 2.1 above, the current system entails risks of delays and loss of information for the Member States concerned in addition to legal uncertainty for the private parties holding relevant data.

In the future, the **need for EU-level solutions to support Member States in countering crimes prepared or committed using cross-border services by private parties will**

---

parties result in a risk of loss of information (e.g. where Europol does not have enough information to identify the Member States concerned).

113 50.7 % of the participants of the targeted consultation by way of questionnaire (see annex 11) consider that in order to fulfil its role as an information hub, Europol should be able to request and obtain data directly from private parties.

114 While Europol could notify the Member States of the need to obtain additional information from private parties, Member States could not request such the information from private parties unless they have an ongoing investigation or reasons to open a new investigation under their applicable national laws.

115 50.7 % of the participants of the targeted consultation by way of questionnaire (see annex 11) see merits in enabling Europol to request and receive personal data directly from private parties on behalf of Member States' law enforcement in order to facilitate exchanges of personal data between Member States' law enforcement and private parties.

116 Council Conclusions on Europol's cooperation with Private Parties (2 December 2019).

increase further. Digital services are likely to hold increasing amounts of personal data relevant for criminal investigations. Each new generation is more versed and used to operating in the digital space. State actors support the digitisation of our societies by digitising administrative procedures and by improving the necessary infrastructure (e.g. with regard to fiber optic cables, and 5G).[117] Private actors equally move to the digital space, to follow demand, to become more cost efficient, and to search for new business opportunities. Events such as the global COVID-19 pandemic accelerate these developments.[118] As a result, criminals are likely to continue to increase their abuse of private parties' cross-border services to facilitate and commit crimes. National law enforcement authorities are likely to find it increasingly difficult to identify cases and information with relevance for their respective jurisdiction, in particular where the cases rely on the analysis of multi-jurisdictional data sets, or data sets where the jurisdiction of the data subjects is difficult to establish. Likewise, private parties will increasingly face difficulties when seeking to report criminals using or abusing their services to the responsible law enforcement authorities.

2.2 Big data challenge for law enforcement authorities

2.2.1 What is the problem?

Data collected in criminal investigations are increasing in size and becoming semantically more complex. Member States' law enforcement authorities collect large datasets in criminal investigations on serious organised crime, terrorism and cyber-crime. Any seizure in an average investigation on organised crime or terrorism can nowadays easily involve terabytes of data, including audio, video and machine-generated data that is increasingly difficult to process manually. For example, in the joint investigation to dismantle *EncroChat,* an encrypted phone network used by criminal networks involved in violent attacks, corruption, attempted murders and large-scale drug transports, investigators had to analyse millions of messages that were exchanged between criminals to plan serious crimes.[119] Law enforcement authorities thus **need to process large and complex datasets** in the context of criminal investigations, which leads to challenges in terms of the necessary IT tools to analyse the data, the facilities to store the large datasets, the expertise and techniques necessary to process the complex datasets, and the related human and financial resources.

Where the crimes and related criminal investigations have a cross-border element, **Member States submit large and complex datasets to Europol**, with the request for operational analysis to detect links to other crimes and criminals in other Member States. Member States cannot detect such cross-border links through their own analysis of the large datasets at national level, as they lack the corresponding data on other crimes and criminals in other Member States. Detecting such cross-border links by way of intergovernmental cooperation would require transmitting the entire dataset to each and every Member State, which is not effective. It would also be ineffective if Member States would limit their contributions to Europol to the result of their own analysis of large and complex datasets. Limiting the data they sent to Europol to pre-analysed and filtered data would risk missing important cross-border links with data held by Europol. Notably at an

117 See for example Europol Report "Do Criminals dream of electric sheep? How technology shapes the future of crime and law enforcement, 18.7.2019.

118 For example, the COVID-19 crisis has resulted in a surge in online distribution of child sexual abuse material (see Europol Report, Exploiting Isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic, 19.6.2020).

119 https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

early stage of an investigation, it is often not possible to establish from the outset if a person is involved or not in the crime under investigation. The purpose of Europol's analysis it to support Member States in identifying persons who are involved in the crime under investigation. For example, Europol received high volumes of data in the context of the Task Force *Fraternité*, set up to support French and Belgian authorities in the investigation of the November 2015 Paris attacks and the March 2016 Brussels attacks.[120]

Moreover, **some Member States might not always have the necessary IT tools, expertise and resources** to analyse large and complex datasets, and therefore turn to Europol for support. One of the very purposes of setting up the European Cybercrime Centre (EC3) and the European Counter Terrorism Centre (ECTC) was to pool the expertise and capabilities necessary for data analysis in complex investigations into cybercrime and terrorism, in order to exploit synergies and economies of scale. While Europol's operational support activities have always included the processing of data to provide operational analysis products, this role expanded considerably with the setting up of the EC3 and the ECTC.[121] As set out by the EDPS, **Europol started receiving large and unfiltered datasets from Member States over the past years**. The processing of these datasets has become an important part of Europol's work to support Member States' law enforcement authorities.[122] The personal data processing activities at stake in the EDPS decision on Europol's big data challenge are linked to the evaluation of the datasets that Member States submit to Europol.[123]

However, **Europol faces a considerable challenge when it comes to the processing of large and complex datasets**. In its decision of 18 September 2020, on the own initiative inquiry on Europol's big data challenge, the EDPS concluded that **the processing of large datasets by Europol does not comply with the data protection safeguards in the Europol Regulation**.[124] Triggered by information provided by the Europol Executive Director in April 2019, the EDPS opened its own initiative inquiry that month on the use of Big Data Analytics by Europol. This inquiry "*showed that it is not possible for Europol, from the outset, when receiving large data sets to ascertain that all the information contained in these large datasets comply with these limitations. The volume of information is so big that its content is often unknown until the moment when the analyst extracts relevant entities for their input into the relevant database.*"[125] As set out

---

120 The aim was to investigate further the international connections of the terrorists by analysing communication, financial, internet and forensic records. Task Force *Fraternité* analysed 19 terabytes of information. Europol's processing of large and complex data resulted in 799 intelligence leads.

121 EC3 has two forensics teams, digital forensics and document forensics that offer advanced digital forensics tools and platforms to investigations and operations in Member States. In 2019, the EC3 provided operational support to 397 cases and delivered 1,084 operational reports. In the area of counter-terrorism, the volume and complexity of the datasets submitted by Member States to the ECTC for operational analysis increased considerably, with complex datasets of multiple terabytes per investigation becoming the standard procedure. The ECTC supported 632 operations in 2019 and issued close to 1,900 operational products (Europol: 2019 Consolidated Annual Activity Report).

122 See the letter from the EDPS to the Co-Chairs of the Europol Joint Parliamentary Scrutiny Group (23.9.2020): https://edps.europa.eu/sites/edp/files/publication/20-09-28_letter_jpsg_en.pdf.

123 Point 5.3 of the EDPS Decision on the own initiative inquiry on Europol's big data challenge.

124 See the EDPS Decision on the own initiative inquiry on Europol's big data challenge: https://edps.europa.eu/sites/edp/files/publication/20-09-18_edps_decision_on_the_own_initiative_inquiry_on_europols_big_data_challenge_en.pdf. The EDPS issued an admonishment pursuant to Article 43(3)(d) of the Europol Regulation to signal data processing activities that are not in line with the applicable data protection framework and to urge Europol to adjust its practices. The EDPS invited Europol to provide an action plan to address the admonishment within two months, and to inform of the measures taken within six months following the issuing of the decision.

125 Point 4.8 of the EDPS Decision on the own initiative inquiry on Europol's big data challenge.

in section 1.3 above, Europol is only allowed to process personal data about certain categories of individuals, namely suspects, convicted criminals, potential future criminals, contacts and associates, victims, witnesses and informants. The EDPS inquiry therefore concluded that "*there is a high likelihood that Europol continually processes personal data on individuals for whom it is not allowed to do so*".[126]

The **structural legal concerns** identified by the EDPS raise a **serious challenge for Europol to fulfil its tasks**, as the processing of large and complex datasets relates to the essence of Europol's working methods and analytical support capabilities, and therefore to core tasks of Europol under the Treaty and under its legal mandate. The issue hence concerns an essential aspect of the support that Member States expect from the agency.[127]

As the analysis of large and complex datasets includes the processing of personal data, including the potential processing of data of persons not related to a crime, the assessment of policy options to address the identified problem needs to take **full account of Fundamental Rights and notably the right to the protection of personal data**.

2.2.2 What are the problem drivers?

There are three problem drivers for the big data challenge for law enforcement. As a *first problem driver*, in today's digital world, the processing of large and complex datasets is inevitable for law enforcement. **Criminals and terrorist use information and communications technology** to communicate among themselves and to prepare and conduct their criminal activity. As more digital content is generated by criminals and terrorists, law enforcement authorities may need to process more data in the context of a criminal investigation in order to detect necessary information. A basic law enforcement procedure in the framework of any criminal investigation nowadays is the seizure of technical equipment that may host necessary information for the investigation during an arrest or house search. As part of the standard operational procedure, law enforcement authorities seize the mobile phones and other **communication devices** used by suspects. The devices may contain data on individuals not related to the criminal investigation, but separating the relevant information from the non-relevant information for the investigation is not possible at the moment of seizing the technical equipment. Likewise, when criminals and terrorists use **physical servers** to store the infrastructure they use for their criminal activities, law enforcement authorities need to seize the entire physical server. It is impossible at the moment of the seizure to determine what data in the physical server is related to the criminal activity and what is not. Criminals and terrorists also communicate through **communication platforms**. The level of criminality in a specific platform may be such that the judicial authorities request the takedown and seizure of the whole communication platform, even if not all users in the platform are involved in criminal activity. A communication platform can contain thousands of users and millions of messages. Separating the users involved in criminal activities from those without criminal implications requires the evaluation of all entities included in the communication platform in a pre-analysis phase.

A *second problem driver* relates to the **nature of large and complex datasets**, and the specific processing operations their analysis requires. To identify data that is necessary for a criminal investigation, law enforcement authorities need to use **digital forensics**[128]

---

126 Point 4.9 of the EDPS Decision on the own initiative inquiry on Europol's big data challenge.

127 In the course of the consultation process, Member States highlighted that the EDPS admonishment touches upon Europol's core business, that there is a clear need for Europol to analyse large datasets and any possible action should be taken to minimise the impact of the EDPS decision (see annex 2).

128 Digital forensics are usually defined as the collection and analysis of data from computer systems,

to analyse large and complex datasets. Through processes of minimising and aggregating information, forensic experts filter and reduce the information contained in the datasets to what is relevant for the criminal investigation, while discarding information that is not relevant to the case.[129] Depending on the size and complexity of the dataset, such data processing may take several months or even years. The EDPS decision indicates that the agency's "*core technical and forensic support activities include the collection, extraction and restitution of computer based evidence.*"[130]

Digital forensics inevitably involves the **processing of data that is not relevant for the criminal investigation**. The purpose of this analysis is to separate necessary information from data not related to the criminal activity. For Europol's support with digital forensics, this implies it is not possible for the agency to analyse large and complex datasets without processing personal data that may not fall into the categories of data subjects in annex II of the Europol Regulation[131]. As set out in the EDPS decision, "*forensic experts' objective in this context is to process all the data received so as to provide a subset of data to the operational analysts*."[132]

Moreover, digital forensics requires the **storage of the entire dataset for the duration of the criminal investigation and, possibly, subsequent judicial proceedings** to ensure (1) data veracity, (2) the reliability of the analysis, and (3) the traceability of the decision-making process by the analysts.[133] For Europol's support with digital forensics, the EDPS decision indicates that "*large datasets are further stored [...] even after the analysts have completed the extraction process in order to ensure that they, potentially with the support of a forensic expert, can come back to the contribution in case of a new lead and to ensure the veracity, reliability and traceability of the criminal intelligence process*." The analytical reports that Europol provides may be used by a Member State as part of judicial proceedings following the criminal investigation. Table II provides a schematic overview of the handling of large and complex datasets by Europol.

---

networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law. See e.g. Suneeta Satpathy, Sachi Nandan Mohanty: Big Data Analytics and Computing for Digital Forensic Investigations (7.3.2020).

129 The techniques of digital forensics "*entails that multiple copies of datasets are created in a specific order, each one refining more and more the data so as to meet the objectives (...) Furthermore, as creating these refined copies is resource intensive, and their storage is required to establish the chain of evidence to ensure that the data is admissible as evidence in a court of law, the copies are retained so that forensic experts may go back to one of the copies as needed (for example, as new information is provided by Member States and new analysis is possible based on this new information).*" (point 3.10 of the EDPS Decision on the own initiative inquiry on Europol's big data challenge).

130 Point 3.3 of the EDPS Decision on the own initiative inquiry on Europol's big data challenge.

131 In in the course of the consultation process Member States highlighted that the nature of police investigations requires large data to be analysed before it can be established whether personal data falls into the categories of data subjects set out in annex II of the Europol Regulation, and that they might not always have the capacity to do the analysis themselves (see annex 2).

132 Point 3.10 of the EDPS Decision on the own initiative inquiry on Europol's big data challenge.

133 Point 3.11 of the EDPS Decision on the own initiative inquiry on Europol's big data challenge.

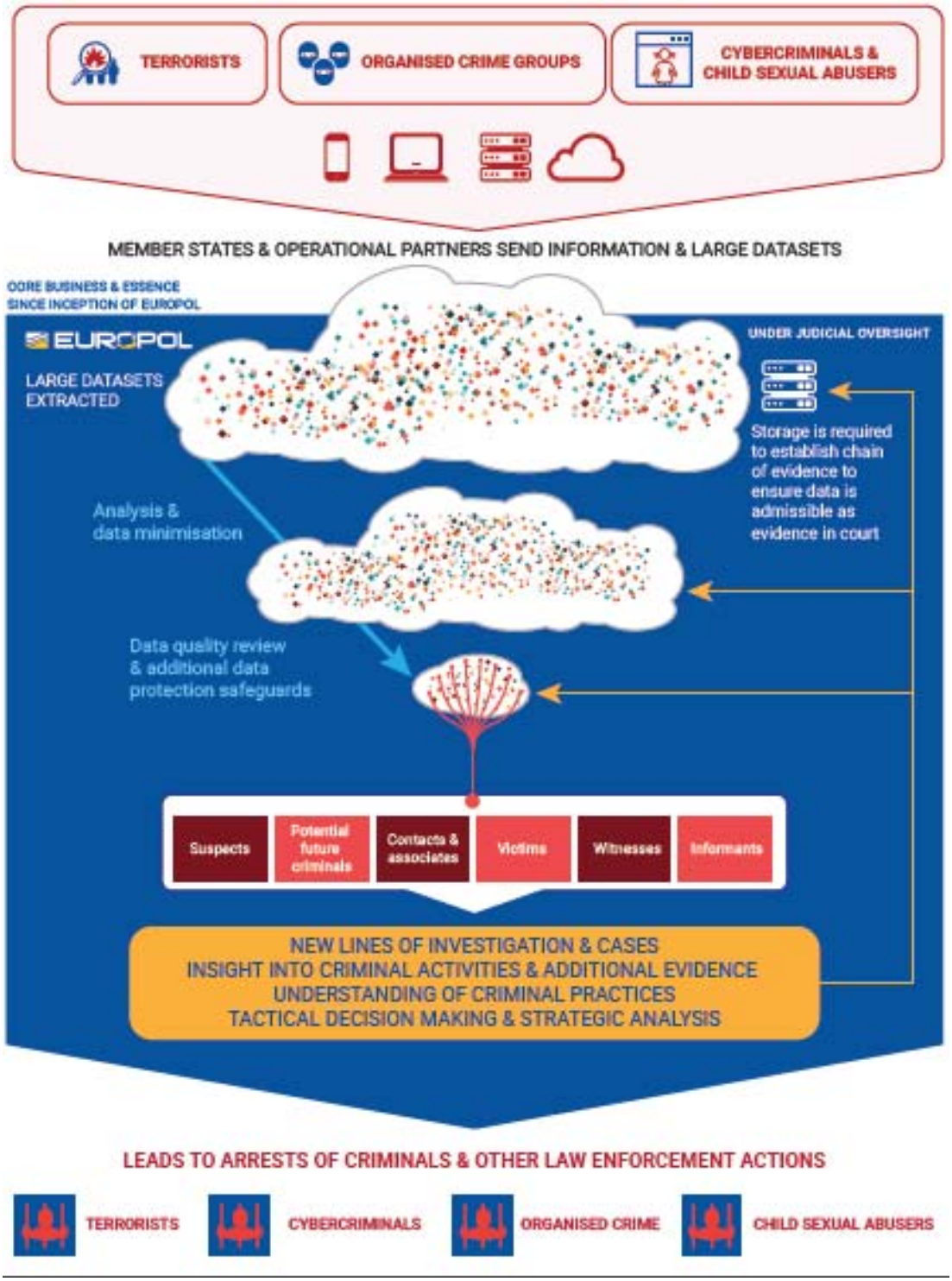

Table 2: Handling of large and complex datasets by Europol

A *third problem driver* relates to the **restrictions in the Europol Regulation**. The Europol Regulation does not explicitly set out how the agency can comply with the requirement related to specific categories of data subjects that are listed in annex II of the Regulation in its data processing, notably when it comes to the analysis of large and complex datasets submitted by Member States in the context of criminal investigations. This **structural legal problem** leads to considerable limitations to Europol's ability to provide analytical support to Member States. Those limitations are twofold:

1) The Europol Regulation does **not enable Europol to ensure its processing of personal data is limited to personal data that falls into one of the categories of data subjects listed in annex II of that Regulation**. Compliance with this

safeguard would require Europol to undertake an initial processing of personal data submitted by Member States with the sole purpose of determining whether such data falls into the specific categories of data subjects listed in annex II, e.g. by collating[134] the data. Such verification might also require checking the data submitted by Member States with data already held by Europol. The need for such initial processing of personal data in the pre-analysis phase might occur in the context of any contribution that Europol receives from Member States, irrespective of the nature of the data. When Member States submit personal data to Europol, they usually do not indicate the categories of data subjects under which the data falls. Moreover, it is not always clear from the outset if a person (to whom the data transmitted by a Member State relate) is related to a crime for which Europol is competent. Indeed, notably at an early stage of an investigation, it is often not possible to establish from the outset if a person is involved or not in the crime under investigation. When it comes to high volumes of personal data received by Europol in specific investigations, the initial data processing for the sole purpose of verification may be time-consuming and may require the use of technology. However, Europol's legal mandate does not explicitly provide for such initial data processing. In fact, the Europol Regulation does not set out any specific procedure that would enable Europol to verify if personal data submitted by Member States fall under the specific categories of data subjects in annex II of that Regulation, which results in a lack of legal clarity.

2) The Europol Regulation does **not take account of the specific requirements for the processing of large and complex datasets**. While digital forensics inevitably involves the processing of data that is not relevant for a criminal investigation, the Europol Regulation does not address the fact that it is not possible for Europol to analyse large and complex datasets without processing personal data that may not comply with the requirements linked to the categories of data subjects. Likewise, the European Regulation does not take into account that digital forensics requires the storage of the entire dataset for the duration of the criminal investigation and, possibly, subsequent judicial proceedings to ensure (1) data veracity, (2) the reliability of the analysis, and (3) the traceability of the decision-making process by the analysts. Indeed, as set out by the EDPS, the problem identified in his decision on Europol's big data challenge "*is structural – it relates to core working methods of Europol and the fact that Member States send Europol large datasets, which are difficult for Europol to process properly – in line with the requirements of the Regulation*".[135] At the same time, the EDPS argues that "*certain aspects of the structural problems could be tackled by legislatives measures*."[136]

The Home Affairs Ministers of the EU underlined in their October 2020 Declaration 'Ten points on the Future of Europol' that Europol's legal framework must ensure the Agency *'is able to fulfil its tasks in the best possible way. Europol must be – and remain – capable of working effectively in the virtual world and of processing large amounts of data. At the same time, a high level of data protection must be guaranteed'*.[137]

---

134 I.e. the pre-analysis phase where unstructured data received is being organised and structured into a format from which it can be analysed.

135 See the speech of the EDPS at the Europol Joint Parliamentary Scrutiny Group - 7th meeting (28.9.2020): https://edps.europa.eu/sites/edp/files/publication/edps-28-09-2020_europol_jpsg_en.pdf.

136 Speech of the EDPS at the Europol Joint Parliamentary Scrutiny Group - 7th meeting (28.9.2020).

137 https://www.eu2020.de/blob/2408882/6dd454a9c78a5e600f065ac3a6f03d2e/10-22-pdf-virtbrotzeit-europol-en-data.pdf.

2.2.3 How will the problem evolve without intervention?

Without any intervention, the support that Member States could seek for the analysis of large and complex datasets, notably to detect cross-border links, would be considerably affected. Given the advancement of technological developments, and the ability of criminals to quickly adapt to new technologies, it can be expected that the operational need for the analysis of large and complex datasets, notably to detect cross-border links, will further increase.

Under the current Europol Regulation, the agency may only process personal data related to specific categories of data subjects (i.e. persons related to a crime for which Europol is competent). If interpreted narrowly, this requirement would considerably limit Europol's ability to support Member States with the analysis of personal data they submit in the context of the prevention and combating of crimes falling under Europol's mandate. Europol would only be able to analyse data that Member States already pre-analysed and filtered prior to the data submission to Europol. This **structural legal issue** would significantly reduce Europol's analytical support and reduce its ability to detect cross-border links with other crimes and with known criminals and terrorists in other Member States. Indeed, without any intervention, Europol will not be able to verify if the personal data it received from Member States fall within the specific categories of personal data it is allowed to process under its legal mandate. Hence Europol could not provide the analytical support requested by the Member State.

Moreover, without any intervention, Europol may not be able to address the **structural legal problem** related to the analysis of large and complex datasets, as identified by the EDPS in its decision on Europol's big data challenge. This would have a significant impact on Europol's core working methods and hence on its operational capabilities, affecting Europol's ability to support Member States in their investigations with its own analysis of large and complex datasets to detect cross-border links.

2.3 Gaps on innovation and research relevant for law enforcement

2.3.1 What is the problem?

Technological developments offer enormous opportunities as well as considerable challenges to the EU's internal security.[138] **Criminals quickly adapt to use new technologies to their criminal ends**. Law enforcement authorities, instead, have difficulties in detecting and investigating crimes that are prepared or carried out with the support of new technologies. For example, while encryption is essential to the digital world, securing digital systems and transactions and also protecting a series of Fundamental Rights, it is also used by criminals to mask their identity, hide the content of their communications, and secretly transfer illicit goods and resources.[139] Indeed, today, a substantial part of investigations against all forms of crime and terrorism involve encrypted information. The increased criminal abuse of secured mobile devices is visible across many criminal threats areas and likely to continue, with a growing market for

[138] These include developments such as 5G mobile networks, artificial intelligence, the internet of things, drones, anonymisation and encryption, 3D printing and biotechnology.

[139] The December 2016 Justice and Home Affairs Council highlighted that „*the use of encryption for communications over the internet has developed dramatically in the last few years. While encryption is a legitimate tool to preserve privacy and cybersecurity, the opportunities offered by encryption technologies are also exploited by criminals in order to hide their data and potential evidence, and to protect their communications and financial transactions.*" In response, Europol and Eurojust set up an observatory function on encryption.

encrypted communication providers dedicated to organised crime groups.[140] For example, the joint investigation to dismantle *EncroChat,* an encrypted phone network used by criminal networks involved in violent attacks, corruption, attempted murders and large-scale drug transports, shows how criminal networks use advanced technologies to cooperate at national and international level.[141] However, as highlighted in Europol's Internet Organised Crime Threat Assessment 2020, "*this type of success is an exception as the rule remains that law enforcement continues to battle the challenges of criminal use of advanced technologies*".[142]

Technological developments and emerging threats require law enforcement authorities to have access to new tools to be able to counter such threats. As set out in the July 2020 Security Union Strategy,[143] "*innovation should be seen as a strategic tool to counter current threats and to anticipate both future risks and opportunities*". For example, given that the work of law enforcement is an information-based activity, the ability of artificial intelligence (AI) tools to rapidly process information "*makes AI a perfect partner for law enforcement*".[144] Indeed, as set out in the Commission's White Paper[145] on Artificial Intelligence – A European approach to excellence and trust, AI tools can provide an opportunity for better protecting EU citizens from crime and acts of terrorism. Such tools could, for example, help identify online terrorist propaganda, discover suspicious transactions in the sales of dangerous products, identify dangerous hidden objects or illicit substances or products, offer assistance to citizens in emergencies and help guide first responders. However, **not all Member States are able to exploit fully the opportunities of new technologies** for fighting crime and terrorism, and to overcome the challenges posed by the abuse of these technologies by criminals and terrorists, given the investment, resources and skills this requires. The significant technical and financial investments required for solutions at national level would strain and possibly exceed the capabilities of individual Member States. Likewise, EU funding for individual national solutions would be a less efficient way of addressing these problems, as it would not create economies of scale. It would also risk maintaining or even increasing the fragmentation of systems and standards. This calls for cooperation at EU level to create synergies and achieve economies of scale.

Moreover, beyond the necessary expertise and infrastructure, **innovation and the development of new technologies often rely on the availability of large amounts of data**. A key precondition to develop reliable technologies is high quality data sets. Unreliable or biased data sets risk leading to biased technology. Moreover, the quality of the data set also depends on the quantity of data it entails. Establishing high quality data sets has considerable financial, training and resources implications, which, again, can be best met at EU level.[146] This is also the case for the training, testing and validation of algorithms for the development of tools for law enforcement, where it is of crucial importance to avoid that biased data results in biased tools.[147] AI systems based on

---

140 Europol and Eurojust Joint Report: Second report of the observatory function on encryption (18.2.2020).

141 https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.

142 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

143 COM(2020) 605 final (24.7.2020), p. 24.

144 Odhran James McCarthy: AI & Global Governance: Turning the tide on crime with predictive policing, Centre for Policy Research, United Nations University (26.2.2019).

145 COM(2020) 65 final (19.2.2020).

146 See the Commission Communication on "A European strategy for data" (COM(2002) 66 final (19.2.2020)).

147 Odhran James McCarthy: AI & Global Governance: Turning the tide on crime with predictive

incomplete or biased data can lead to inaccurate outcomes that infringe on people's fundamental rights, including discrimination.[148] More generally, the use of AI systems for law enforcement can substantially impact Fundamental Rights.[149] This calls for transparency in the development of such systems and tools, in order to allow for the detection of any discrimination in their application and to enable effective remedies.[150] However, in the absence of an EU approach to innovation in the area of law enforcement, national law enforcement authorities often rely on tools and products developed outside the EU.[151] Indeed, as shown in a European Parliament study on AI and law enforcement, "*the advent of AI in the field of law enforcement and criminal justice is already a reality, as AI systems are increasingly being adopted or considered*."[152] Notably where law enforcement authorities rely on tools and products that were developed outside the EU, and hence not necessarily in a transparent way that complies with EU norms and Fundamental Rights, such use of modern technology for law enforcement has generated significant controversy.[153] This calls for an EU-level capacity to train, test and validate algorithms for the development of tools, including AI-based tools, for law enforcement, in full compliance with Fundamental Rights and with the necessary transparency.

Reflecting the **need for an EU approach to innovation in the area of law enforcement**, at the October 2019 Justice and Home Affairs Council, "*Ministers expressed their overall support for the creation of an innovation lab at Europol which could act as an observatory of new technological developments and drive innovation, including by developing common technological solutions for member states in the field of internal security.*"[154] Likewise, in a December 2018 Resolution, the European Parliament called "*for the active involvement of EU agencies such as Europol and CEPOL in EU security research projects*."[155] Indeed, Europol could have a real added value in supporting Member States in fully exploiting the advantages of new technologies for fighting serious crime and terrorism by coordinating Members States' efforts in this field.[156] Moreover, with its access to high quality operational data from law enforcement, Europol would also be well suited to train, test and validate algorithms for the development of tools for law enforcement. There is no other entity at EU level which can provide this kind of support to Member States' law enforcement authorities.

However, **Europol does not have a mandate** to support Member States on fostering innovation and using the results of research relevant for law enforcement. Notably, the Europol Regulation does not provide for an active role of the agency in steering innovation and research efforts in support of Member States' fight against serious crime

---

policing, Centre for Policy Research, United Nations University (26.2.2019).

148 EU Agency for Fundamental Rights: Data quality and artificial intelligence – mitigating bias and error to protect Fundamental Rights (2019).

149 European Parliament Study: Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights (July 2020).

150 EU Agency for Fundamental Rights: #BiGData: Dicrimination in data-supported decision making (2018).

151 This also relates to the risk of technological dependency.

152 European Parliament Study: Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights (July 2020), p 8.

153 See, for example, the letter by the European Data Protection Board on the use of the Clearview AI application by law enforcement authorities in the EU (10.6.2020): https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf.

154 https://www.consilium.europa.eu/media/41015/st12837-en19_both-days_edited.pdf.

155 European Parliament resolution of 12 December 2018 on findings and recommendations of the Special Committee on Terrorism.

156 74.65 % of the participants of the targeted consultation by way of questionnaire (see annex 11) consider that there is a need for Europol to step up its support to Member States on research and innovation.

and terrorism.

As the use of innovation and modern technology for law enforcement involves the processing of personal data for the development of tools, the assessment of policy options to address the identified problem also needs to take full account of Fundamental Rights and notably the right to the protection of personal data.

2.3.2 What are the problem drivers?

Technological developments, and the use that criminals and terrorists make of new technologies, amplify the **gaps on innovation and research relevant for law enforcement**. There are three drivers for this problem.

As a *first problem driver*, **not all Member States are well equipped to exploit fully the advantages of new technologies for law enforcement** and to tackle effectively the considerable security challenges stemming from the abuse of these technologies by criminals and terrorists, given the resources and skills this requires. Only a few Member States have national security research programmes in place while some Member States implement initiatives to modernise their law enforcement authorities in that respect.[157] This requires significant technical and financial investment, calling for cooperation at EU level to achieve economies of scale. **EU security research responds to that need**, with security research funding under Horizon 2020 representing a very significant part (circa 50%) of all public funding in the EU on research in the security sector.[158] Indeed, with over 600 projects launched for an overall value close to €3 billion since 2007, EU-funded security research is a key instrument to drive technology and knowledge in support of security solutions.

Building on that, the next generation of EU funding proposals can act as a major stimulus for the security dimension of EU research, innovation and technological development.[159] EU research, innovation and technological development indeed offer the opportunity to take the security dimension – and hence the needs to law enforcement authorities – into account as these technologies and their application are developed, with the aim to scale up the technological capacities of law enforcement across Europe. Moreover, by fostering cross-border projects, EU security research takes account of the cross-border dimension of many of today's security threats, as well as the need for cross-border cooperation among law enforcement authorities to tackle these threats. This requires close cooperation between the law enforcement community, research, industry, policy makers and citizens. A number of initiatives address this need for cooperation in the context of EU security-related funding under Horizon 2020 and the EU Internal Security Fund, such as the mandatory participation of end-users in security research projects, or the involvement of dedicated networks of practitioners.[160] However, there is still a **gap on the coordination of research and innovation needs on the side of law enforcement**, which constitutes the *second problem driver*. Consolidating the end-user needs of the law enforcement community in Europe would help ensuring a strong EU-added value of EU

---

157 European Commission: Security research and innovation - Boosting effectiveness of the Security Union (August 2017).

158 Horizon 2020 Protection And Security Advisory Group: Improving the Effectiveness of Market Uptake of EU Research within the Security Sector (July 2020).

159 The Commission's proposals for Horizon Europe, the Internal Security Fund, the Integrated Border Management Fund, the EUInvest Programme, the European Regional Development Fund and the Digital Europe Programme will all support the development and deployment of innovative security technologies and solutions along the security value chain.

160 Networks such as ENLETS (http://www.enlets.eu/), ENFSI (https://enfsi.eu), I-LEAD (https://i-lead.eu) and ILEAnet (https://www.ileanet.eu).

security research. Europol, the EU agency for law enforcement cooperation, is at the heart of the EU internal security architecture and would therefore be well positioned to close that gap, in the same way as the European Border and Coast Guard Agency[161] plays this role for research and innovation activities relevant for border management.

However, **Europol does not have a mandate to support Member States in fostering research and innovation relevant for law enforcement**, which constitutes a *third problem driver*. The related restrictions in the Europol Regulation are twofold:

- First, the Europol Regulation does not foresee any role for the agency to implement its own innovation projects and contribute to research and innovation activities relevant for law enforcement.[162] While this does not prevent the Agency from engaging in punctual activities that fall under its mandate,[163] the lack of a clear legal basis has an impact on the resources available to Europol for playing a broad and central role in related activities. Notably, the Europol Regulation does not foresee any role for Europol to assist the Commission in identifying key research themes, drawing up and steering the Union framework programmes for research and innovation activities that are relevant for law enforcement, as well as supporting the uptake of the outcome of that research.[164] Again, while this does not prevent the Commission from involving Europol in the implementation of relevant Union framework programmes, the lack of a clear legal basis has an impact on the resources available to Europol for such activities.
- Second, while the Europol Regulation provides for the processing of personal data for historical, statistical or scientific research purposes,[165] this does arguably not enable the agency to process personal data for the training, testing and validation of algorithms for the development of tools, including AI-based tools, for law enforcement. The EDPS has indeed taken this view, and has started an inquiry into Europol's processing of operational data for data science purposes.[166] As innovation and the development of new technologies often rely on the availability of large amounts of data, the restrictions in Europol's current legal mandate hamper the agency's ability to support Member States in fostering research and innovation relevant for law enforcement.

2.3.3 How will the problem evolve without intervention?

The **gaps on innovation and research relevant for law enforcement** will have even greater impact in the future. As the technological developments will advance, and given that criminals have proven very efficient in the misuse of new technologies, the

---

161 See Article 66 of Regulation (EU) 2019/1896. See also the Terms of Reference to improve collaboration on research and innovation relevant for EU border security, as co-signed by the Commission's Directorate-General for Migration and Home Affairs and the European Border and Coast Guard Agency (6.2.2020): https://ec.europa.eu/home-affairs/sites/homeaffairs/files/20200206_tor-ec-dg-home-frontex.pdf.

162 For the area of border management, such a role is provided for the European Border and Coast Guard Agency in its mandate (see Article 66(1) and (4) of Regulation (EU) 2019/1896).

163 For example, Europol will be part of three Horizon 2020 security research projects related to: (1) the use of AI for the fight against child sexual exploitation material online, (GRACE), (2) the use of AI to increase efficiency of investigations in counter-terrorism and cybercrime (AIDA), and (3) the setting up of a virtual reality-based environment for complex investigations (INFINITY).

164 For the area of border management, such a role is provided for the European Border and Coast Guard Agency in its mandate (see Article 66(2) of Regulation (EU) 2019/1896).

165 See Article 28(1)(b) of Regulation (EU) 2016/794.

166 See the letter from the EDPS to the Co-Chairs of the Europol Joint Parliamentary Scrutiny Group (23.9.2020): https://edps.europa.eu/sites/edp/files/publication/20-09-28_letter_jpsg_en.pdf.

challenges posed by technology to the EU's internal security will even increase. The advancement and increased implementation of new technologies will further complicate the ability of law enforcement to gain access to and gather necessary data for criminal investigations. Without an intervention, technological developments will make it even easier for criminals and terrorists to mask their identity, hide the content of their communications, and secretly transfer illicit goods and resources.

The need for investment, resources and skills to tackle this security challenge will persist or even increase. They would strain and possibly exceed the capabilities of individual **Member States**. Without any intervention, the support that Member States will get from EU security-related funding will not develop its full potential due to the gap on the coordination of research and innovation needs on the side of law enforcement.

In terms of **possible EU-level solutions**, Europol is well placed to support Member States in fostering research and innovation relevant for law enforcement. However, without any intervention, the agency's ability to do so will remain constrained by the lack of a clear legal basis to work on innovation for law enforcement, as well as by the lack of clear legal grounds for the processing of personal data for the training, testing and validation of algorithms for the development of tools, including AI-based tools, for law enforcement.

3. WHY SHOULD THE EU ACT?

3.1. Legal basis

The legal basis of the initiative is Article 88 of the Treaty on the Functioning of the European Union (TFEU). Article 88(1) TFEU stipulates that Europol's mission shall be to support and strengthen action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy. It provides for Europol to be governed by a Regulation to be adopted in accordance with the ordinary legislative procedure.

3.2. Subsidiarity: Necessity of EU action

According to the principle of subsidiarity laid down in Article 5(3) TEU, action at EU level should be taken only when the aims envisaged cannot be achieved sufficiently by Member States alone and can therefore, by reason of the scale or effects of the proposed action, be better achieved by the EU. Furthermore, there is a need to match the nature and intensity of a given measure to the identified problem (proportionality).

Member States are responsible for the maintenance of law and order and the safeguarding of internal security.[167] Indeed, the Union shall respect Member States' essential state functions, including maintaining law and order and safeguarding national security.[168] As serious crime and terrorism are of a transnational nature, action at national level alone cannot counter them effectively. This is why Member States choose to work together within the framework of the EU to tackle the threats posed by serious crime and terrorism. They seek to coordinate their law enforcement action and cooperate in addressing shared security challenges. They decide to pool resources at EU level and share expertise. As the EU agency for law enforcement cooperation, Europol is a strong

[167] Article 72 TFEU.
[168] Article 4(2) TEU.

expression of this endeavour by the Member States to keep their citizens safe by working together. Europol provides a framework for Member States to coordinate their law enforcement action. Member States use their liaison officers at Europol and the information exchange channel the agency provides to exchange information and cooperate in their criminal investigations. They pool resources by tasking Europol to process their information in its databases and provide joint analysis. They use the growing expertise that Europol brings together on a variety of aspects of policing. This has made Europol the most visible component of EU-level support for Member States' law enforcement authorities.

Evolving security threats, driven by the way criminals exploit the advantages that the digital transformation and new technologies bring about, also call for effective EU level support to the work of national law enforcement authorities. There are of course differences in the way individual Member States, their regions and local communities confront specific types of crime. This is why their law enforcement authorities can choose where to seek EU-level support from Europol and what joint initiatives to participate in. In any case, law enforcement authorities across all Member States, regions and local levels face the same evolving security threats. Consequently, there is a need for EU action to step up the support to Member States in fighting serious crime and terrorism to keep pace with these threats.

Indeed, for all three problems discussed in chapter 2, Member States alone would not be able to effectively tackle these problems:

- As regards the **lack of effective cooperation between private parties and law enforcement authorities** to counter the abuse of cross-border services by criminals, national authorities cannot alone analyse multi-jurisdictional or non-attributable data sets effectively, as it is very resource intensive to sift through large data sets in order to identify the data relevant for the respective jurisdiction. Alternatively, if the national law enforcement authorities obtain smaller data sets targeted to their respective jurisdiction, they fall short of the entire intelligence picture. Furthermore, Member States cannot effectively address these problems through an intergovernmental cooperation, by which the Member State of establishment were to receive the data, analyse and then distribute it to the Member States concerned. This would not only entail disproportionate resource implications for the Member States of establishment, but also legal difficulties in situations, where the criminal activity has no or limited link to the jurisdiction of that Member State.
- As regards the **big data challenge for law enforcement**, Member States cannot detect such cross-border links through their own analysis of the large datasets at national level, as they lack the corresponding data on other crimes and criminals in other Member States. Moreover, some Member States might not always have the necessary IT tools, expertise and resources to analyse large and complex datasets.
- As regards **gaps on innovation and research relevant for law enforcement**, not all Member States are able to exploit fully the opportunities of new technologies for fighting crime and terrorism, and to overcome the challenges posed by the abuse of these technologies by criminals and terrorists, given the investment, resources and skills this requires. The significant technical and financial investments required for this would strain and possibly exceed the capabilities of individual Member States. This calls for cooperation at EU level to create synergies and achieve economies of scale.

Many of the problems and problem drivers identified in chapter 2 relate to the limitations identified in the Europol legal mandate. As Europol is an EU agency governed by a Regulation, EU action is needed to strengthen Europol and provide it with the capabilities and tools its needs to support effectively Member States in countering serious crime and terrorism in a changing security landscape.

3.3. Subsidiarity: Added value of EU action

As set out in chapter 2, all problems addressed in this impact assessment call, in one way or another, for **EU-level support** for Member States to tackle these problems effectively:

- As regards the **lack of effective cooperation between private parties and law enforcement authorities** to counter the abuse of cross-border services by criminals, these problems can be tackled more effectively and efficiently at EU level than at national level, by analysing multi-jurisdictional or non-attributable data sets at EU level in order to identify the data relevant for the respective Member States concerned, and by creating an EU level channel for requests containing personal data to private parties.
- As regards the **big data challenge for law enforcement**, these problems can be tackled more effectively and efficiently at EU level than at national level, by assisting Member States in processing large and complex datasets to support their criminal investigations with cross-border leads. This would include techniques of digital forensics to identify the necessary information and detect links with crimes and criminals in other Member States.
- As regards **gaps on innovation and research relevant for law enforcement**, and given the significant technical and financial investments required, these problems can be tackled more effectively and efficiently at EU level than at national level, by creating synergies and achieving economies of scale. For that to bring most added value in terms on EU funding for security research, there is a need to close the gap on the coordination of research and innovation needs on the side of law enforcement. Moreover, innovation and the development of new technologies often rely on the availability of large amounts of data, which can be realised better at EU level. Training, testing and validating algorithms for the development of tools, including AI-based tools, for law enforcement, in full compliance with Fundamental Rights as well as with the necessary transparency, can be done more effectively at EU than at national level. Moreover, by promoting the development of EU tools to counter serious crime and terrorism, an EU approach to innovation takes account of the cross-border dimension of many of today's security threats, as well as the need for cross-border cooperation among law enforcement authorities to tackle these threats.

As the EU agency for law enforcement cooperation, Europol would be well positioned to provide this EU-level support. Indeed, Europol has proven very effective in supporting national law enforcement authorities in countering serious crime and terrorism. The Management Board of Europol, bringing together representatives of the Member States and the Commission to effectively supervise the work of the agency, notes that "*'users' satisfaction with Europol's products and services and with how Europol's work contributed to achieve operational outcomes, is very high (...), thereby confirming the continued trust of Member States in Europol's ability to support their action in preventing and combating serious organised crime and terrorism*".[169] The stakeholder consultation carried out in the preparation of the impact assessment also showed a very

[169] Europol: 2019 Consolidated Annual Activity Report (9.6.2020).

high level of satisfaction with Europol. There are clear synergies and economies of scale for Member States resulting, for example, from the joint processing of information by Europol, or from the expertise that the specialised Centres[170] pool and offer to Member States. Member States expect, and operationally need, the same level of support from Europol when it comes to evolving security threats.

Law enforcement cooperation at EU-level through Europol does not replace different national policies on internal security. It does not substitute the work of national law enforcement authorities. Quite the contrary, EU-level action and the services provided by Europol support and reinforce national security policies and the work of national law enforcement authorities, helping them to enforce the law against criminals and terrorist that act across borders. Differences in the legal systems and traditions of the Member States, as acknowledged by the Treaties,[171] remain unaffected by this EU level support.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1. General objectives

The general objectives of this initiative result from the Treaty-based goals:

- for Europol to support and strengthen action by the Member States' law enforcement authorities and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy;[172]
- to endeavour to ensure a high level of security through measures to prevent and combat crime.[173]

4.2. Specific objectives

The specific policy objectives addressed in this impact assessment respond to the three problems identified in chapter 2. They derive from the general objectives set out in section 4.1.

- ***Objective I***: Enabling effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals.
- ***Objective II***: Enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with Fundamental Rights.
- ***Objective III***: Enabling Member States to use new technologies for law enforcement.

Objective I: Enabling effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals

The first specific objective is to enable law enforcement authorities to cooperate effectively with private parties. The aim is to find an effective EU-level solution to support Member States in identifying cases and information with relevance for their

170 European Cybercrime Centre, European Migrant Smuggling Centre, European Counter Terrorism Centre and European Financial and Economic Crime Centre.
171 Article 67(1) TFEU.
172 Article 88 TFEU.
173 Article 67 TFEU.

respective jurisdictions, in particular where the cases rely on the analysis of multi-jurisdictional data sets, or data sets where the jurisdiction of the data subjects is difficult to establish, and to be able to serve as a channel to transmit Member States' requests containing personal data to private parties.[174]

This specific objective addresses the problems resulting from private parties holding increasing amounts of non-attributable or multi-jurisdictional data sets relevant for law enforcement authorities in multiple jurisdictions, the difficulties faced by private parties in sharing relevant data with the Member States concerned, and the challenges faced by Member States in identifying and obtaining data relevant for their respective jurisdictions.

This specific objective raises the **policy choice** about the extent to which Europol should be able to receive and request personal data relating to criminal activities from private parties. This relates to the core function of Europol as the EU's information hub for criminal intelligence and operational support capabilities, and therefore to core tasks of Europol under its legal mandate that Member States expect from the agency.

This policy choice should create synergies and avoid overlaps with existing policy instruments, notably with regard to the work of the **financial intelligence units** (FIUs). Europol should remain limited to processing criminal intelligence with a clear link to forms of crime falling under the agency's mandate. Any cooperation with private parties should remain strictly within the limits of Europol's mandate and should neither duplicate nor interfere with the activities of the FIUs. Europol will continue to cooperate with FIUs via their national units in full respect of their competence and mandate as foreseen under Article 7 (8) of the Europol Regulation and under Articles 11 to 14 of the Directive (EU) 2019/1153.

As regards cyber security, Europol's ability to cooperate with private parties would complement the work of the European Union Agency for Cybersecurity (ENISA) and the cyber security community such as Computer Security Incident Response Teams (CSIRTs). While the cyber security community works mostly on resilience (i.e. on preventing or mitigating cyber attacks through awareness raising or better coordination), Europol could provide added value in supporting Member States investigating the criminal activities behind cyber attacks.[175] Europol and ENISA have concluded a Memorandum of Understanding,[176] and have already in the past successfully cooperated on large scale cyber attacks such as WannaCry.[177] In addition, national authorities could benefit from using Europol's infrastructure when exchanging critical information amongst each other or with private parties in the context of large scale cyber attacks.

As the cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals includes the processing of personal data, the assessment of policy options to achieve the identified objective needs to take **full account of Fundamental Rights and notably the right to the protection of personal**

---

174 For example, this would enable that Member States to make use of channels set up by Europol to ensure co-ordination with regards to removal orders and referrals as foreseen by Article 13 of the proposed Regulation on preventing the dissemination of terrorist content online.

175 The NIS Directive (2016/1148) provides a framework for cooperation in the cybersecurity area, including, where appropriate, with law enforcement authorities. EU Member State authorities could benefit from Europol's support in this area.

176 https://www.europol.europa.eu/newsroom/news/four-eu-cybersecurity-organisations-enhance-cooperation

177 https://www.europol.europa.eu/newsroom/news/2017-year-when-cybercrime-hit-close-to-home.

data.

<u>Objective II</u>: Enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with Fundamental Rights

The second specific objective is to **enable law enforcement authorities to analyse large and complex datasets to detect cross-border links**, in full compliance with Fundamental Rights. Data collected in criminal investigations are increasing in size and becoming semantically more complex.

This specific objective addresses the **big data challenge for law enforcement authorities**, which results from the fact that criminals and terrorist use information and communications technology to communicate among themselves and to prepare and conduct their criminal activity.

As set out above, where the crimes and related criminal investigations have a cross-border element, **Member States** cannot detect cross-border links with crimes and criminals in other Member States through their own analysis.

This calls for **EU-level support** in the processing of large and complex datasets from Member States to support their criminal investigations with cross-border leads. This would include techniques of digital forensics to identify the necessary information and detect links with crimes and criminals in other Member States.

This specific objective raises the **policy choice** whether Europol should continue to be able to support Member States' criminal investigations falling under Europol's mandate with the processing of large and complex datasets to detect cross-border links. Europol would indeed be best placed to provide this EU-level support, as it relates to the essence of Europol's working methods and operational support capabilities, and therefore to core tasks of Europol under its legal mandate that Member States expect from the agency.

As the analysis of large and complex datasets includes the processing of personal data, including the potential processing of data of persons not related to a crime, the assessment of policy options to achieve the identified objective needs to take **full account of Fundamental Rights and notably the right to the protection of personal data**.

<u>Objective III</u>: Enabling Member States to use new technologies for law enforcement

The third specific objective is to **enable Member States to use new technologies for law enforcement.** The abuse of modern technologies by criminals and terrorists raises considerable security threats. At the same time, modern technologies offer enormous opportunities for law enforcement to better prevent, detect and investigate crimes.

This specific objective addresses the **problem of gaps on innovation relevant for law enforcement authorities**. It addresses the identified gap on the coordination of research and innovation needs on the side of law enforcement, as well as the identified need for a capacity to train, test and validate algorithms for the development of tools, including AI-based tools, for law enforcement, in full compliance with Fundamental Rights and with the necessary transparency

As set out above, the need for investment, resources and skills to tackle the identified security threats would strain and possibly exceed the capabilities of individual **Member States**.

Indeed, the significant technical and financial investments required **call for cooperation at EU level** to create synergies and achieve economies of scale. For that to bring most added value in terms of EU funding for security research, there is a need to close the gap on the coordination of research and innovation needs on the side of law enforcement. Moreover, innovation and the development of new technologies often rely on the availability of large amounts of data, which again calls for an EU approach.[178] There is a real need for an EU-level capacity to train, test and validate algorithms for the development of tools, including AI-based tools, for law enforcement, in full compliance with Fundamental Rights as well as with the necessary transparency.

This specific objective raises the **policy choice** whether Europol should be able to support Member States in fully exploiting the advantages of new technologies for fighting serious crime and terrorism, including by assisting the Commission in implementing the Union framework programmes for research and innovation activities relevant for law enforcement. As the EU agency for law enforcement cooperation, Europol would be well placed to close the identified gap on the coordination of research and innovation needs on the side of law enforcement. Moreover, this specific objective raises the policy choice whether Europol should be able to process personal data for the training, testing and validation of algorithms for the development of tools, including AI-based tools, for law enforcement, in full compliance with Fundamental Rights and with the necessary transparency.

As the specific objective includes the processing of personal data for training, testing and validation of algorithms for the development of tools, including AI-based tools, for law enforcement, the assessment of policy options to achieve the identified objective needs to take **full account of Fundamental Rights and notably the right to the protection of personal data**.

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

This chapter sets out the available policy options, which include the baseline as well as several options requiring regulatory or non-regulatory interventions. A number of policy options, which were discarded at an early stage, are set out in annex 9.

5.1. Baseline representing current situation

The baseline is a 'no policy change' scenario.

With regard to **private parties**, the baseline scenario would be to maintain the current legal regime. Under this regime, Europol can receive personal data from private parties only via competent intermediaries (Member States' National Units, contact points of third countries or international organisations with which Europol can exchange personal data). In cases where private parties proactively share personal data directly with Europol, the agency may process this data only to identify the responsible national unit, transfer it to that national unit and then delete it. The national unit may then decide to resubmit the data. If Europol cannot identify the responsible national unit within four months, it will delete the data in question even if it is clearly relevant to its tasks.[179]

---

[178] See the Commission Communication on "A European strategy for data" (COM(2002) 66 final (19.2.2020)).

[179] There are only three exceptions which allow Europol to transfer personal data directly to private parties, namely (i) if the transfer is undoubtedly in the interest of the data subject; (ii) if the transfer is absolutely necessary in the interest of preventing the imminent perpetration of a crime; or (iii) if the

Europol is prohibited from contacting private parties with requests for personal data. This situation increases the risks of delays (e.g. where the identification of the Member State concerned is difficult and time-consuming), increase the risk of loss of information (e.g. where Europol does not have enough information to identify the Member State concerned), and lead to a lack of legal certainty for private parties, when they submit personal data to Europol (see chapter 2.1).

As regards the objective to **enable law enforcement to analyse large and complex datasets to detect cross-border links**, in full compliance with Fundamental Rights, the baseline assumes that Europol's legal mandate would remain ambiguous on how the agency can ensure its data processing is limited to personal data that fall into the specific categories of data subjects that Europol is entitled to process (namely suspects, convicted criminals, potential future criminals, contacts and associates, victims, witnesses and informants), including for preventive action and criminal intelligence. Moreover, in the baseline scenario, Europol may not be able to address the structural legal problem related to the analysis of large and complex datasets, as identified by the EDPS in its decision on Europol's big data challenge. This would have an impact on Europol's core working methods and hence on its operational capabilities, affecting Europol's ability to support Member States in the analysis of large and complex datasets to detect cross-border links. This, in turn, would seriously hamper Member States' ability to investigate serious cross-border crimes that require the analysis of large and complex datasets.

When it comes to the objective to **enable Europol to provide effective support to Member States on the development and use of new technologies**, the baseline scenario takes account of the next generation of EU funding proposals that can act as a major stimulus for the security dimension of EU research, innovation and technological development.[180] However, the support that Member States will get from EU security-related funding might not develop its full potential due to the gap on the coordination of research and innovation needs on the side of law enforcement. Moreover, in the absence of an EU approach to innovation in the area of law enforcement, and in light of technological development, it will become even more difficult for individual national law enforcement authorities to counter criminals and terrorists who use modern technology to mask their identity, hide the content of their communications, and secretly transfer illicit goods and resources. Without a legal intervention, it would not be possible to step up effective cooperation of national law enforcement authorities on research and innovation, as it would lack the necessary structure and resources to ensure such coordination and, notably, to carry out related research and innovation activities.

5.2. Description of policy options requiring an intervention

This impact assessment addresses policy options requiring a regulatory intervention. A number of non-regulatory options had been considered at earlier stages of the analysis but were eventually discarded (see annex 9 on policy options discarded at an early stage). The focus on options requiring a regulatory intervention does not come as a surprise, given that the problems identified in this impact assessment are partially driven by

---

transfer concerns publicly available data and is strictly necessary for preventing and combatting internet-facilitated crimes (so-called referrals). Following such referrals of publicly available data, Europol may in connection therewith also receive personal data from private parties, if that private party declares it is legally allowed to transmit this data in accordance with the applicable law.

180 The Commission's proposals for Horizon Europe, the Internal Security Fund, the Integrated Border Management Fund, the InvestEU Programme, the European Regional Development Fund and the Digital Europe Programme will all support the development and deployment of innovative security technologies and solutions along the security value chain.

restrictions in the Europol Regulation (see chapter 2).

specific objectives	**policy options requiring a regulatory intervention**
Objective I: enabling effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals	• ***Policy option 1***: allowing Europol to process data received directly from private parties • ***Policy option 2***: allowing Europol to exchange personal data with private parties to establish jurisdiction, as well as to serve as a channel to transmit Member States' requests to private parties • ***Policy option 3***: allowing Europol to directly query databases managed by private parties in specific investigations
Objective II: enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with Fundamental Rights	• ***Policy option 4***: clarifying the provisions on the purposes of information processing activities and enabling Europol to analyse large and complex datasets • ***Policy option 5***: introducing a new category of data subjects whose data Europol can process
Objective III: enabling Member States to use new technologies for law enforcement	• ***Policy option 6***: regulating Europol's support to the EU security research programme, the innovation lab at Europol, and Europol's support to the EU innovation hub • ***Policy option 7***: enabling Europol to process personal data for the purpose of innovation in areas relevant for its support to law enforcement

Table 3: Link between objectives and policy options

5.2.1 Enabling effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals

Policy option 1: allowing Europol to process data received directly from private parties

Policy option 1 would **allow Europol to fully process data received directly from private parties on their own initiative**.

As explained in section 2.1 above, national authorities cannot effectively analyse multi-jurisdictional or non-attributable data sets through national solutions or through intergovernmental cooperation. Moreover, in terms of **possible EU-level solution**, Europol is best placed to support Member States in analysing multi-jurisdictional or non-attributable data sets from private parties with a view to identifying the Member States, which would be able to establish jurisdiction.

Private parties can already share personal data directly with Europol, which they are legally allowed to transmit in accordance with their applicable laws (Article 26(3) of the Europol Regulation). However, under this provision, Europol assesses such personal data in a technically isolated way without analysing it against other data in its systems, without enriching this data with further analysis that would help the Member States concerned to establish their jurisdiction, and only within a timeframe of four months (Article 26(2) of the Europol Regulation).

Under this policy option, Europol would process the data more broadly in line with Article 18 Europol Regulation and within the general time-limits for the processing of such data (Article 31 of the Europol Regulation). Europol would not only transmit the personal data itself to all Member States concerned, but also the analysis resulting from its processing with a view to supporting Member States concerned in establishing their jurisdiction. Europol would no longer be obliged to delete the data after four months, if the agency cannot identify the national unit, contact point or authority concerned within this timeframe, but can continue to analyse the data in order to establish the Member States concerned. As regards the necessary safeguards, all the safeguards set out in the rules applicable to personal data, which Europol receives from competent authorities, would also apply to personal data, which Europol receives directly from private parties.[181] Applicable safeguards include the following:

- Upon receiving the data, Europol would process the personal data only temporarily for as long is necessary to determine whether the data is relevant to its tasks. If the data is not relevant for its tasks, Europol would delete the data after six months (Article 18 (6) Europol Regulation). Only if the data is relevant to its tasks, would Europol process the data further. In practice, this would mean that Europol would delete personal data on data subjects, which are not associated with a serious crime falling within Europol's mandate. There should be a high threshold with clear criteria and strict conditions for Europol to determine whether data received from private parties is relevant for Europol's objectives and should become part of Europol's operational data.
- Furthermore, Europol would be limited in the way it can process special categories of data (e.g. on ethnicity or religious beliefs) and different categories of data subjects (e.g. victims and witnesses) (Article 30 Europol Regulation).

[181] See p. 45 of the Opinion of the European Union Agency for Fundamental Rights on Interoperability and fundamental rights implications (11.4.2018).

- Moreover, Europol would not be allowed to process the data for longer than necessary and proportionate, and within the time-limits set by the Europol Regulation (Article 31).
- Also, the Europol Regulation would ensure the necessary data subject rights, in particular a right of access (Article 36), and a right to rectification, erasure and restriction (Article 37).
- In addition, the Europol Regulation would ensure the possibility for an individual to pursue legal remedies (Article 47 and 48 Europol Regulation).

This option would partly address the first problem driver identified in section 2.1 above, by providing private parties with a contact point to share multi-jurisdictional or non-attributable data sets with law enforcement. This option would also partly address the second problem driver identified above, by enabling Europol to fully process and enrich data received from private parties with a view to identifying all Member States concerned, which would be able to establish their jurisdiction. Even if Europol would not be able to immediately identify the Member State concerned, the agency would not have to delete this data after four months, so the risk of data loss would be mitigated. Finally, this policy option would partly address the fourth problem driver, as far as it enables Europol to receive personal data directly from private parties.

However, under this option Europol could not give any feedback to the private parties, in particular in cases where the information submitted by the private party is insufficient to identify the Member States concerned. It would therefore remain unclear to private parties, whether the agency is able to use this data for the purposes for which the private party has shared it, namely to identify the Member States concerned. Moreover, Europol could not request additional data from private parties that would help the agency to support Member States in establishing their jurisdiction. This could result in significant delays, which could ultimately render the information received useless, in spite of its clear relevance for criminal investigations. Moreover, this policy option would not address the third problem driver, because Europol could not act as a service provider for Member States, who want to transmit requests containing personal data to private parties.

Responses on the targeted consultation by way of questionnaire (see annex 11) stated that Europol should be able to request and obtain data directly from private parties with the involvement of national authorities, however some Member States confronted this by taking the position that this power should remain with national authorities, as there are procedural safeguards and accountability mechanisms in place under the national jurisdiction.

The survey above also revealed that there is a wide agreement that, in the possible future regime, it would be important the sharing of information by the private parties concerned to Europol to be in a voluntary basis (i.e. no obligation to share personal data with Europol), to be in full compliance with fundamental rights (including a fair trial) and applicable European legislation on data protection and based on a procedure of consent from the Member States (e.g. from Europol's Management Board). Similarly, the consultation on the Inception Impact Assessment portrayed that participated businesses associations favour voluntary versus mandatory data disclosure under exchange of data with private parties.

The policy option raises the **policy choice** whether Europol should be able to receive and analyse the personal data from private parties to identify the Member States concerned with a view to supporting them in establishing their jurisdiction. This would enhance Europol's capability to support Member States in preventing and combating serious crime and terrorism, but it would result in Europol receiving personal data which has not

been previously assessed by national authorities as to its relevance for Europol's tasks. As it would extend the scope of entities, which could share personal data with Europol to private parties, the assessment of the impact of this policy needs to take full account of Fundamental Rights and notably the right to the protection of personal data.

This policy option is not interdependent with any other policy options related to other objectives.[182] Consequently, the decision on policy options under other objectives do not have an impact on the assessment of this policy option.

This policy option would lead to an increase in the amount of personal data processed by Europol. This may have an impact on other processing activities proposed under this initiative. In particular, some private parties are ready to share large and complex data sets, for example on Child Sexual Abuse Material. Europol's processing of such personal data would therefore have to be subject to the same rules and safeguards that govern the processing of personal data received from other sources.

Policy option 2: allowing Europol to exchange personal data with private parties to establish jurisdiction, as well as to serve as a channel to transmit Member States' requests to private parties (regulatory intervention)

This option would allow Europol to exchange personal data directly with private parties to establish the jurisdiction of the Member States concerned, as well as to serve as a channel to transmit Member States' requests containing personal data to private parties, in addition to the possibility to process personal data received from private parties under policy option 1. This policy option therefore complements policy option 1 and develops it further by allowing Europol not only to receive personal data directly from private parties, but also to share personal data under the conditions set out below.

As explained in section 2.1 above, national authorities cannot effectively analyse multi-jurisdictional or non-attributable data sets through national solutions or through intergovernmental cooperation. Moreover, in terms of **possible EU-level solution**, Europol is best placed to support Member States in analysing multi-jurisdictional or non-attributable data sets from private parties with a view to identifying the Member States, which would be able to establish jurisdiction, as well as to act as a channel for Member States' requests containing personal data to private parties.

Under this option, Europol would be able to:

a) exchange information with a private party as part of a **follow-up** to that private party having shared personal data with the agency in the first place in order to notify that private party about the information missing for the agency to establish the jurisdiction of the Member State concerned; or
b) request personal data indirectly from private parties on its **own initiative**, by sending a reasoned request to the Member State of establishment (or the Member States in which the legal representative is based)[183] to obtain this personal data under its national procedure, in order to establish the jurisdiction of the Member States concerned for a crime falling under Europol's mandate (e.g. when a data set received from a private party requires additional information from another

[182] This means that choosing more 'ambitious' policy options under one objective, could not compensate for choosing less 'ambitious' policy options under another objective.

[183] Hereafter the notion of 'Member State of establishment' will refer to (i) the Member State in which the private party is established, and (ii) the Member State in which the private party has a legal representative.

private party in order to establish the jurisdiction of the Member State concerned); or

c) serve as a **channel** to transmit Member States' requests containing personal data to private parties[184] (e.g. to ensure co-ordination with regards to removal orders and referrals as foreseen by Article 13 of the proposed Regulation on removing terrorist content online).[185]

This option would fully address the first problem driver identified in section 2.1 above, by providing private parties with a contact point to share multi-jurisdictional or non-attributable data sets with law enforcement. Under this option Europol could give feedback to private parties, in particular in cases where the information submitted by the private party is insufficient to identify the Member States concerned. This would enable private parties to assess, whether the agency is able to use this data for the purposes for which the private party has shared it, namely to identify the Member States concerned.

This option would also fully address the second problem driver identified above, by enabling Europol to fully process and enrich the data to identify all Member States concerned, which would be able to establish their jurisdiction. Europol could request additional data that would help the agency to support Member States in establishing their jurisdiction. This would avoid delays, which could ultimately render the information received useless, in spite of its clear relevance for criminal investigations.

Moreover, this policy option would address the third problem driver, because Europol could act as a service provider for Member States, who want to transmit requests containing personal data to private parties. Finally, this policy option would also address the fourth problem driver, as it would address the limitations of the current legal mandate.

The policy option raises the **policy choice** whether Europol should be able to receive and share personal data from private parties to identify the Member States concerned with a view to supporting them in establishing their jurisdiction, as well as to serve as a channel to transmit Member States' requests containing personal data to private parties. This would enhance Europol's capability to support Member States in preventing and combating serious crime and terrorism, but it would result in Europol exchanging personal data directly with private parties. As it would extend the scope of entities, which could exchange personal data with Europol to private parties, the assessment of the impact of this policy needs to take full account of Fundamental Rights and notably the right to the protection of personal data as well as the right to conduct business.

Follow-up request

In cases, in which a private party proactively shares information with Europol as described under option a) above, the agency could confirm the receipt of the personal data and – if necessary – notify the private party about information that might be missing for the agency to establish the jurisdiction of the Member States concerned.

Such notifications, which do not amount to a request, would be subject to strict conditions and safeguards, namely:

- All the safeguards for data subjects set out in the current Europol Regulation,

[184] Such channels set up by Europol should not duplicate existing or future other channels, such as might be set up in the framework for e-evidence.

[185] Article 13 of the Proposal for a Regulation on preventing the dissemination of terrorist content online, COM(2018) 640 final (12.9.2018).

which are applicable to personal data received by Europol from competent authorities, would also apply to personal data received by Europol directly from private parties. These safeguards have been listed above (see policy option 1).

- In addition, an obligation to periodically publish in an aggregate form information on the number of exchanges with private parties could enhance transparency.[186]
- Europol would issue such notifications solely for the purpose of gathering information to establish the jurisdiction of the Member States concerned over a form of crime falling within the Agency's mandate.[187]
- The personal data referred to in these notifications would have to have a clear link with and would have to complement the information previously shared by the private party.
- Such notifications would have to be as targeted as possible,[188] and should refer to the least sensitive data that is strictly necessary for Europol to establish the jurisdiction of the Member State concerned.
- It should be clear that such notifications do not oblige the private party concerned to proactively share additional information.[189]

Such notifications would also enable the Europol to provide the private party with the possibility to assess whether the proactive transmission has served its legitimate interest as intended, and whether it wishes to complement the information already provided.

Own initiative requests

In cases, in which Europol would request personal data held by private parties on its own initiative, as under option b) above, Europol would send a **request to the Member State of establishment** to obtain the information under its applicable national laws.

Such requests would be subject to strict conditions and safeguards, namely:

- Europol would have to provide a reasoned request to the Member State of establishment, which should be as targeted as possible,[190] and should refer to the least sensitive data that is strictly necessary for Europol to establish the jurisdiction of the Member State concerned.
- The **Member States of establishment would assess the request** in the light of the European interest, but based on the **standards of its applicable national law**.[191] This would ensure that the request does not go beyond what national law

---

186 See p.15 of the Opinion of the European Union Agency for Fundamental Rights on Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications (12.2.2019).

187 It is noted that Europol's tasks should be clearly distinguished from those performed by financial intelligence units. Europol will remain limited to processing criminal intelligence with a clear link to forms of crime falling under Europol's mandate. Any cooperation with private parties will remain strictly within the limits of Europol's mandate and will neither duplicate nor interfere with the activities of the FIUs. Europol will continue to cooperate with FIUs via their national units in full respect of their competence and mandate as foreseen under Article 7 (8) of the Europol Regulation and under Articles 11 to 14 of the Directive (EU) 2019/1153.

188 See also p. 6 of the Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (13.2.2019).

189 See p. 38 of the Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Regulation on preventing the dissemination of terrorist content online (12.2.2019)

190 See also p. 6 of the Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (13.2.2019).

191 On the involvement of the Member State of establishment, see also p. 12 of the opinion of the European Data Protection Supervisor: EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters (6.11.2019).

enforcement authorities of said Member State could request without judicial authorisation in terms of the type of information concerned (e.g. subscriber data, access data, traffic data, or content data), as well as with regard to the procedural aspects of the request (e.g. form, language requirements, delay in which the private party would have to reply to a similar request from national law enforcement authorities). This would also ensure that the applicable national thresholds for requesting more sensitive personal data (such as content data) also apply. The Member State of establishment would then request the private party concerned to provide the personal data to Europol. The national requests would have to be subject to the appropriate judicial supervision[192] and provide access to an effective remedy.[193]

The private party would subsequently have to process the request and provide the necessary information. **Article 6(1)(c) GDPR would provide the private party with a lawful basis** for the processing of personal data in such cases.

Upon receiving the personal data, Europol would analyse the personal data, identify the Member States concerned, and share the personal data with these Member States as well as with the Member State of establishment without undue delay.

If the private party does not reply to the request, Europol would inform the Member State concerned without undue delay, who should **enforce its request under the applicable national law**. Member States would have to ensure that there are effective, proportionate and deterrent pecuniary fines available when private parties do not comply with their obligations. Private parties should have the possibility to seek judicial remedy under the applicable national law.

Europol as a channel for Member States' requests

In cases, in which Europol would serve as a channel to transmit Member States' requests containing personal data to private parties, as under point c) above, it would follow the rules and procedures of the underlying legislation allowing for such requests (e.g. proposed Regulation on preventing the dissemination of terrorist content online.)[194]

Such a 'channel-function' would be subject to strict conditions and safeguards, namely:

- The Member State using Europol as a channel for its exchanges with private parties would follow the rules and procedures of the underlying legislation allowing for such exchanges (e.g. proposed Regulation on preventing the dissemination of terrorist content online).[195]
- The Member States would provide assurance that its request is in line with their applicable laws, which would have to provide sufficient safeguards to the affected fundamental rights, including access to an effective remedy.[196]

Relation to other EU initiatives

192 See p. 23 of the Opinion of the European Union Agency for Fundamental Rights on Proposal for a Regulation on preventing the dissemination of terrorist content online (12.2.2019).

193 See p. 28 of the Opinion of the European Union Agency for Fundamental Rights on Proposal for a Regulation on preventing the dissemination of terrorist content online (12.2.2019).

194 COM(2018) 640 final (12.9.2018).

195 COM(2018) 640 final (12.9.2018).

196 See p. 28 of the Opinion of the European Union Agency for Fundamental Rights on Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications (12.2.2019).

This policy option should further create synergies and avoid overlaps with other legislative initiatives.

Once adopted, the **e-evidence package**[197] will provide national law enforcement and judicial authorities with the possibility of sending European Production Order Certificates and European Preservation Order Certificates to service providers or its legal representatives to obtain electronic evidence for criminal investigations.[198] Therefore, the present initiative to enable Europol to exchange personal data with private parties would not duplicate the tools foreseen under the e-evidence initiative, but rather complement them.

Moreover, the legislation on the removal of **terrorist content online** will require co-ordination with regards to removal orders and referrals as foreseen by Article 13 of the proposed Regulation on removing terrorist content online. This policy objective is complementary in that regard, as it would enable Europol to host the necessary IT infrastructure for such exchanges.

Similarly, this policy choice could be complementary to the Commission's EU Strategy for a more effective fight against **child sexual abuse**.[199] This strategy foresees setting up a European Centre to prevent and counter child sexual abuse, and a strong involvement of Europol in that regard. The legal form for such a centre still needs to be determined, but if it would be established under private law, this policy option would enable Europol to effectively cooperate with this centre in order to support investigations into child sexual abuse.

Policy option 3: allowing Europol to directly query databases managed by private parties in specific investigations

In addition to the possibility to receive and request data from private parties under option 2, policy option 3 would **allow Europol to directly query databases managed by private parties** in specific investigations. This policy option therefore complements policy option 1 and 2 and develops it further by allowing Europol not only to receive and share personal data with private parties, but also to 'retrieve' personal data directly from data bases managed by private parties. In other words, Europol would directly submit requests that would allow it to automatically obtain information from certain databases managed by private parties that contain information relevant for criminal investigations and proceedings. This policy option has been discussed in the context of the Study on the practice of direct exchanges of personal data between Europol and private parties.[200]

As explained in section 2.1 above, national authorities cannot effectively analyse multi-jurisdictional or non-attributable data sets through national solutions or through intergovernmental cooperation. Moreover, in terms of **possible EU-level solution**, Europol is best placed to support Member States in analysing multi-jurisdictional or non-attributable data sets from private parties with a view to identifying the Member States, which would be able to establish jurisdiction, as well as to act as a channel for Member States request containing personal data to private parties.

197 COM(2018) 225 final and 226 final

198 This possibility will apply irrespective of the location of the establishment of the provider or the storage of the information as long as they offer their services in the European Union

199 COM(2020) 607 final.

200 Milieu, 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 (not yet published) (see annex 4 for main findings).

Under this option, Europol would request access to private parties' databases in specific investigations, after having obtained the approval of the Member State in which the private party is established. Europol would then have the possibility to make several queries in those data bases for the purpose of the specific investigation. This policy option would not only guarantee swift access to relevant personal data for European law enforcement, but it would also relieve private parties from the administrative burden of processing individual requests.

As options 1, 2 and 3 are cumulative, this policy options would – like option 2 - also address all three problem drivers. In particular, it would further strengthen the response to the third problem driver, by enabling Europol to directly query data bases managed by private parties in order to support Member States in specific investigations.

This policy option raises the **policy choice** whether Europol should be able not only to exchange personal data with private parties, but also to directly retrieve personal data from data bases held by private parties to identify the Member States concerned with a view to supporting them in establishing their jurisdiction. This would enhance Europol's capability to support Member States in preventing and combating serious crime and terrorism, but it would result in Europol directly retrieving personal data from data bases held by private parties. As it would extend the scope of entities, which could exchange personal data with Europol to private parties, and allow Europol to directly query their data bases, the assessment of the impact of this policy needs to take full account of Fundamental Rights and notably the right to the protection of personal data as well as the right to conduct business.

5.2.2 Enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with Fundamental Rights

Policy option 4: clarifying the provisions on the purposes of information processing activities and enabling Europol to analyse large and complex datasets

This policy option consists of **clarifying the provisions on the purposes of information processing activities** of the Europol Regulation to enable Europol to effectively fulfil its mandate in full compliance with Fundamental Rights, including by way of **analysing large and complex datasets**. It would provide a clear legal basis and the necessary safeguards for such data processing, addressing the fact that criminals and terrorist use information and communications technology to communicate among themselves and to prepare and conduct their criminal activity. The policy option is inspired by the EDPS decision on Europol's big data challenge.

This regulatory intervention would maintain the obligation on Europol to limit its data processing to the specific categories of data subjects listed in annex II of the Europol Regulation (i.e. persons related to a crime for which Europol is competent), while clarifying that:

- when Europol receives personal data, it might carry out, in case of doubt and prior to any further data processing, an **initial processing of such data (e.g. by way of collation[201]), including a check against data held in its databases, for the sole purpose of verifying** if the data falls into the categories of data subjects set out in annex II of the Europol Regulation. This initial data processing would constitute a **pre-analysis**, prior to Europol's data processing for cross-checking,

[201] I.e. the pre-analysis phase where unstructured data received is being organised and structured into a format from which it can be analysed.

strategic analysis, operational analysis or exchange of information.[202] When it comes to high volumes of personal data received in the context of a specific investigation, this pre-analysis might involve the use of technology and might exceptionally require more time for the verification. This would provide the **necessary legal clarity** for Europol to process personal data in compliance with the requirement related to the specific categories of data subjects listed in annex II of the Europol Regulation.

- when Europol **analyses large and complex data sets by way of digital forensics to support a criminal investigation** in a Member State, it may **exceptionally process and store data of persons who are not related to a crime**. Such data processing would only be allowed where, due to the nature of the large dataset, it is necessary for the operational analysis to also process data of persons who are not related to a crime, and only for as long as it supports the criminal investigation for which the large dataset was provided. This **narrow and justified exception** would extend the grounds for data processing by Europol. Moreover, upon request of the Member State that provided the large and complex dataset to Europol in support of a criminal investigation, Europol may store that dataset and the outcome of its operational analysis beyond the criminal investigation. Such data storage would only be possible for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as it is necessary for the judicial proceedings related to that criminal investigation. During that period, the data would be blocked for any other processing.

This policy option would **address the structural legal problems** identified by the EDPS in its decision on Europol's big data challenge. By way of an initial data processing (pre-analysis phase), it would enable Europol to verify, in case of doubt, if it is authorised to analyse the personal data it received in the context of the prevention and countering of crimes falling under Europol's mandate. It would also address the problems related to the analysis of large and complex datasets by Europol. In doing so, the policy option would address all three problem drivers identified in section 2.2 above.

The policy option raises the **policy choice** whether Europol should be able to continue to analyse large and complex datasets, and in turn exceptionally process data of persons who do not have any connection to a crime. This would enhance Europol's capability to support Member States in preventing and combating serious crime and terrorism, but at the same limit the exercise of Fundamental Rights, notably the right to the protection of personal data.

As the policy option would extend the scope of persons whose data may be processed by Europol on an exceptional basis, **the assessment of the impact of this policy option needs to take full account of Fundamental Rights and notably the right to the protection of personal data**.

Policy option 5: introducing a new category of data subjects whose data Europol can process

This policy option consists of **introducing a new category of data subjects** in annex II of the Europol Regulation covering persons who do not have any connection to a crime. It would address the fact that criminals and terrorist use information and communications technology to communicate among themselves and to prepare and conduct their criminal

[202] See Article 18(2) of Regulation (EU) 2016/794.

activity, and that digital forensics inevitably involves the processing of data of persons who do not have any connection to the crime under investigation. This policy option is a genuine alternative to policy option 4.

This regulatory intervention would maintain the obligation on Europol to limit its data processing to categories of data subjects listed in annex II. However, this policy option would significantly extend the scope of persons covered by these categories to basically all persons. At the same time, the policy option would keep a distinction between suspects, convicted persons and potential future criminals, contacts and associates, victims, witnesses and informants of criminal activities on the one hand, and persons not related to any crime on the other hand. It would set out specific requirements and safeguards for the processing of persons falling into this new category of data subjects without any connection to a crime.

This policy option would **address the structural legal problem** related to the analysis of large and complex datasets by Europol, as identified by the EDPS in its decision on Europol's big data challenge. As the policy option would enable Europol to process the data of any person, it would de facto remove the requirement that limits Europol's data processing to certain categories of data subjects only, and hence the requirement that is at the heart of the big data challenge. In doing so, the policy option would address all three problem drivers identified in section 2.2 above.

The policy option raises the **policy choice** whether Europol should be allowed to process data on a structural basis of persons who do not have any connection to a crime. This would enhance Europol's capability to support Member States in preventing and combating serious crime and terrorism, but at the same limit the exercise of Fundamental Rights, notably the right to the protection of personal data.

As the policy option would significantly extend the scope of persons whose data may be processed by Europol on a structural basis, **the assessment of the impact of this policy option needs to take full account of Fundamental Rights and notably the right to the protection of personal data**.

5.2.3 Enabling Member States to use new technologies relevant for law enforcement

Policy option 6: regulating Europol's support to the EU security research programme, the innovation lab at Europol, and Europol's support to the EU innovation hub

With a view to fulfil the objective of enabling Member States to use new technologies relevant for law enforcement, **this policy option would**: (1) provide Europol with a mandate to support the Commission in the implementation of Union framework programmes for research and innovation activities that are relevant for law enforcement; (2) regulate the existing innovation lab at Europol; as well as (3) regulate Europol's support to the EU innovation hub[203] for internal security. This policy option is inspired by

[203] During the workshop on the revision of Europol Regulation, organised as part of the consultation (see Annex 11) participants expressed their overall support of the innovation hub, which is of particular importance in the digital age. Furthermore, in the context of semi-structured interviews with stakeholders conducted as part of the consultation (see Annex 11), participating representatives of the innovation and research communities expressed strong support for enhancing the role of Europol on fostering innovation and supporting the management of research relevant for law enforcement. Participants also highlighted the importance of involving all Member States in this, referring to the risk that close cooperation between Europol and more advanced Member States could otherwise lead to even bigger gaps between forerunners and less advanced Member States when it comes to

the competences the European Border and Coast Guard Agency[204] has on research and innovation relevant for border management, as well as by calls from the European Parliament[205] and the Council[206] to involve Europol in security research.

First, this policy option would provide Europol with a legal basis, and hence the necessary resources, to assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes (notably the upcoming **Horizon Europe)**[207] for research and innovation activities that are relevant for law enforcement. The policy option would therefore support and complement the EU funding for security research, creating synergies and helping the EU funding to develop its full potential. Notably, with the aim to ensure that the consolidated needs of law enforcement are adequately addressed, Europol would assist the Commission in the entire **cycle of EU funding for security research**, i.e. by:

- supporting the setting of priorities;
- contributing to the definition of the calls;
- participating in the evaluation process;
- steering relevant successful projects, in order to help ensure that technologies developed in the framework of the selected topics can be applied to concrete and meaningful law enforcement tools; and
- supporting the dissemination and facilitating the uptake of the results of the projects.

Second, this policy option would provide a clear legal basis, and hence the necessary resources, for the work of the **Europol innovation lab**, with a focus on:

- proactively monitoring research and innovation activities relevant for law enforcement;
- supporting (groups of) Member States in their work on innovative technologies to develop tools and provide solutions to serve the operational needs of law enforcement;
- implementing its own innovation projects regarding matters covered by Europol's legal mandate, covering notably the uptake of applied research (prototypes) towards deployment, and the work towards a final product available for the use by law enforcement, based on specific authorisations for each such pilot project;
- supporting the uptake of the results of innovation projects, including by disseminating their results to authorised bodies, analysing their implementation, and formulating general recommendations, including for technical standards for interoperability purposes and best practices.
- maintaining and using networks for outreach to industry, civil society, international organisations and academia;
- producing technology foresight and providing assessment on the risks, threats and opportunities of emerging technologies for law enforcement; and
- supporting the screening of specific cases of foreign direct investments that concern contract providers of technologies and software for police forces, in line with the Regulation on establishing a framework for the screening of foreign

innovation and research relevant for law enforcement.

204 See Article 66 of Regulation (EU) 2019/1896.

205 European Parliament resolution of 12 December 2018 on findings and recommendations of the Special Committee on Terrorism.

206 https://www.consilium.europa.eu/media/41015/st12837-en19_both-days_edited.pdf.

207 COM(2018) 435 final (7.6.2018).

direct investments into the Union.[208]

Moreover, by promoting the development of EU tools to counter serious crime and terrorism, the Europol' innovation lab would take account of the cross-border dimension of many of today's security threats, as well as the need for cross-border cooperation among law enforcement authorities to tackle these threats. Europol's innovation lab would not be involved in fundamental research.

Third, under this policy option, Europol would also provide secretarial support to the **EU innovation hub for internal security** that is being set up among EU agencies and the Commission's Joint Research Centre, based on their existing legal mandates. The EU innovation hub will serve as a collaborative network of their innovation labs. Responding to a request by the Council, the EU innovation hub will primarily be a coordination mechanism to support the participating entities in the sharing of information and knowledge, the setting up of joint projects, and the dissemination of finding and technological solutions developed, as announced in the EU Security Union Strategy.

This policy option would **address the gap on the coordination of research and innovation needs on the side of law enforcement**, as part of the problem of gaps on innovation and research relevant for law enforcement. This policy option would therefore address the part of the considerable security challenges posed by the abuse of modern technologies by criminals and terrorists. In doing so, the policy option would address the first problem driver (not all Member States are well equipped to exploit fully the advantages of new technologies for law enforcement) and part of the second problem driver (gap on the coordination of research and innovation needs on the side of law enforcement) identified in section 2.3 above.

The policy option raises the **policy choice** whether Europol should be able to support Member States in fully exploiting the advantages of new technologies for fighting serious crime and terrorism, including by assisting the Commission in implementing the Union framework programmes for research and innovation relevant for law enforcement.

The policy option would not provide any new legal grounds for Europol for the processing of personal data.

Policy option 7: enabling Europol to process personal data for the purpose of innovation in areas relevant for its support to law enforcement

This policy option would build on policy option 6 and include all aspects listed above under that option. This policy option is therefore not a genuine alternative to policy option 6, but would complement the latter.

This policy option would enable Europol to **process personal data**, including high volumes of personal data, **for the purpose of innovation in areas relevant for its support to law enforcement**. This would include the training, testing and validation of algorithms for the development of tools, including AI-based tools, for law enforcement. The policy option is inspired by the call from the Council that Europol should "*drive innovation, including by developing common technological solutions for member states in the field of internal security.*"[209]

The policy option would consist of a regulatory intervention to amend the purposes of

[208] Regulation (EU) 2019/452.
[209] https://www.consilium.europa.eu/media/41015/st12837-en19_both-days_edited.pdf.

data processing at Europol, introducing a legal ground for the processing of personal data for research and innovation regarding matters covered by Europol's mandate. The policy option would not, however, address the possible subsequent use of any specific technological application by Europol or any Member State.

This policy option would **address the need for an EU-level capacity to train, test and validate algorithms for the development of tools, including AI-based tools, for law enforcement**, in full compliance with Fundamental Rights and with the necessary transparency. The processing of personal data by Europol for research and innovation activities would be limited to personal data that fall into one of the data categories of Annex II of the Europol Regulation, i.e. personal data that is linked to a crime. It would address an important part of the problem of gaps on innovation and research relevant for law enforcement. In doing so, the policy option would address the considerable security challenges posed by the abuse of modern technologies by criminals and terrorists. As the policy option would build on policy option 6 and include all aspects listed above under that option, it would address all problem drivers identified in section 2.2. above.

The policy option would enable Europol to participate in the roll-out of the **European Strategy for Data,**[210] thus creating important synergies. The processing of personal data is envisaged to take place, under strict conditions, in the European Security Data Space to be established under the Strategy and co-funded by the Digital Europe Programme. Europol would be a major stakeholder in the establishment and use of the European Security Data Space. The policy option also takes account of the Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust, which sets out that AI can equip "*law enforcement authorities with appropriate tools to ensure the security of citizens, with proper safeguards to respect their rights and freedoms*".[211]

The policy option would also help strengthening **technological sovereignty and strategic autonomy** of Member States and the EU in the area of internal security, which is a fundamental public interest and a matter of national security.

This policy options raises the **policy choice** whether Europol should be able to process personal data for the training, testing and validation of algorithms for the development of tools, including AI-based tools, for law enforcement, in full compliance with Fundamental Rights and with the necessary transparency. This would considerably enhance Europol's capability to support Member States in using new technologies relevant for law enforcement, but at the same limit the exercise of Fundamental Rights, notably the right to the protection of personal data.

As the policy option includes the processing of personal data for innovation and research, **the assessment of the impact of this policy option needs to take full account of Fundamental Rights and notably the right to the protection of personal data**.

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

This chapter assesses all policy options identified in section 5.2 against the baseline scenario. Given that the baseline scenario is evidently unsuited to address the problems identified in chapter 2 on the problem definition, this impact assessment will not assess the baseline scenario any further.

---

210 COM(2020) 66 final (19.2.2020).
211 COM(2020) 65 final (19.2.2020), p. 2.

Given that many policy options concern a change in Europol's legal basis, most of the assessment of impacts are of a legal nature which is not suitable for quantification. Given the role of Europol as EU agency for law enforcement cooperation, the main impact of the policy options assessed in this chapter will be on citizens, national authorities and EU bodies, with limited impact on businesses. A notable exception to this are the policy options under *Objective I* on enabling effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals.

As the processing of personal data is an important aspect of the support that Europol provides to national law enforcement authorities, and hence of many of the policy options assessed in this impact assessment, this chapter puts a particular focus on the assessment of the impact on Fundamental Rights. This detailed assessment is based on an even more comprehensive assessment of the policy options in terms of their limitations on the exercise of Fundamental Rights as set out in annex 5.

6.1 Enabling effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals

Policy option 1: allowing Europol to process data received directly from private parties

Expected impact of policy option 1[212]
1) impact on citizens [+]
• Positive impact to the security of the European citizens and societies. Europol could receive and analyse multi-jurisdictional and non-attributable data sets to establish the jurisdictions of the Member States concerned. This would enable Member States to more effectively counter crimes, including cybercrime, financial crime, trafficking in human beings, and child sexual abuse, as it would avoid delays and data losses associated with the current system.
2) impact on national authorities [+]
• Positive impact on national authorities, which could more efficiently combat serious crime and terrorism, because Europol – upon receiving a non-attributable or multi-jurisdictional data set from private parties - would identify the personal data relevant for their jurisdiction, analyse it in the context of the wider data set, and enrich with information which is already available in its data bases put may not be available at national level.
3) impact on EU bodies [+]
• While this policy option would increase the workload for Europol, it would have a positive impact on the Agency's ability to effectively perform its tasks of supporting Member States by identifying the relevant jurisdiction of the Member States concerned in cases, in which private parties share personal data proactively with the agency.
4) impact on businesses [+]
• Positive impact on businesses, as private parties would spend less resources on identifying the relevant jurisdiction, because they would be able to share multi-jurisdictional or non-attributable data sets with Europol, who would take over the task of identifying the Member States concerned. • However, private parties would still have to devote additional resources to verifying and replying to national requests Member States. • Also, private parties would still bear risk of being liable to damage claims from data

[212] The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

subjects, which is inherent in the voluntary sharing of data.

5) impact on Fundamental Rights [-]

a) identification of Fundamental Rights limited by the measure

- The policy options limits the Fundamental Right to the protection of personal data as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to respect for private life (Article 7 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.
- This policy option does not adversely affect the essence of the Fundamental Rights to the protection of personal data and to respect for private life, as transfers would be limited to situations where they are in the legitimate interest of the private party sharing the data.
- Subsequent processing would be limited to legitimate purposes under Europol's mandate and subject to adequate safeguards set out in the Europol Regulation.

b) assessment of necessity

- The policy option is **genuinely effective** to achieve the specific objective of improving Europol's ability to support Member States in identifying cases and information with relevance for their respective jurisdictions, in particular where the cases rely on the analysis of multi-jurisdictional data sets, or data sets where the jurisdiction of the data subjects is difficult to establish, and therefore also essential to the fight against serious crime and terrorism as objectives of general interest in EU law.
- Enabling Europol to receive personal data directly from private parties **effectively contributes to achieve these objectives**, as it provides private parties with a central point of contact, when they see the need to share personal data with unclear or multiple jurisdiction.
- This policy option addresses the problems that private parties and national law enforcement face in identifying the jurisdiction that is responsible for the investigation of a crime committed with the abuse of cross-border services. It does so **more effectively** than non-legislative options such as best practices. Indeed, **best practices would be less intrusive but insufficient** to address the problem. Also, national authorities cannot effectively investigate such crimes through national solutions, or by way of intergovernmental cooperation.[213] Likewise, existing rules on the exchange of personal data between Europol and private parties, even if their application is reinforced, are insufficient to address the problem.[214] In particular, private parties cannot effectively share multi-jurisdictional or non-attributable data sets indirectly with Europol via national law enforcement authorities, as they focus on identifying data relevant for their respective jurisdictions, and are not well placed to identify personal data relevant to other jurisdictions. Such an indirect way of sharing personal data entails risks of delays and even data loss.
- As there are no other effective but less intrusive options, the policy option is **essential and limited to what is absolutely necessary** to achieve the specific objective of enabling Europol to cooperate effectively with private parties, and hence the fight against serious crime and terrorism as objectives of general interest in EU law.

c) assessment of proportionality

- The policy option affects data subjects who are associated with a serious crime falling within Europol's mandate, such as criminals, suspects, witnesses and victims, and whose personal data private parties share with Europol. The policy option raises **collateral intrusions** as private parties may share data on data subjects who are not associated with a crime for which Europol is competent, and hence of persons other than individuals targeted by the measure.

213 See Chapter 2.1 of the impact assessment on the problem description.

214 See Chapter 2 of the impact assessment on the problem description, the problem drivers, and how the problem will evolve.

This risk will be mitigated with the introduction of necessary safeguards described below.

- The policy option does **not impose a disproportionate and excessive burden** on the persons affected by the limitation, in relation to the specific objective of enabling Europol to cooperate effectively with private parties and hence the fight against serious crime and terrorism as objectives of general interest in EU law, as Europol's data protection regime will provide for adequate safeguards (see step 4).
- No potential harmful effect of the policy option on other Fundamental Rights has been identified, as the impact of this policy option is limited to impacts on the right to the protection of personal data and the respect for private life.
- Weighing up the intensity of the interference with the Fundamental Rights to the protection of personal data and to respect for private life as described under step 2 with the legitimacy of the objectives to fight serious crime and terrorism as objectives of general interest in EU law, the policy option constitutes a **proportionate response** to the need to solve the problem resulting from limits in Europol's ability to effectively support Member States in countering crimes prepared or committed using cross-border services offered by private parties.
- However, in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of enabling Europol to effectively cooperate with private parties, a **number of safeguards are required**.

d) necessary safeguards

- All the safeguards set out in the rules applicable to personal data, which Europol receives from competent authorities, would also apply to personal data, which Europol receives directly from private parties.[215]
- In particular, upon receiving the data, Europol would process the personal data only temporarily for as long is necessary to determine whether the data is relevant to its tasks. If the data is not relevant for its tasks, Europol would delete the data after six months. Only if the data is relevant to its tasks, would Europol process the data further (Article 18 (6) Europol Regulation). In practice, this would mean that Europol would delete personal data on data subjects, which are not associated with a serious crime falling within Europol's mandate. There should be a high threshold with clear criteria and strict conditions for Europol to determine whether data received from private parties is relevant for Europol's objectives and should become part of Europol's operational data.
- Furthermore, Europol would be limited in the way it can process special categories of data (e.g. on ethnicity or religious beliefs) and different categories of data subjects (e.g. victims and witnesses) (Article 30 Europol Regulation).
- Moreover, Europol would not be allowed to process the data for longer than necessary and proportionate, and within the time-limits set by the Europol Regulation (Article 31).
- Also, the Europol Regulation would ensure the necessary data subject rights, in particular a right of access (Article 36), and a right to rectification, erasure and restriction (Article 37).
- In addition, the Europol Regulation would ensure the possibility for an individual to pursue legal remedies (Article 47 and 48 Europol Regulation).

6) effectiveness in meeting the policy objectives [+]

- This policy option would partly address the objective of enabling effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals and would therefore have an EU added value.
- Europol could act as a point of contact when private parties want to share multi-jurisdictional or non-attributable data sets.

[215] See p. 45 of the Opinion of the European Union Agency for Fundamental Rights on Interoperability and fundamental rights implications (11.4.2018).

• Europol could process the data to identify the Member States concerned, but could not request additional data necessary for this purpose, which could result in delays and could ultimately render the information received useless. • Also, Europol could not act as a service provider for Member States, who want to transmit requests containing personal data to private parties.
7) efficiency in meeting the policy objectives [+]
• As the policy option would extend the scope of entities, which can share personal data with Europol, to private parties. It would hence increase the amount of personal data that Europol would further process and store, it would lead to addition workload and costs for the agency. • At the same time, under this policy option Europol could more efficiently support Member States in preventing and combatting serious crime and terrorism, because of the economies of scale of performing such tasks at EU level.
8) legal/technical feasibility [++]
• This policy option would require changes to the Europol regulation. • This policy option would be technically feasible.
9) political feasibility [+]
• The policy option would only partly meet the Council Conclusions of December 2019 calling for Europol to be able to receive and request personal data directly from private parties.[216] • The European Parliament will require detailed justification for necessity, as well as data protection safeguards.
10) coherence with other measures [-]
• This policy option would not complement other Commission initiatives such as the Commission proposal for legislation on preventing the dissemination of terrorist content online,[217] as it would not enable the agency to act as a channel for Member States' requests.

Policy option 2: allowing Europol to exchange personal data with private parties to establish jurisdiction, as well as to serve as a channel to transmit Member States' requests to private parties

Expected impact of policy option 2[218]
1) impact on citizens [++]
• Very positive impact to the security of the European citizens and societies. As Europol could exchange data with private parties beyond just receiving data (option 1), the agency would establish the jurisdictions of the Member States concerned more effectively than under option 1. The risk of delays and data losses would be further reduced. In addition, Europol serving as a channel to transmit Member States request to private parties, would also benefit Member States ability to effectively counter crimes.
2) impact on national authorities [++]
• Very positive impact on national authorities. Member States would devote some resources on dealing with Europol's own-initiative requests, but would benefit significantly from Europol's improved ability to analyse large multi-jurisdictional or non-attributable data sets for data relevant to their jurisdiction. Europol would more efficiently analyse and enrich such

216 Council Conclusions Europol's cooperation with Private Parties, Document 14745/19, 2 December 2019.

217 Proposal for a regulation on preventing the dissemination of terrorist content online, COM(2018) 640.

218 The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

data, because it would be able not only to receive personal data from private parties, but also to engage in follow-up exchanges with a view to identifying the Member States concerned.

- In addition, Member States would devote less resources on transferring requests to private parties. When transmitting such requests, law enforcement authorities usually need to identify the correct interlocutor within the organisation, comply with substantive and formal conditions for the request, and identify as genuine law enforcement authorities. This can be a complex and time consuming procedure, as each private party may have different rules and procedures for dealing with such requests. Europol can support Member States, by establishing simplified and streamlined procedures with a number of private parties and by certifying the genuineness of such requests.

3) impact on EU bodies [++]

- While this policy option would further increase the workload for Europol compared to Option 1, it would have a very positive impact on the Agency's ability to effectively perform its tasks of supporting Member States by identifying the relevant jurisdiction of the Member States concerned.
- In addition, Europol could support Member States in transferring requests containing personal data to private parties.

4) impact on businesses [+]

- Positive impact on businesses, as private parties would spend less resources on identifying the relevant jurisdiction, because they would be able to share multi-jurisdictional or non-attributable data sets with Europol, who would take over the task of identifying the Member States concerned.
- Private parties spend less resources to verifying and replying to national requests Member States, where Member States transmit such requests through channels set up by Europol.
- Moreover, private parties would be less exposed to the risk of being liable to damage claims from data subjects, if they share personal data with Europol on the basis of binding requests from the Member State in which they are established.
- Private parties would be less exposed to reputational damages from criminals abusing their services.

5) impact on Fundamental Rights [-]

a) identification of Fundamental Rights limited by the measure

- The policy options limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). The policy option also limits the fundamental rights of private parties to **conduct business** (Article 16 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.
- The policy option does **not adversely affect the essence** of the Fundamental Right to protection of personal data, respect for private life and the right to conduct business, as exchanges would be limited to situations, in which Europol requires additional information in order to process data it has previously received, or upon a request from a Member State, for legitimate purposes under Europol's mandate and subject to adequate safeguards enshrined in the Europol Regulation.

b) assessment of necessity

- The policy option is **genuinely effective to achieve the specific objective** of enabling Europol to improve Europol's ability to support Member States in identifying cases and information with relevance for their respective jurisdictions, in particular where the cases rely on the analysis of multi-jurisdictional data sets, or data sets where the jurisdiction of the data

subjects is difficult to establish, and to be able to serve as a channel to transmit Member States' requests containing personal data to private parties, and therefore also essential to fight against serious crime and terrorism as objectives of general interest in EU law

- Enabling Europol to exchange personal data directly with private parties to establish the jurisdiction of the Member States concerned, as well as to serve as a channel to transmit Member States' requests containing personal data to private parties (in addition to the possibility to process personal data received from private parties under policy option 1) **effectively contributes to achieve this objective**, as it enables Europol to obtain additional information necessary to establish the jurisdiction of the Member States concerned, and to serve as a channel or Member States' requests to private parties.
- This policy option addresses the problems that Member States and private parties face in identifying the jurisdiction that is responsible for the investigation of a crime committed with the abuse of cross-border services, and when private parties receive request from law enforcement authorities of another country, **more effectively than non-legislative options** such as best practices. Indeed, **best practices would be less intrusive but insufficient to address the problem**.
- Likewise, **existing rules** on the exchange of personal data between Europol and private parties, even if their application is reinforced, are **insufficient** to address the problem. The current system does not allow for a point of contact for private parties in multi-jurisdictional cases or in cases where the jurisdiction is unclear, nor can it ensure that this type of data is shared with other Member States concerned.[219]
- Notably, private parties cannot effectively share multi-jurisdictional or non-attributable data sets indirectly with Europol via national law enforcement authorities, as they focus on identifying data relevant for their respective jurisdictions, and are not well placed to identify personal data relevant to other jurisdictions. Such an indirect way of sharing personal data entails risks of delays and even data loss. Moreover, the current system does not allow for Europol to serve as a channel for Member States requests for private parties.
- As there are no other effective but less intrusive options, the policy option is **essential and limited to what is absolutely necessary** to achieve the specific objective of enabling Europol to cooperate effectively with private parties, and hence the fight against serious crime and terrorism as objectives of general interest in EU law.

c) assessment of proportionality

- The policy option **corresponds to the identified need and partially solves the problem** of Europol's inability to support Member States in countering crimes prepared or committed using cross-border services offered by private parties. The policy option is effective and efficient to fulfil the objective.
- This policy option affects data subjects who are associated with a serious crime falling within Europol's mandate (as discussed under policy option 1), as well as data subjects, which are subject to a criminal investigation at national level, but not necessarily associated with a crime falling within Europol's mandate.
- In both cases, the policy option raises **collateral intrusions** as Europol may process personal data of data subjects, which are not associated with a serious crime falling within Europol's mandate. This risk will be mitigated with the introduction of necessary safeguards as described below.
- This policy option also affects private parties' right to conduct business, insofar as Europol would request personal data indirectly from private parties on its own initiative, by sending a

[219] See chapter 2 of the impact assessment on the problem description, the problem drivers, and how the problem will evolve.

reasoned request to the Member State of establishment (or the Member States in which the legal representative is based)[220] to obtain this personal data under its national procedure. This risk will also be mitigated with the introduction of necessary safeguards as described below.

- The policy option does **not impose a disproportionate and excessive burden** on the persons affected by the limitation, namely data subjects who are not associated with a crime for which Europol is competent, in relation to the specific objective of enabling Europol to cooperate effectively with private parties and hence the fight against serious crime and terrorism as objectives of general interest in EU law.
- No potential harmful effect of the policy option on other Fundamental Rights has been identified, as the impact of this policy option is limited to impacts on the right to the protection of personal data, the respect for private life, and the right to conduct business.
- Weighing up the intensity of the interference with the Fundamental Rights of data subjects regarding the protection of personal data and to respect for private life, as well as with the Fundamental Rights of private parties' right to conduct business with the legitimacy of the objectives to fight against serious crime and terrorism as objectives of general interest in EU law, the policy option constitutes a **proportionate response to the need to solve the problem**, that Member States cannot effectively counter crimes prepared or committed using cross-border services offered by private parties.
- However, in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of enabling Europol to effectively cooperate with private parties, a **number of safeguards are required**.

d) necessary safeguards

- All the safeguards for data subjects set out in the current Europol Regulation, which are applicable to personal data received by Europol from competent authorities, would also apply to personal data received by Europol directly from private parties. These safeguards have been listed above (see policy option 1 above). In addition, an obligation to periodically publish in an aggregate form information on the number of exchanges with private parties could enhance transparency.[221]
- As regards follow-up exchanges, the policy option would introduce additional safeguards. Europol would issue such notifications solely for the purpose of gathering information to establish the jurisdiction of the Member State concerned over a form of crime falling within the Agency's mandate,[222] the personal data referred to in these notifications would have to have a clear link with and would have to complement the information previously shared by the private party. Such notifications would have to be as targeted as possible,[223] and should refer to the least sensitive data that is strictly necessary for Europol to establish the jurisdiction of the Member State concerned. It should be clear that such notifications do not oblige the private party concerned to proactively share additional information.[224]

---

220 Hereafter the notion of 'Member State of establishment' will refer to (i) the Member State in which the private party is established, and (ii) the Member State in which the private party has a legal representative.

221 See p.15 of the Opinion of the European Union Agency for Fundamental Rights on Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications (12.2.2019).

222 It is noted that Europol's tasks should be clearly distinguished from those performed by financial intelligence units. Europol will remain limited to processing criminal intelligence with a clear link to forms of crime falling under Europol's mandate. Any cooperation with private parties will remain strictly within the limits of Europol's mandate and will neither duplicate nor interfere with the activities of the FIUs. Europol will continue to cooperate with FIUs via their national units in full respect of their competence and mandate as foreseen under Article 7 (8) of the Europol Regulation and under Articles 11 to 14 of the Directive (EU) 2019/1153.

223 See also p. 6 of the Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (13.2.2019).

224 See p. 38 of the Opinion of the European Union Agency for Fundamental Rights on the Proposal for a

- As regards own-initiative requests, Europol would have to provide a reasoned request to the Member State of establishment, which should be as targeted as possible,[225] and should refer to the least sensitive data that is strictly necessary for Europol to establish the jurisdiction of the Member State concerned. The Member State of establishment would assess the request in the light of the European interest, but based on the standards of its applicable national law.[226] This would ensure that the request does not go beyond what the national law enforcement authorities of this Member State could request without judicial authorisation in terms of the type of information requested (e.g. subscriber data, access data, traffic data, or content data), as well as with regard to the procedural aspects of the request (e.g. form, language requirements, delay in which the private party would have to reply to a similar request from national law enforcement authorities). This would also ensure that the applicable national thresholds for requesting more sensitive personal data (such as content data) also apply. The national requests would have to be subject to the appropriate judicial supervision[227] and provide access to an effective remedy.[228]
- As regards Europol serving as a channel for Member States requests to private parties, the Member State would follow the rules and procedures of the underlying legislation allowing for such requests (e.g. proposed Regulation on preventing the dissemination of terrorist content online[229]), and provide assurance that its request is in line with its applicable laws, which would have to provide sufficient safeguards to the affected fundamental rights, including access to an effective remedy.[230]

6) effectiveness in meeting the policy objectives [++]

- This policy option would be fully effective in addressing the objective of enabling effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals. It would therefore have a clear EU added value.
- It would enable Europol to send and receive personal data from private parties and to act as a channel for Member States' request to private parties containing personal data.
- At the same time, this policy option would provide for sufficient safeguards for fundamental rights, in particular data protection rights.

7) efficiency in meeting the policy objectives [++]

- This policy option would lead to additional costs for the Agency, in particular because of the need for additional resources to deal with an increase in the amount of personal data from private parties, to deal with follow-up exchanges with private parties about missing information, to deal with own-initiative requests to Member States of establishment, and to set up and maintain IT infrastructure to act as a channel for Member States' requests to

Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications (12.2.2019)

225 See also p. 6 of the of the Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (13.2.2019).

226 On the involvement of the Member State of establishment, see also p. 12 of the opinion of the European Data Protection Supervisor: EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters (6.11.2019).

227 See p. 23 of the Opinion of the European Union Agency for Fundamental Rights on Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications (12.2.2019).

228 See p. 28 of the Opinion of the European Union Agency for Fundamental Rights on Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications (12.2.2019).

229 COM(2018) 640 final (12.9.2018).

230 See p. 28 of the Opinion of the European Union Agency for Fundamental Rights on Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications (12.2.2019).

private parties. • At the same time, under this policy option Europol could much more efficiently support Member States in preventing and combatting serious crime and terrorism, because of the economies of scale of performing such tasks at EU level.
8) legal/technical feasibility [+]
• This policy option would require changes to the Europol regulation. • Moreover, Member States would need to take the necessary steps to ensure that they can request personal data from private parties based on reasoned requests from Europol.
9) political feasibility [+]
• The European Parliament will require detailed justification for necessity, as well as data protection safeguards. • The Council has supported such an approach in its Council Conclusions.[231]
10) coherence with other measures [+]
• This policy option would complement other Commission initiatives such as the Commission proposal for legislation on preventing the dissemination of terrorist content online.[232]

Policy option 3: allowing Europol to directly query databases managed by private parties in specific investigations

Expected impact of policy option 3[233]
1) impact on citizens [++]
• Very positive impact to the security of the European citizens and societies. In addition to receiving personal data (option 1), requesting personal and serving as a channel to transmit Member States request to private parties (option 2), Europol's ability to query private parties' data bases would ensure speedy access to this information for law enforcement, and would enable Member States to more effectively protect citizens from serious crimes.
2) impact on national authorities [+]
• Positive impact on national authorities, as Member States would obtain relevant criminal intelligence speedier and with less resources. However, the Member States of establishment would have to set up a system of ex post controls of Europol's access to these data bases.
3) impact on EU bodies [++]
• While this policy option would even further increase the workload for Europol compared to option 2, it Europol would be able to support Member States even more effectively by querying private parties' data bases directly.
4) impact on businesses [-]
• Private parties would spend less resources on replying to requests for personal data from multiple Member States, as far as Member States would channel such requests through Europol, and would be less exposed to risk of being liable to damage claims from data subjects. • However, private parties might suffer reputational damages, as some 'regular' customers may not appreciate their data being directly accessibly to law enforcement.

231 Council Conclusions Europol's cooperation with Private Parties, 2 December 2019.
232 Proposal regulation on preventing the dissemination of terrorist content online, COM(2018) 640 final.
233 The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

5) impact on Fundamental Rights [--]

a) identification of Fundamental Rights limited by the measure

- The policy options limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). The policy option also limits the fundamental rights of private parties to **conduct business** (Article 16 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.
- The policy option **does not adversely affect the essence** of the Fundamental Rights to protection of personal data, respect for private life and the right to conduct business, as such queries would be limited to specific investigations, and subsequent processing would be limited to legitimate purposes under Europol's mandate and subject to adequate safeguards enshrined in the Europol Regulation.

b) assessment of necessity

- The policy option is **genuinely effective** to achieve the specific objective of enabling Europol to cooperate effectively with private parties in order to effectively support Member States in countering crimes prepared or committed using cross-border services offered by private parties, and therefore the fight against serious crime and terrorism as objectives of general interest in EU law.
- Enabling Europol to directly query data bases managed by private parties (in addition to enabling the Agency to receive, and request personal data in line with policy option 1 and option 2) **effectively contributes to achieve this objective**.
- **Existing possibilities** to meet the objective, notably the promotion of best practices, are **insufficient** to address the problem. Likewise, existing rules on the exchange of personal data between Europol and private parties, even if their application is reinforced, are insufficient to address the problem.
- However, **policy option 2 addresses the problem equally effective** as policy option 3 by enabling Europol to issue requests for personal data to private parties, while being **less intrusive** as it does not oblige private parties to accept a direct access by Europol to their data bases. Instead, policy option 2 would ensure that private parties maintain control over the data bases they manage. Moreover, under policy option 2, the Member State of establishment would have to assess Europol's request. Furthermore, policy option 2 would ensure the possibility of ex ante judicial remedy against individual own-initiative requests under applicable laws of the Member State concerned. In particular, the safeguards under option 2 would ensure that Europol's request would not circumvent national safeguards, by ensuring that the applicable national thresholds for requesting more sensitive personal data (such as content data) also apply to Europol. Policy option 2 would therefore be less intrusive, both for data subjects and for private parties.
- Consequently, as a less intrusive measure is available that is equally effective in meeting the objective, policy option 3 is not limited to what is strictly necessary to achieve the objective. **The policy option does therefore not pass the necessity test.** The policy option shall therefore **not be assessed in terms of its proportionality**.[234]

[234] As set out in the toolkit provided by the EDPS on assessing necessity, "*only if existing or less intrusive measures are not available according to an evidence-based analysis, and only if such analysis shows that the envisaged measure is essential and limited to what is absolutely necessary to achieve the objective of general interest, this measure should proceed on to the proportionality test*". Likewise, the Commission's Operational guidance on taking account of Fundamental Rights in Commission impact assessments states that "*if it can be established that there are two policy options which are equally effective in achieving the objective but have different negative impacts on fundamental rights, then it is necessary to choose that option which is the least intrusive*".

c) assessment of proportionality
• As the policy option did not pass the necessity test, and therefore is not limited to what is strictly necessary, the policy option shall **not be assessed in terms of its proportionality**.
6) effectiveness in meeting the policy objectives [+]
• This policy option would enable effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals. It would enable Europol a speedier access to personal data held by private parties in investigations. However, it would entail a significant impact on fundamental rights (see above).
7) efficiency in meeting the policy objectives [+]
• While there would be some additional costs for Europol for solutions enabling such direct queries, this policy option would provide an efficient solution for a speedy access to relevant personal data held by private parties.
8) legal/technical feasibility [+]
• This policy option would require changes to the Europol regulation. • Moreover, Member States would need to take the necessary steps to ensure that Europol can request access to data bases held by private parties in specific investigations.
9) political feasibility [-]
• The European Parliament would likely object to this policy option, because of its significant impact on fundamental rights. Similarly, the Council would likely not support such an approach in the current context as it goes beyond what Member States have supported in their Council Conclusions.[235]
10) coherence with other measures [-]
• This policy option would go beyond what it necessary to complement other Commission initiatives such as the Commission proposal for legislation on preventing the dissemination of terrorist content online.[236]

6.2 Enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with Fundamental Rights

Policy option 4: clarifying the provisions on the purposes of information processing activities and enabling Europol to analyse large and complex datasets

Expected impact of policy option 4[237]
1) impact on citizens [+]
• Very positive impact on the security of the European citizens and societies. Europol would continue to support Member States' competent authorities with effective data processing, including the analysis of large and complex data sets to identify cross-border links. • In exceptional cases, Europol would process and store the data of persons who are not related to a crime, where this is necessary for the analysis of large and complex data sets.
2) impact on national authorities [++]
• Very positive impact on national authorities, as they will continue to receive effective

235 Council Conclusions Europol's cooperation with Private Parties, 2 December 2019.
236 Proposal regulation on preventing the dissemination of terrorist content online, COM(2018) 640 final.
237 The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

operational support by Europol and its data processing, including the analysis of large and complex datasets by way of digital forensics to identify cross-border links. It would maintain and enhance their capabilities in preventing and investigating crime, taking into account that law enforcement authorities rely on information to perform their tasks.

- Europol would be able to continue critical activities to support national competent authorities (e.g. analysis of large and complex datasets) and implement foreseen ones (e.g. PIU.net).

3) impact on EU bodies [++]

- Very positive benefits to Europol, as it will safeguard the status quo of Europol's daily work in supporting Member States by way of data processing, including the analysis of large and complex datasets by way of digital forensics.
- It would enable Europol to comply with the requirement related to specific categories of data subjects while carrying out its core tasks on data processing. It would also allow Europol to address the structural legal problem related to the analysis of large and complex datasets by Europol, as identified by the EDPS in its decision on Europol's big data challenge. It would indeed take account of the specific situation where Europol receives large and complex datasets to support criminal investigations.
- The agency would be in the position to effectively perform its tasks and process personal data related to crime in order to support Member States.

4) impact on businesses [0]

- No impact on businesses.

5) impact on Fundamental Rights [-]

a) identification of Fundamental Rights limited by the measure

- The policy limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As this policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). Consequently, the policy option needs to comply with the conditions set out in Article 52(1) of the Charter.
- The policy option does **not adversely affect the essence** of the Fundamental Rights to the protection of personal data and to respect for private life.

b) assessment of necessity

- The policy option is **genuinely effective** to achieve the specific objective of enabling Europol to fulfil its mandate and support Member States with the processing of personal data they submitted in the context of preventing and combating crimes that fall under Europol's mandate, and therefore the fight against serious crime and terrorism as objectives of general interest in EU law.
- The **existing rules** on this requirement and safeguard, even if their application is reinforced, are insufficient to address the problem of a lack of clarity on Europol's information processing activities, as they do not enable Europol to meet this requirement in practice when processing personal data it received, notably large and complex datasets. In case of doubt, the current rules do not provide for any possibility for Europol to verify if personal data received fall into the specific categories of data subjects listed in annex II of the Europol Regulation. Moreover, the current rules do not take account of the specific requirement of the processing of large and complex datasets, including by way of digital forensics. Policy option 4, instead, would provide the **necessary legal clarity and foreseeability**, as it would enable Europol to apply in principle the requirement related to specific categories of data subjects in its data processing, thus ensuring that the processing of personal data is limited to personal data that falls into the categories of data subjects listed in annex II. In that respect, the policy option would provide for an initial data processing would constitute a pre-analysis, prior to Europol's data processing for cross-checking, strategic analysis, operational analysis or

exchange of information. The policy option would take account of the operational reality that Member States might submit large and complex datasets where necessary for specific investigation, and enable Europol to process such large and complex datasets. The policy option would provide a **new legal ground for data processing by Europol**, which would limit the exercise of Fundamental Rights. Notably, it would provide for the exceptional processing of data of persons who are not linked to a crime and who therefore do not fall under any of the categories of data subjects listed in annex II of the Europol Regulation. Such data processing would constitute a **narrow and justified exception**, only applicable where such data processing is necessary for the analysis of a large and complex dataset in the context of Europol's support to a specific criminal investigation in a Member State.

- In terms of alternatives, the policy option is **less intrusive** than policy option 5 (see below), as it maintains the requirement and safeguard related to the specific categories of data subjects listed in annex II of the Europol Regulation. Policy option 5 introduces a new category of data subjects in annex II that does not have any connection to a crime. This option would introduce the possibility for Europol to process further the personal data of persons for whom no link to any crime could be established by the Member States or by Europol. This would soften – and basically undermine – the requirement related to specific categories of data subjects. Policy option 5 would therefore go beyond the need to clarify the legal regime and to take account of the nature of large and complex datasets. It would therefore raise important questions of necessity and proportionality. Policy option 4, instead, would **in principle maintain the obligation on Europol to limit its data processing to the specific categories of data subjects listed in annex II**, while taking into account the specific requirements of the processing of large and complex datasets. In doing so, policy option 4 would set out a procedure that would enable the Agency to meet this requirement when processing personal data as part of carrying out its tasks and fulfilling its mandate, including large and complex datasets.
- Consequently, policy option 4 is **essential and limited to what is strictly necessary** to achieve the specific objective of clarifying Europol's mandate in a way that enables the agency to fulfil its mandate and support Member States effectively, and hence to fight serious crime and terrorism as objectives of general interest in EU law.

c) assessment of proportionality

- The policy option and its purpose of clarifying the rules on Europol's information processing activities **correspond to the identified need**. They solve the problem resulting from the big data challenge as far as Europol is concerned. The policy option is effective and efficient to fulfil the objective
- The policy option does **not impose a disproportionate and excessive burden** on the persons affected by the limitation in relation to the specific objective of clarifying the rules on Europol's data processing activities to enable the agency to fulfil its mandate, and hence to the objectives of fighting serious crime and terrorism as objectives of general interest in EU law.
- As regards the aspect related to an initial data processing, the **sole purpose of the interference** is to verify, in case of doubt, if personal data submitted in the context of preventing and countering crimes falling under Europol's mandate actually fall within one of the specific categories of data subjects listed in annex II of the Europol Regulation. In other words, the sole purpose of the interference is to determine if Europol is authorised to process further such personal data. If this pre-analysis shows that personal data does not fall within one of the specific categories of data subjects listed in annex II of the Europol Regulation, Europol is not allowed to further process that data and needs to delete it.
- As regards the aspect on the analysis of large and complex datasets, the **sole purpose of the interference** is to enable Europol to process, as part of the large and complex dataset, the data of persons who are related to the serious crime or act of terrorism under investigation. For persons whose data is included in the large and complex dataset although they do not have any link to the crime under investigation, their data is not relevant to the criminal

investigation and shall not be used therein.

- Weighing up the intensity of the interference with the Fundamental Rights to the protection of personal data and to respect for private life, as described under step 3, with the legitimacy of the objectives to fight against serious crime and terrorism as objectives of general interest in EU law, the policy option constitutes a **proportionate response** to the need to solve the problem resulting from the lack of clarity in Europol's legal mandate as regards data processing activities, as well as from the need to process large and complex datasets in support of a specific criminal investigation.
- However, in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of enabling Europol to fulfil its mandate when processing personal data received, and including large and complex datasets in support of a specific criminal investigation, a **number of safeguards are necessary**.

d) necessary safeguards

- Ensuring that the **sole purpose** of the initial processing of personal data is the verification if data submitted to Europol relate to the specific categories of data subjects set out in annex II of the Europol Regulation. If this verification confirms that the data is related to a crime that falls under Europol's mandate, and hence falls into one of the categories of data subjects in annex II, Europol is authorised to further process the data for the purposes for which it was submitted. If, instead, the verification does not indicate any link to a crime, and hence the personal data does not fall into any of the categories of data subjects in annex II, Europol is not authorised to process the data further. It needs to delete that data.
- Ensuring that, in case of doubt, the verification of personal data submitted by Member States takes place **within six months of receipt** of the data by Europol, in line with the six-month period provided for in Article 18(6) of the Europol Regulation to determine whether data is relevant to Europol's tasks.
- Ensuring that the **exceptional extension of the six-month time limit** that applies to the initial data processing is limited to specific situations where such an exceptions is strictly necessary. Any exceptional extension of the six-month time limit shall be subject to prior authorisation by the EDPS.
- Ensuring that the **exceptional processing** of data of persons who are not related to a crime is strictly limited to **narrow and justified exceptions**, namely to the **specific situation** where such processing is strictly necessary to enable Europol to analyse a large and complex dataset it received from a Member State for operational support to a specific criminal investigation. In other words, such exceptional data processing shall only be allowed if it is not possible for Europol to carry out the operational analysis of the large dataset without processing personal data that falls into one of the categories of data subjects in annex II of the Europol Regulation. **This requires a clear definition of the situations where the narrow and justified exception applies.**
- Ensuring that the **sole purpose** of the processing of data of persons who are not related to a crime, but whose data is part of the large and complex dataset, is the operational support that Europol provides to the specific criminal investigation in the Member State that submitted the dataset. Or, subsequently, the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process for judicial proceedings.
- Ensuring the processing of data of persons who are not related to a crime, but whose data is part of the large and complex dataset, is **only allowed for as long as Europol supports the specific criminal investigation** for which the large dataset was provided. Or, **only for as long as it is necessary for judicial proceedings related to the criminal investigation** in a Member State. During that period, the data shall be blocked for any other processing.

6) effectiveness in meeting the policy objectives [++]

- It would constitute a very effective option to address the problem of a lack of clarity on Europol's information processing activities, as well as the structural legal problem related to

the analysis of large and complex datasets by Europol, as identified by the EDPS in its decision on Europol's big data challenge. • It would provide legal clarity and foreseeability, as it would enable Europol to apply the requirement related to specific categories of data subjects in its data processing. • It would take account of the operational reality that Member States might need to submit large and complex datasets to Europol where necessary for specific investigations.
7) efficiency in meeting the policy objectives [-]
• As the policy option would safeguard the status quo of Europol's work in supporting Member States by way of data processing, it would not have cost implications for IT development. • However, given the advancement of technological developments, and the ability of criminals to quickly adapt to new technologies, it can be expected that the operational need for the analysis of large and complex datasets, notably to detect cross-border links, will further increase, which would lead to some costs for Europol.
8) legal/technical feasibility [+]
• It is a feasible option to address the current issues of legal interpretation as well as the structural legal problem related to the analysis of large and complex datasets by Europol, as identified by the EDPS in its decision on Europol's big data challenge, by a legislative intervention in Article 18. As set out by the EDPS, "*certain aspects of the structural problems could be tackled by legislative measures*."
9) political feasibility [+]
• The aspect of extending the legal grounds for data processing by Europol is expected to be carefully assessed by the co-legislators. • Member States called on the Commission to address the related problems, notably the structural legal problem related to the analysis of large and complex datasets by Europol, as identified by the EDPS in its decision on Europol's big data challenge. Member States in the Council are therefore expected to support the policy option. • While the position of the European Parliament is not clear at this stage, it is expected that the European Parliament will take due account of the EDPS decision on Europol's big data challenge. This policy option is inspired by that decision and its reasoning.
10) coherence with other measures [0]
• Not applicable.

<u>Policy option 5</u>: introducing a new category of data subjects whose data Europol can process

<u>Expected impact of policy option 5</u>[238]
1) impact on citizens [-]
• It would remedy the current problem of a lack of certainty on Europol's information processing activities, including the analysis of large and complex data sets to identify cross-border links. • At the same time, it would go beyond the need to clarify the current legal regime. It would raise important questions of necessity and proportionality as regards the structural possibility to process personal data by Europol of persons who are not related to a crime.
2) impact on national authorities [0]

[238] The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

- It would result in a positive impact on national authorities in their daily operation, as it would extend the support that Europol could provide in terms of data processing. It would not only enable Europol to continue performing existing critical activities (e.g. the analysis of large and complex datasets by way of digital forensics) and implement foreseen ones (e.g. PIU.net), but also enable Europol to support Member States with the processing of data of persons who are not related to a crime.
- Questions on necessity and proportionality would be raised. This might affect the general public's perception of law enforcement work and notably of the work of Europol, due to the structural possibility to process data of persons who are not related to a crime.

3) impact on EU bodies [0]

- Facilitation of the data processing by Europol, as it would remove existing limitations related to the specific categories of data subjects that Europol is allowed to process. It would allow Europol to process data of persons who are not related to a crime.
- Questions on necessity and proportionality would be raised, as this option would go beyond what is necessary to clarify the legal regime and to enable Europol to analyse large and complex datasets. This might affect the general public's perception of Europol's work and its role on EU internal security. Concerns might be raised e.g. with regard to the risk of transforming Europol into a European 'information-clearing house'.

4) impact on businesses [0]

- No impact on businesses.

5) impact on Fundamental Rights[239] [--]

a) identification of Fundamental Rights limited by the measure

- The policy option limits the Fundamental Right to the protection of personal data as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to respect for private life (Article 7 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.
- The policy option does **not adversely affect the essence** of the Fundamental Rights to the protection of personal data and to respect for private life.

b) assessment of necessity

- The policy option is **genuinely effective** as it achieves the specific objective of enabling Europol to fulfil its mandate and support Member States effectively, and therefore the fight against serious crime and terrorism as objectives of general interest in EU law. Introducing the new category of data subjects would allow Europol to process any personal data submitted by Member States in order to meet its objectives and fulfil its tasks, including large and complex datasets.
- In terms of alternatives, the policy option addresses the problem **equally effective** as policy option 4 (see above). The latter would provide for an initial cross-check of personal data submitted by Member States against data held in Europol's databases, for the sole purpose of verifying if the data received relates to the specific categories of data subjects set out in annex II of the Europol Regulation. However, **policy option 4 is less intrusive**, as it would maintain the existing categories of data subjects as set out in annex II of the Europol Regulation. While policy option 5 basically undermines the requirement and safeguard related to the categories of data subjects, policy option 4 maintains that requirement while providing Europol with a possibility to fulfil it in practice.
- Consequently, as a less intrusive measure is available that is equally effective in meeting the

[239] For more information, see the detailed analysis of the impact on Fundamental Rights in Annex 5.

objective, policy option 5 is not limited to what is strictly necessary to achieve the objective. **The policy option does therefore not pass the necessity test.** The policy option shall therefore **not be assessed in terms of its proportionality**.[240]

c) assessment of proportionality

- A less intrusive measure is available with policy option 4 that is equally effective in meeting the objective. Policy option 5 is therefore not limited to what is strictly necessary. The policy option shall therefore not be assessed in terms of its proportionality.

6) effectiveness in meeting the policy objectives [++]

- It would constitute a very effective option to address the problem of a lack of clarity on Europol's information processing activities, as well as the structural legal problem related to the analysis of large and complex datasets by Europol, as identified by the EDPS in its decision on Europol's big data challenge.
- It would provide legal clarity and foreseeability, as it would enable Europol to process the personal data of any person, including persons who are not related to a crime.
- It would take account of the operational reality that Member States might need to submit large and complex datasets to Europol where necessary for specific investigations.

7) efficiency in meeting the policy objectives [-]

- As the policy option would significantly extend the scope of persons whose data can be processed by Europol, and hence increase the amount of personal data that Europol would further process and store, it would lead to additional costs for the agency.

8) legal/technical feasibility [+]

- It is a feasible option to address the current issues of legal interpretation as well as the structural legal problem related to the analysis of large and complex datasets by Europol, as identified by the EDPS in its decision on Europol's big data challenge, by a legislative intervention in Article 18. As set out by the EDPS, "*certain aspects of the structural problems could be tackled by legislatives measures*."

9) political feasibility [-]

- As the co-legislators decided in 2016 to limit the processing of personal data by Europol to specific data categories that are linked to a crime (i.e. namely suspects, convicted criminals, potential future criminals, contacts and associates, victims, witnesses and informants), it is considered unlikely that the co-legislators would agree to a legal solution that would de facto cave out that safeguard by extending the categories of data subjects to any person.

10) coherence with other measures [0]

- Not applicable.

6.3 Enabling Member States to use new technologies relevant for law enforcement

Policy option 6: regulating Europol's support to the EU security research programme, the innovation lab at Europol, and Europol's support to the EU

[240] As set out in the toolkit provided by the EDPS on assessing necessity, "*only if existing or less intrusive measures are not available according to an evidence-based analysis, and only if such analysis shows that the envisaged measure is essential and limited to what is absolutely necessary to achieve the objective of general interest, this measure should proceed on to the proportionality test*". Likewise, the Commission's Operational guidance on taking account of Fundamental Rights in Commission impact assessments states that "*if it can be established that there are two policy options which are equally effective in achieving the objective but have different negative impacts on fundamental rights, then it is necessary to choose that option which is the least intrusive*".

innovation hub

Expected impact of policy option 6[241]
1) impact on citizens [+]
• Europol's support to Member States in terms of fostering innovation and participating in the management of research related to law enforcement would enhance their ability to use modern technologies to counter serious crime and terrorism. This would enhance EU internal security and therefore have a positive impact on citizens.
2) impact on national authorities [+]
• National authorities would benefit from Europol's support in terms of a fortified coordination and fostering of innovation processes and in the assistance to the management of all the phases of the security research cycle. This would bring the operational needs of end-users closer to the innovation and research cycles and hence help to ensure that new products and tools respond to the needs of law enforcement. There would be synergies and economies of scale in innovation and research relevant for law enforcement.
3) impact on EU bodies [+]
• Europol would be able to support Member States in fostering innovation and assist in the management of security research. • Europol's innovation lab would support the screening of specific cases of foreign direct investments that concern contract providers of technologies and software for police forces. • Other EU agencies in area of justice and home affairs text as well as the Commission's Joint Research Centre would benefit from the secretarial support that Europol would provide to the EU innovation hub for internal security.
4) impact on businesses [+]
• Businesses active in the market of security products would benefit from closer links and interaction between the operational needs of law enforcement and security research, bringing the development of new products closer to the needs of end-users and hence supporting the uptake of new products.
5) impact on Fundamental Rights [0]
• The policy option does not provide for any new legal grounds for Europol for the processing of personal data. It does not limit any Fundamental Rights. • The involvement of Europol in innovation and research activities related to law enforcement, and notably its support role in the management of research under the upcoming Horizon Europe programme, exposes Europol to the general risks implied in security research, notably risks related to ethical principles. The overall legal framework for EU security research contains the necessary safeguards to mitigate these risks.[242] These safeguards would thus also apply directly to Europol's support to the management of research activities.
6) effectiveness in meeting the policy objectives [+]
• The policy option is partially effective in meeting the policy objective of enabling Europol to

241 The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

242 Under the current Horizon 2020 programme, all research and innovation activities shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols (Article 19 of Regulation (EU) 1291/2013). Procedures such as ethical screening and security scrutiny are in place to ensure compliance with these principles and legal requirements.

foster innovation and support the management of research. It would fall short of supporting Member States with the deployment of new tools to fight serious crime and terrorism that require the processing of personal data.
7) efficiency in meeting the policy objectives [+]
• The policy option would reduce costs for national authorities, as they would benefit from synergies and economies of scale created by the Europol innovation lab. These synergies, in turn, would create some costs at Europol, notably for staff of the Europol innovation lab. The synergies and reduced costs at national level would clearly outweigh these costs.
8) legal/technical feasibility [+]
• This is a feasible policy option which is supported by stakeholders.
9) political feasibility [++]
• Both co-legislators have called for the involvement of Europol in security research, and are therefore expected to support the policy option.
10) coherence with other measures [+]
• The policy option supports the wider work of the Commission on security research and innovation, notably the upcoming Horizon Europe programme. Europol would assist the Commission in the implementation of Union framework programmes for research and innovation activities that are relevant for law enforcement.

Policy option 7: Enabling Europol to process personal data for the purpose of innovation in areas relevant for its support to law enforcement

Expected impact of policy option 7[243]
1) impact on citizens [++]
• Europol's support to Member States in terms of fostering innovation and participating in the management of research related to law enforcement would enhance their ability to use modern technologies to counter serious crime and terrorism, including the use of new tools that require the processing of personal data. This would enhance EU internal security and therefore have a positive impact on citizens. • It would increase the public trust in law enforcement tools, as the development of these tools would take place with trusted, high quality EU datasets in a controlled environment. • It would reduce the dependency on products that were developed outside the EU, which might be developed based on different data, according to different rules, and with different objectives, and hence not necessarily in a transparent way that complies with EU norms and Fundamental Rights. It would therefore reduce the risk of biased and thus inaccurate outcomes, which in turn reduces the risk of discrimination.
2) impact on national authorities [++]
• National authorities would strongly benefit from Europol's support in terms of coordination and fostering of innovation processes and in the management of security research, bringing the operational needs of end-users closer to the innovation and research cycles, hence helping to ensure that new products and tools respond to the needs of law enforcement. There would be synergies and economies of scale in innovation and research relevant for law enforcement. • The policy option would provide national authorities with tools, including AI-based tools, for law enforcement that they could use on the basis of national legislation, thus enhancing their capabilities to use modern technologies for fighting serious crime and terrorism.

[243] The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

3) impact on EU bodies [++]

- Europol would effectively support Member States in fostering innovation and participate in the management of security research. Europol would train, test and validate algorithms for the development of tools, including AI-based tools, for law enforcement, with specific requirements and safeguards (see below).
- Europol's innovation lab would support the screening of specific cases of foreign direct investments that concern contract providers of technologies and software for police forces.
- Other EU agencies in the area of justice and home affairs as well as the Commission's Joint Research Centre would benefit from the support that Europol would provide to the EU innovation hub for internal security.

4) impact on businesses [+]

- Businesses active in the market of security products would benefit from closer links and interaction between the operational needs of law enforcement and security research, bringing the development of new products closer to the needs of end-users, hence supporting the uptake of new products.

5) impact on Fundamental Rights [-]

a) identification of Fundamental Rights limited by the measure

- The policy option limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.
- The policy option does **not adversely affect the essence** of the Fundamental Rights to the protection of personal data and to respect for private life.

b) assessment of necessity

- The policy option is **genuinely effective** to achieve the specific objective of enabling Europol to provide effective support to Member States on the use of new technologies for law enforcement, and therefore the fight against serious crime and terrorism as objectives of general interest in EU law.
- **Existing rules** on the processing of personal data by Europol for statistical or scientific research purposes are too general and therefore **insufficient** to address the problem, even if their application is reinforced.
- In terms of alternatives, the policy option addresses the problem resulting from gaps on innovation and research relevant for law enforcement **more effectively** than policy option 6. Indeed, policy option 6 is less intrusive as it does not provide for the processing of personal data, but it is insufficient to address the problem. The use of AI and algorithms in the area of law enforcement needs testing, as highlighted in the European ethical Charter on the use of artificial intelligence in judicial systems.[244] For this testing to be effective, the processing of personal data is necessary. Without testing on real data, an algorithm cannot produce results that are sufficiently precise.
- Consequently, the policy option is **essential and limited** to what is absolutely necessary to achieve the specific objective of enabling Europol to provide effective support to Member States on the use of new technologies for law enforcement, and hence the fight against serious crime and terrorism as objectives of general interest in EU law.

c) assessment of proportionality

[244] European Commission for the Efficiency of Justice of the Council of Europe: European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (3-4.12.2018).

- The policy option and its purpose of enabling Europol to process personal data for the purpose of innovation in areas relevant for its support to Member States' law enforcement authorities **correspond to the identified need and solves the problem**. The policy option is effective and efficient to fulfil the objective as explained below.
- Given the processing of personal data for the development of algorithms, the policy option risks having a harmful effect on the Fundamental Right to **non-discrimination** (Article 21 of the Charter).[245] This risk might even increase with the use of low data quality.[246] Moreover, Europol would use part of its operational data for the development of algorithms, and such law enforcement data was collected for the purposes of crime fighting and is not representative for the entire population. The use of such specific data for the development of algorithms might entail the risk of biased results. These risks will be mitigated with the introduction of necessary safeguards (see below).
- The policy option restricts the Fundamental Rights of the data subjects by processing their personal data for the training, testing and validating of algorithms. This would **not include the processing of special categories** of data. As part of the training, testing and validating of algorithms, the processing of personal data amounts to **profiling** of individuals. This needs to be accompanied with the necessary safeguards (see below).
- The policy option does **not impose a disproportionate and excessive burden** on the persons affected by the limitation (i.e. persons for whom Europol processes information in accordance with its existing tasks and objective) in relation to the specific objective of enabling Europol to provide effective support to Member States on the use of new technologies for law enforcement, and hence to the objectives of fighting serious crime and terrorism as objectives of general interest in EU law.
- Weighing up the intensity of the interference with the Fundamental Rights to the protection of personal data and to respect for private life as described under step 3 with the legitimacy of the objectives to fight against serious crime and terrorism as objectives of general interest in EU law, the policy option constitutes a **proportionate response** to the need to solve the problem resulting from gaps on innovation and research relevant for law enforcement.[247]
- The fundamental data protection principles – especially purpose limitation and minimisation – should be interpreted in such a way that they do not exclude the use of personal data for machine learning purposes.[248] They should not preclude the creation of training sets and the construction of algorithmic models, whenever the resulting AI systems are socially beneficial and compliant with data protection rights.
- However, in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of enabling Europol to provide effective support to Member States on the use of new technologies for law enforcement, a **number of safeguards are necessary**.

---

245 EU Agency for Fundamental Rights: #BiGData: Dicrimination in data-supported decision making (2018).

246 EU Agency for Fundamental Rights: Data quality and artificial intelligence – mitigating bias and error to protect Fundamental Rights (2019).

247 See the study of the European Parliamentary Research Service on The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (June 2020): "*In general, the inclusion of a person's data in a training set is not going to affect to a large extent that particular person, since the record concerning a single individual is unlikely to a make a difference in a model that is based in a vast set of such records. However, the inclusion of a single record exposes the data subject to risks concerning the possible misuse of his or her data, unless the information concerning that person is anonymised or deleted once the model is constructed.*"

248 Study of the European Parliamentary Research Service on The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (June 2020).

d) necessary safeguards

- Requirement to conduct a **fundamental rights impact assessment**[249] prior to any training, testing and validation of algorithms for the development of tools, including AI-based tools, for law enforcement:
  - assessing necessity and proportionality separately for each application;
  - ensuring compliance with ethical standards;
  - identifying potential biases in the operational data to be used for the development of algorithms, including an assessment of the potential for discrimination;
  - identifying potential biases and abuses in the application of and output from algorithms, including an assessment of the potential for discrimination; and
  - requiring prior authorisation of for each application, taking into account the risk of biased outcomes resulting from the use of law enforcement data.
- Requirement to ensure the **quality of the data**[250] used for the training, testing and validation of algorithms: while it may be challenging to assess the quality of all data used for building algorithms, it is essential to collect metadata and make quality assessments of the correctness and generalizability of the data.
- Requirement to ensure **separate data processing environment**:
  - separating the processing for training, testing and validation of algorithms from any processing of personal data for the operational tasks of objectives of Europol;
  - setting out clear criteria, and requiring specific authorisation, for the temporary transfer of data from the operational data processing environment to the separate data processing environment for the development of algorithms, based on strict necessity;
  - limiting the access to the separate data processing environment to specifically authorised staff of Europol;
  - deleting the outcome of the processing of personal data for training, testing and validation of algorithms once the digital tool is validated.[251]
- Requirement to keep the **data retention rules** and periods applicable: re-purposing the data does not result in the prolongation or re-initiation of the retention periods. Therefore, any technical solution must ensure the timely and automatic deletion of data used for the development of algorithms once the retention period of the corresponding data in the operational environment ends.
- Requirement to ensure that data processed for training, testing and validation of algorithms is **not used to support measures or decisions regarding individuals**:[252] avoiding any use of the personal data for predictions or decisions concerning individuals.
- Requirement to embed **lawfulness 'by design' and 'by default'**:[253]
  - limiting the processing of different types of personal data to what is strictly necessary for a specific purpose, e.g. processing anonymised and pseudonymised data for the development of algorithms;
  - processing of full data for testing in an operational scenario.
- Requirement to ensure **transparency** about the way the algorithm was built and operates, including a description of the process and rationale behind the calculations feeding the decision making, and possible biases resulting from the data: facilitating access for remedies for people who challenge subsequent decisions taken based on the algorithm.[254]

---

249 EU Agency for Fundamental Rights: #BiGData: Dicrimination in data-supported decision making (2018).

250 EU Agency for Fundamental Rights: Data quality and artificial intelligence – mitigating bias and error to protect Fundamental Rights (2019).

251 European Parliamentary Research Service: The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (June 2020).

252 European Data Protection Supervisor: A Preliminary Opinion on data protection and scientific research (6.1.2020).

253 EU Agency for Fundamental Rights: Preventing unlawful profiling today and in the future: a guide (2018).

254 EU Agency for Fundamental Rights: #BiGData: Dicrimination in data-supported decision making (2018).

• Requirement to avoid the use of artificial intelligence where this is **evidently incompatible with Fundamental Rights**:[255] applying a cautious and risk-adapted approach by completely or partially banning algorithmic systems with an untenable potential for harm.[256]
6) effectiveness in meeting the policy objectives [++]
• The policy option is very effective in enabling Europol to foster innovation and participate in the management of research relevant for law enforcement. The cooperation at EU level to create synergies and achieve economies of scale. Europol would be well placed to process personal data for the training, testing and validation of algorithms for the development of tools, including AI-based tools, for law enforcement, in full compliance with Fundamental Rights and with the necessary transparency.
7) efficiency in meeting the policy objectives [++]
• The policy option would reduce costs for national authorities, as they would benefit from synergies and economies of scale created by the Europol innovation lab. Notably synergies and economies of scale resulting from Europol's ability to provide Member States with tools, including AI-based tools, for law enforcement that would otherwise require significant investments at national level. These synergies, in turn, would create some costs at Europol, notably for staff and IT equipment of the Europol innovation lab. The synergies and reduces costs at national level clearly outweigh these costs.
8) legal/technical feasibility [+]
• The policy option is a feasible option to effectively enable Europol to foster innovation and participate in the management of research. It is supported by stakeholders.
9) political feasibility [0]
• The aspect of extending the legal grounds for data processing by Europol is expected to be carefully assessed by the co-legislators. • Member States in the Council are expected to support the policy option. • The position of the European Parliament is not clear at this stage. The European Parliament is currently discussing a Draft Report on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters. The European Parliament set up a special committee on AI on 18 June 2020.
10) coherence with other measures [++]
• The policy option supports the wider work of the Commission on security research and innovation, notably the upcoming Horizon Europe programme. Europol would assist the Commission in the implementation of Union framework programmes for research and innovation activities that are relevant for law enforcement. • The policy option enables Europol to participate in the roll-out of the European Strategy for Data. The policy option also takes account of the Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust, which sets out that AI can equip "*law enforcement authorities with appropriate tools to ensure the security of citizens, with proper safeguards to respect their rights and freedoms*".

7. HOW DO THE OPTIONS COMPARE?

7.1 Enabling effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals

[255] European Data Protection Supervisor: EDPS opinion on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust (29.6.2020).

[256] Data Ethics Commission: Opinion of the Data Ethics Commission (22.1.2020).

Comparative assessment for objective I			
	option 1	**option 2**	**option 3**
1) impact on citizens	+	++	++
2) impact on national authorities	+	++	+
3) impact on EU bodies	+	++	++
4) impact on businesses	+	+	-
5) impact on Fundamental Rights	-	-	--
6) effectiveness in meeting the policy objectives	+	++	+
7) efficiency in meeting the policy objectives	+	++	+
8) legal/technical feasibility	++	+	+
9) political feasibility	0	++	-
10) coherence with other measures	-	+	-
preferred policy option		**X**	

The policy options are cumulative in the sense that policy option 2 builds on policy option 1, and policy option 3 builds on policy options 1 and 2.

Policy option 2 is the preferred option. Under this policy option Europol would not only be able to receive personal data (policy option 1), but would also be able to exchange personal data with private parties in order to support Member States in establishing their jurisdiction, as well as to serve as a channel to transmit Member States' requests containing personal data to private parties.

This policy option is more efficient than **policy option 1**. National authorities will spend additional resources on dealing with Europol own-initiative request for personal data from private parties. However this will be offset by significant savings, as national authorities will spend less resources on identifying large data sets for information relevant to their jurisdiction, because Europol will be able to perform this task for them. In addition, Member States will spend less resources on transferring requests containing personal data to private parties outside their jurisdiction, as they can use Europol as a channel to transmit such requests. Businesses will spend additional resources on dealing with requests from Europol, but this will be offset by significant savings. Businesses will spend less resources on identifying the relevant national jurisdictions themselves, and will be less exposed to liability risks when sharing data with Europol.

Moreover, unlike policy option 3, policy option 2 (which comprises policy option 1) meets the proportionality test. While all three policy options limit Fundamental Rights, these limitations can be justified for policy 2, as this policy option constitutes a necessary and proportionate response to enable an effective cooperation with private parties. Moreover, the identified safeguards will mitigate the limitations on the exercise of Fundamental Rights. By contrast, **policy option 3 does not pass the necessity test** due to its significant impact on the rights of individuals to the protection of personal data and the rights of private parties to conduct business, and the fact that option 2 provides a similarly effective but less intrusive way of meeting the policy objectives. Policy option

3 shall therefore **not be assessed in terms of its proportionality**.[257]

In addition, policy option 2 is politically feasible and has already received some support from Member States in the Council.[258] Policy option 1 falls short of these Council conclusions, while policy option 3 goes too far.

Finally, and unlike policy option 1, this policy option would complement other initiatives at EU level, such as the proposed legislation on preventing the dissemination of terrorist content online, by enabling Europol to serve as a channel for Member States requests to private parties.

7.2 Enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with Fundamental Rights

Comparative assessment for objective II		
	option 4	**option 5**
1) impact on citizens	+	-
2) impact on national authorities	++	0
3) impact on EU bodies	++	0
4) impact on businesses	0	0
5) impact on Fundamental Rights	-	--
6) effectiveness in meeting the policy objectives	++	++
7) efficiency in meeting the policy objectives	-	-
8) legal/technical feasibility	+	+
9) political feasibility	+	-
10) coherence with other measures	0	0
preferred policy option	X	

Policy option 5 is a genuine alternative to policy option 4, as it would not adversely affect the essence of Fundamental Rights. However, policy option 4 scores better than policy option 5 in many aspects.

Both policy options are **equally efficient** in meeting the objective of enabling law enforcement to analyse large and complex datasets to detect cross-border links. Positive impact to national authorities in their daily operation. It will enhance their capabilities in preventing and investigating crime, especially taking into account that law enforcement

---

257 As set out in the toolkit provided by the EDPS on assessing necessity, "*only if existing or less intrusive measures are not available according to an evidence-based analysis, and only if such analysis shows that the envisaged measure is essential and limited to what is absolutely necessary to achieve the objective of general interest, this measure should proceed on to the proportionality test*". Likewise, the Commission's Operational guidance on taking account of Fundamental Rights in Commission impact assessments states that "*if it can be established that there are two policy options which are equally effective in achieving the objective but have different negative impacts on fundamental rights, then it is necessary to choose that option which is the least intrusive*".

258 Council Conclusions on Europol's cooperation with Private Parties, 2 December 2019.

authorities worldwide rely on information to perform their tasks, which needs to be analysed and transformed to actionable criminal intelligence that would provide direction in investigations, in the course of the 'intelligence cycle process' (direction - planning, collection, evaluation, collation, analysis, dissemination). It will facilitate identifying links between suspects and criminal activities and thus enhancing investigations. Europol will be able to continue performing existing critical activities to support national competent authorities (e.g. large data processing) and implement foreseen ones (e.g. PIU.net). It will drive to adequately interpreting the criminal environment at tactical, operational and strategic levels and achieving informed decision-making. It will positively affect resource allocation by the national competent authorities in the Member States. Both policy options would have an indirect positive impact on businesses. The option will enhance security in the EU. Maintaining a secure environment is an important prerequisite for conducting business.

Both policy options are **equally effective** in meeting the objective of enabling law enforcement to analyse large and complex datasets to detect cross-border links. They would provide clear **EU added value**. **Policy option 4 is less intrusive compared to policy option 5** in terms of limitations on the exercise of Fundamental Rights. Policy option 4 would maintain the obligation on Europol to limit its data processing to the specific categories of data subjects listed in annex II of the Europol Regulation (i.e. persons related to a crime for which Europol is competent), while clarifying that:

- when Europol receives personal data, it might carry out, in case of doubt and prior to any further data processing, an initial processing of such data (e.g. by way of collation),[259] including a check against data held in its databases, for the sole purpose of verifying if the data falls into the categories of data subjects set out in annex II of the Europol Regulation;
- when Europol analyses large and complex data sets by way of digital forensics to support a criminal investigation in a Member State, it may exceptionally process and store data of persons who are not related to the crime.

Policy option 5, instead, would enable Europol to process the data of any person. It would de facto remove the requirement that limits Europol's data processing to certain categories of data subjects only. Consequently, policy option 5 would enable Europol to process data on a structural basis persons who do not have any connection to a crime.

Consequently, as a less intrusive measure is available that is equally effective in meeting the objective, policy option 5 is not limited to what is strictly necessary to achieve the objective. **Policy option 5 does therefore not pass the necessity test.** Policy option 5shall therefore **not be assessed in terms of its proportionality**.[260]

Policy option 4 also limits the exercise of Fundamental Rights. These limitations can be justified, as the policy option constitutes a necessary and proportionate response to the need to enable law enforcement to analyse large and complex datasets to detect cross-

---

259 I.e. the pre-analysis phase where unstructured data received is being organised and structured into a format from which it can be analysed.

260 As set out in the toolkit provided by the EDPS on assessing necessity, "*only if existing or less intrusive measures are not available according to an evidence-based analysis, and only if such analysis shows that the envisaged measure is essential and limited to what is absolutely necessary to achieve the objective of general interest, this measure should proceed on to the proportionality test*". Likewise, the Commission's Operational guidance on taking account of Fundamental Rights in Commission impact assessments states that "*if it can be established that there are two policy options which are equally effective in achieving the objective but have different negative impacts on fundamental rights, then it is necessary to choose that option which is the least intrusive*".

border links. Moreover, the identified safeguards will mitigate the limitations on the exercise of Fundamental Rights. Notably, there is a need to ensure that the **exceptional processing** of data of persons who are not related to a crime is strictly limited to **narrow and justified exceptions**, namely to the **specific situation** where such processing is strictly necessary to enable Europol to analyse a large and complex dataset it received from a Member State for operational support to a specific criminal investigation.

As **policy option 4** would safeguard the status quo of Europol's daily work in supporting Member States by way of data processing, it would not have any cost implications for IT development. However, given the advancement of technological developments, and the ability of criminals to quickly adapt to new technologies, it can be expected that the operational need for the analysis of large and complex datasets, notably to detect cross-border links, will further increase, which would lead to some costs for Europol.

Option 4 provides a politically feasible option. Member States in the Council are expected to support the policy option. While the position of the European Parliament is not clear at this stage, it is expected that the European Parliament will take due account of the EDPS decision on Europol's big data challenge. This policy option is inspired by that decision and its reasoning.

Policy option 4 passes both the necessity and proportionality tests and is the preferred option.

7.3 Enabling Member States to use new technologies for law enforcement

Comparative assessment for objective III		
	option 6	**option 7**
1) impact on citizens	+	++
2) impact on national authorities	+	++
3) impact on EU bodies	+	++
4) impact on businesses	+	+
5) impact on Fundamental Rights	0	-
6) effectiveness in meeting the policy objectives	+	++
7) efficiency in meeting the policy objectives	+	++
8) legal/technical feasibility	+	+
9) political feasibility	++	0
10) coherence with other measures	+	++
preferred policy option		**X**

Policy option 7 builds on policy option 6 and includes all its components, including the support that the Europol innovation lab will provide to the screening of specific cases of foreign direct investments that concern contract providers of technologies and software for police forces. Policy option 7 is therefore not a genuine alternative to policy option 6, but would rather complement the latter.

Both policy options would reduce costs for national authorities, as the latter would

benefit from synergies and economies of scale created by the Europol innovation lab. This is notably the case for policy option 7, with its synergies and economies of scale resulting from Europol's ability to provide Member States with tools, including AI-based tools, for law enforcement that would otherwise require significant investments at national level. These synergies offered by policy option 7, in turn, would create some costs at Europol, notably for staff and IT equipment of the Europol innovation lab. The synergies and reduces costs at national level clearly outweigh these costs. Businesses active in the market of security products would benefit from closer links and interaction between the operational needs of law enforcement and security research, bringing the development of new products closer to the needs of end-users and hence supporting the uptake of new products.

Policy option 7 would address the problem resulting from gaps on innovation and research relevant for law enforcement **more effectively than policy option 6** that does not provide for the processing of personal data for innovation and research. **Policy option 7** provides clear **EU added value**, as it would close the identified gap on the coordination of research and innovation needs on the side of law enforcement, while at the same time addressing the need for an EU-level capacity to train, test and validate algorithms for the development of tools, including AI-based tools, for law enforcement.

Policy option 6, in turn, is less intrusive compared to policy option 7 when it comes to the limitations on the exercise of Fundamental Rights, as it does not provide for the processing of personal data. Instead, policy option 7 limits the exercise of Fundamental Rights. These limitations can be justified, the policy option constitutes a necessary and proportionate response to the need to solve the problem resulting from gaps on innovation and research relevant for law enforcement. Moreover, the identified safeguards will mitigate the limitations on the exercise of Fundamental Rights.

While Member States in the Council are expected to support policy option 7, the position of the European Parliament is not clear at this stage. Work is currently on-going in the European Parliament on a Draft Report on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters

Policy option 6 is <u>insufficient</u> to address the full scale of the problem identified. There is a need at national level for new technological tools for countering serious crime and terrorism that are based on the processing of personal data, and hence for the support of Europol in providing such tools. This, in turn, requires Europol to be able to train, test and validate algorithms for the development of tools, including AI-based tools, for law enforcement. Europol therefore needs to get the ability to process personal data for the purpose of innovation in areas relevant for its support to Member States' law enforcement authorities, within what is authorised by law, and with the necessary safeguards. Otherwise, Europol would not be able to provide full-scale effective support to Member States on the use of new technologies for law enforcement.

Consequently, policy option 7 is the <u>preferred option</u>.

8. PREFERRED POLICY OPTIONS: STRENGTHENING EUROPOL'S SUPPORT IN FULL RESPECT OF FUNDAMENTAL RIGHTS

Taken together, the preferred policy options identified in chapter 7 provide Europol with strong tools and capabilities to step up its support to Member States in countering emerging threats, in full compliance with Fundamental Rights.

Overview of preferred policy options	
specific objectives	**preferred policy options**
Objective I: enabling Europol to cooperate effectively with private parties	• ***Policy option 2***: allowing Europol to process data received directly from private parties, to exchange personal data with private parties to establish jurisdiction, as well as to serve as a channel to transmit Member States' requests containing personal data to private parties
Objective II: enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with Fundamental Rights	• ***Policy option 4:*** clarifying the provisions on the purposes of information processing activities and enabling Europol to analyse large and complex datasets
Objective III: enabling Member States to use new technologies for law enforcement	• ***Policy option 7:*** enabling Europol to process personal data for the purpose of innovation in areas relevant for its support to law enforcement

Table 4: Overview of preferred policy option

It should be noted that the objectives pursued – while serving the common goal of enabling Member States to more efficiently fight crime – are self-standing and not interdependent with each other. In practical terms, this means that choosing more 'ambitious' policy options under one objective (such as enabling Europol to analyse large and complex datasets under policy option 4), could not compensate for choosing less 'ambitious' policy options under another objective (such as limiting Europol's ability to interact with private parties to merely allowing the Agency to receive personal data from private parties under policy option 1).

The preferred policy options also take up the assessment carried out in separate annexes[261] on Europol's ability to provide frontline officers (police officers and border guards) with the result of the analysis of third-countries sourced information on suspects and criminals, on Europol's cooperation with third countries and on Europol's capacity to request the initiation of criminal investigations. In that respect, the package of preferred policy options will include:

- introducing a new alert category in the Schengen Information System to be used exclusively by Europol;
- a targeted revision aligning the provision on the transfer of personal data in specific situations with the provision of the Data Protection Law Enforcement Police Directive;
- seeking best practices and guidance on the application of provisions of the Europol Regulation;
- enabling Europol to request the initiation of criminal investigations in cases affecting only one Member State that concern forms of crime which affect a common interest covered by a Union policy.

Moreover, as set out in chapter 2 above, the package of preferred policy options includes the alignment of Europol's data protection regime with Chapter IX of Regulation (EU)

[261] See annex 6, annex 7 and annex 8.

2018/1725 and the strengthening of Europol's cooperation with the EPPO.

Given that chapter 7 assessed the policy options per objective, it is necessary to **assess the accumulated proportionality of all the preferred options**. Three dimensions are of relevance here, namely the accumulated impact on (1) Europol's support role under Article 88 TFEU, (2) Fundamental Rights, and (3) costs and benefits.

8.1 Accumulated impact of the preferred options on Europol's role

The preferred options will equip Europol with effective means to meet Member States' needs and demands for enhanced support. This includes tools and capabilities that so far have been the prerogative of national law enforcement authorities. This is notably the case for the possibilities to request personal data from private companies. In that respect, the accumulated impact of the preferred options might appear as moving Europol closer to an ordinary police authority.

However, the preferred options **remain within the framework of Article 88 TFEU** and the support role it stipulates for Europol. In fact, they are a consequence of the impact of evolving security threats on Europol's ability to fulfil its support role effectively, requiring new tools and capabilities for Europol to be able to support and strengthen actions by the Member States. Moreover, they contain safeguards to ensure that when Europol applies the new tools and capabilities, it does not go beyond what is necessary to support national law enforcement authorities:

- To issue follow-up requests for information held by private parties in order to establish jurisdiction, Europol would keep the Member State of establishment informed.
- To issue own initiative requests for information held by private parties in order to establish jurisdiction, Europol would send a reasoned request to the Member State of establishment, which would assess this request, before issuing its own request to the private party in question under its national procedures to share the personal data with Europol.

Consequently, Member States remain the beneficiaries of Europol's support role and keep control of its activities.

8.2 Accumulated impact of the preferred options on Fundamental Rights

All preferred policy options provide new legal grounds for Europol to process personal data where this is necessary to fulfil its objectives and tasks. Consequently, these policy options have an impact on Fundamental Rights and limit in particular the rights to the protection of personal data (Article 8 of the Charter) and to respect for private life (Article 7 of the Charter). The preferred policy options that would provide for new legal grounds for Europol:

- to ask private parties to share personal data with Europol as a follow-up to that private party having shared personal data with the agency, in order to establish jurisdiction, to ask Member States to request private parties to share personal data with Europol to establish jurisdiction, and to serve as a channel for Member States' request containing personal data to private parties;
- to process data of persons who are not linked to a crime and who therefore do not fall under any of the categories of data subjects listed in annex II of the Europol Regulation, where such data processing is necessary for the analysis of a large and complex dataset in the context of Europol's support to a specific criminal investigation in a Member State; and

- to process personal data to train, test and validate algorithms for the development of tools, including AI-based tools, for law enforcement, which would enable Europol to support national law enforcement authorities in fostering innovation in areas relevant for law enforcement.

As shown in the detailed assessment of the policy options in terms of their limitations on the exercise of Fundamental Rights in annex 5, the preferred policy options are strictly limited to what is necessary and proportionate and include the necessary safeguards.

Given that a legislative initiative to strengthen the Europol legal mandate would combine these preferred policy options, there is a need to assess the accumulated proportionality of all the preferred options and their accumulated impact on Fundamental Rights. It is noted that providing Europol with data processing tools and capability that so far have been the prerogative of national law enforcement authorities requires **reinforcing the democratic oversight and accountability of Europol**. Indeed, a July 2020 European Parliament Resolution[262] "*recalls that a strengthened mandate should go hand-in-hand with adequate parliamentary scrutiny*". To that end, the preferred policy options should be combined with an obligation on Europol to provide, as part of its existing reporting obligations and in the necessary confidentiality, the following information to the European Parliament on an annual basis:

- the number of cases in which Europol issued follow-up requests to private parties or own-initiative requests to member States of establishment for the transmission of personal data, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks;
- the number of instances where Member States requested Europol to analyse large and/or complex data sets, and the number of time; and
- the number of pilot projects in which Europol processed personal data to train, test and validate algorithms for the development of tools, including AI-based tools, for law enforcement, including information on the purposes of these projects and the law enforcement needs they seek to address.

Moreover, the alignment of the Europol Regulation with Regulation[263] on the processing of personal data by EU institutions, bodies, offices and agencies directly applicable to Europol's data protection regime, complemented with more detailed rules on data protection in the Europol Regulation where needed, would further strengthen Europol's data protection regime and streamline the rules on supervision.

Moreover, in order to provide for a future assessment of the accumulated impact of the preferred policy options on Fundamental Rights in practice, the preferred policy options should be accompanied by a provision requiring an assessment of their impact on Fundamental Rights two years after their entry into applications. This would follow the example of a related obligation in the Directive on combating terrorism.[264]

8.3 Accumulated impact of the preferred options on costs and benefits for key stakeholders

The ultimate beneficiaries of all preferred options are the citizens, who will directly and indirectly benefit from lower crime rates, reduced economic damages, and less crime and

---

262 European Parliament resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing (2020/2686(RSP)).

263 Regulation (EU) 2018/1725.

264 Article 29 of Directive (EU) 2017/541 (15.3.2017).

security related costs.

The **benefits for society at large** in terms of a reduction in crime have been estimated at approximately EUR 1 000 million over 10 years. It is widely acknowledged that societal benefits of fighting and preventing crime are inherently difficult to estimate.[265] These benefits are a function of the direct and indirect costs of crime for society and are influenced by a variety of tangible and intangible costs for the victims (such as medical costs, pain, lost quality of life), offenders (such as lost productivity), or tax payers (such as costs of criminal justice system). Against this background, the estimated impact of the benefits of the initiative to strengthen the Europol mandate was based on several resources, including available reports on the costs of specific types of crime, such as terrorism and corruption (e.g. the costs of corruption alone are estimated to be at least EUR 200 billion per year),[266] studies on the total criminal proceeds in the EU, which are estimated to be at least EUR 110 billion annually,[267] and previous Commission impact assessments from the area of law enforcement, in particular on the e-evidence proposal, which estimated the benefits of this proposal at EUR 3 000 billion over 10 years.[268] The chosen estimate therefore reflects – in a conservative manner - the magnitude of the effects of serious crime on society, and the potential benefits of high-impact EU level solutions on combatting and preventing crimes on a European scale.

The benefits in terms of **savings in administrative costs** have been estimated at approximately EUR 200 million over 10 years. These figures have been estimated in a conservative manner as a direct function of envisaged costs of the current initiative for Europol. These costs are estimated to be at least EUR 120 million over six years, resulting in an average of EUR 20 million per year. On this basis the administrative savings for national administrations were estimated at EUR 20 million per year and EUR 200 million over 10 years. [269]

C**ost estimates** have been calculated in cooperation with Europol. They took into consideration the increase in workload as stakeholders make more use of Europol's services over time, and the time needed for Europol to absorb resources to avoid a situation where the agency would not be able to fully implement its EU contribution and commit appropriations in due time. Staff costs, representing an important share of the overall costs estimates, have been estimated based on Commission average unit costs, to which was applied the correction coefficient for the Netherlands (111,5%).

The **economic impacts** of the preferred policy options can be summarised as follows:

- **Policy option 2** (Europol's ability exchange personal data with private parties) would reduce the costs for private parties and national authorities of analysing multi-jurisdictional or non-attributable data sets in order to establish the

---

265 Organised Crime and Corruption, Cost of Non-Europe Report, Wouter van Ballegooij, Thomas Zandstra, European Parliamentary Research Service, 2016.

266 Organised Crime and Corruption, Cost of Non-Europe Report, Wouter van Ballegooij, Thomas Zandstra, European Parliamentary Research Service, 2016.

267 Final Report of Project OCP – Organised Crime Portfolio: From illegal markets to legitimate businesses: the portfolio of organised crime in Europe, Savona Ernesto, Michele Riccardi (Eds.), 2015.

268 COM SWD(2018) 118 final.

269 An alternative way of calculating the savings in administrative costs would be as a direct function of the costs of 27 national solutions corrected for the costs of the envisaged proposal (EUR 120-150 million over 6 years). On this basis the savings in administrative costs would amount to more than EUR 5 billion. However, such an approach would not control for a number of important factors including the unwillingness or inability of some Member States to undertake such investments.

jurisdiction of the Member State concerned, as far as Europol performs these tasks for them. In addition, Europol could serve as a channel for transmitting Member States requests to private parties, which would reduce the costs for private parties to verify the authenticity of the requests, and for national law enforcement to transmit these requests through a secure and efficient channel. This policy option would require an estimated 60-70 FTE as well as EUR 7 million at the level of Europol.

- **Policy option 4** (Clarification of provisions on data processing in Europol's mandate and enabling Europol to analyse large and complex datasets) would lead to some costs for Europol as the operational need for the analysis of large and complex datasets, notably to detect cross-border links, will further increase due to the advancement of technological developments, and the ability of criminals to quickly adapt to new technologies. This policy option would require an estimated 5-15 FTE and EUR 0.1 million at the level of Europol.
- **Policy option 7** (Europol's ability to process data for innovation) would reduce costs for national authorities, as they would benefit from synergies and economies of scale created by the Europol innovation lab. This policy option would require an estimated 25-35 FTE and EUR 15 million at the level of Europol.

The table below illustrates how Europol's increased ability to support Member States in fighting and preventing crime creates efficiencies, for national authorities and private parties (policy option 2), and benefits citizens in general.

Economic Impact				
preferred policy options	**citizens**	**businesses**	**National authorities**	**EU bodies**
Policy option 2	[+]	[+]	[+]	[-]
Policy option 4	[+]	[0]	[0]	[-]
Policy option 7	[+]	[0]	[+]	[-]

Table 5: Overview of the economic impacts

While all preferred options serve the common objective of enabling Member States to more efficiently fight crime in order to ensure the security of EU citizens, they are also self-standing and not dependent on each other. Consequently, **it is not possible to achieve the same objectives as efficiently by another combination of the policy options**. Therefore, this package of policy options consists of the preferred policy options under the respective objectives.

The preferred policy options are expected to have an **impact on the budget and staff needs of Europol**. Since 2016 and the last revision of Europol's legal mandate, the trend has been towards an exponential growth of the agency's data flows and demand on its services, leading to yearly budget and staff reinforcements above the levels initially programmed. At this stage, it is difficult to quantify precisely some of the individual policy options, notably because of the complexity of the development of the proposed IT infrastructures and systems. It is noted that more than 20% of Europol's overall budget is dedicated to operational ICTs due to the agency's constant need to maintain and update its IT infrastructure to ensure its core task as the EU information hub. The resource needs presented in annex 3 have been estimated taking these trends into consideration.

As a consequence, the preferred options would require financial and human reinforcements compared to the resources earmarked in the Commission proposal of May 2020 for the Multiannual Financial Framework 2021-2027, which plan for a 2% yearly increase of the EU contribution to Europol. It is estimated that an **additional budget of around EUR 120 to 150 million and around 150 additional posts** would be needed for

the overall MFF period to ensure that Europol has the necessary resources to enforce its revised mandate.[270]

The estimates presented in annex 3 as well as the overall budget and number of posts are subject to the outcome of the negotiations on the Multiannual Financial Framework 2021-2027. In any case, any increase of the EU contribution to Europol's budget resulting from a strengthening of Europol mandate would need to stay within the ceilings in heading 5 ('security and defence') of the Multiannual Financial Framework 2021-2027, which also include the funds for other agencies in the area of security, the Internal Security Fund (ISF), nuclear decommissioning, defence and crisis response, as well as a margin. The increase of the EU contribution to Europol's budget would require a reallocation of funds from other positions under heading 5 to Europol.

9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

It will be essential that the implementation of the preferred policy options and the achievement of the objectives is closely monitored. With the envisaged strengthening of Europol's mandate, important new tasks will be added to the agency, while others will be clarified, codified and detailed. These interventions to Europol's mandate would constitute important opportunities for the agency to provide enhanced and effective operational support to the Member States, but also significant obligations to undertake. These new functions would have to be closely assessed. Monitoring and evaluation should also focus on potential risks in terms of data protection. A **robust monitoring and evaluation mechanism would be crucial** to ensure that the envisaged beneficial effects of the strengthened Europol Regulation materialise in practice.

The monitoring and evaluation of Europol's reinforced mandate would largely be performed by the applicable mechanisms under the existing Europol Regulation. Article 68 foresees an evaluation which assesses, in particular, the impact, effectiveness and efficiency of Europol and of its working practices and may address the possible need to modify the structure, operation, field of action and tasks of Europol, and the financial implications of any such modification. Further to this evaluation, the Commission will draw data through its representation in Europol's Management Board meetings and its supervision, along with the Member States, of Europol's work (Article 11).

Based on Article 7(11) of Europol Regulation, the Commission will also draw data from Europol's annual report on the information provided by Member States. This report is performed on the basis of quantitative and qualitative evaluation criteria defined by the Management Board. Further data will be collected via Europol's multiannual programming and annual work programmes[271] (Article 12), as well as Europol's consolidated annual activity report[272] (Article 16(5)(g)). The Commission will collect data through its participation as an observer to the meetings of the heads of the national units. Concerning data protection risks, the Commission will consult the EDPS.

In order to ensure an effective implementation of the measures foreseen and to monitor

---

270 These figures include the estimates related to the introduction of a new alert category in the Schengen Information System exclusively for Europol (annex 6), Europol's cooperation with third countries (annex 7), Europol's capacity to request the initiation of criminal investigations (annex 8), and Europol's cooperation with the European Public Prosecutor's Office.

271 https://www.europol.europa.eu/publications-documents/europol-programming-document.

272 The Europol Consolidated Annual Activity Reports (CAAR) contain a comprehensive and thorough account of the activities carried out by Europol in implementing its mandate. The report also provides a detailed overview of the results achieved in relation to the objectives set in the Work Programmes.

their results, the Commission would work closely with relevant authorities in Member States, EU agencies (especially Europol), bodies (e.g. the EPPO) and institutions. The data collection would include the Serious and Organised Threat Assessment, publically available reports and feedback from Eurostat and Eurobarometer.

In line with better regulation rules, the evaluation of strengthening Europol's mandate will be based on a detailed programme for monitoring the outputs, results, impacts and data protection risks realised. The monitoring programme shall set out the indicators and means by which, and the intervals at which, the data and other necessary evidence will be collected. These indictors[273] reflect and define, in practice, the success of the policy options and will be measured on a yearly basis. Overall success will be assessed after four years of the entry into force of the new provisions in Europol's mandate. Targeted surveys may be carried out to collect further information.

Table 6 summarises tentative indicators (subject to further refinement in the envisaged monitoring programme) to monitor the achievement of specific objectives as well as the operational objectives linked to the building blocks of the preferred policy options.

Specific objectives	Operational objectives	Indicators	Collection Strategy
Enable effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals	- Process data received directly from private parties - request personal data held by private parties to establish jurisdiction - serve as a channel to transmit Member States' requests containing personal data to private parties	- Number of contributions received from private parties - Number of requests to establish jurisdiction - Number of requests to channel - Member States' requests to private parties - Level of end users' satisfaction with Europol's products and services and with how Europol's work contributed to achieve operational outcomes[274]	Europol's data EDPS
Enable law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with Fundamental Rights	- Perform an initial processing of personal data for purpose of verifying if the data falls into the categories of data subjects set out in annex II of the Europol Regulation Exceptionally process and store data of persons who are not related to a crime when analysing large and complex data sets by	- Number of entities cross-checked for the purpose of verifying if the data received relates to the specific categories of data subjects set out in annex II of the Europol Regulation - Number of cases where high volumes of personal data is received - Level of end users' satisfaction with Europol's products and services and with how Europol's work contributed to achieve operational outcomes[275] - Number of operations supported - Number of analytical reports produced - Number of Joint Investigation Teams (JITs[276]) supported	Europol's data EDPS

273 It should be noted that these indicators do not include fix quantitative targets as they are dependant to external factors. In particular, they correspond to law enforcement activities reactive to unpredicted criminal activities. However, a measure will be considered successful if the indicators show an upwards trend on an annual basis.

274 Europol carries out regular surveys, which assess the level of satisfaction of national law enforcement authorities with Europol services.

275 Europol carries out regular surveys, which assess the level of satisfaction of national law enforcement authorities with Europol services.

276 https://www.europol.europa.eu/activities-services/joint-investigation-teams

	way of digital forensics to support a criminal investigation.	- Number of actions days coordinated/supported - Number of mobile office support[277] (on the spot analysis) requested and deployed - Number of forensic kit[278] requests and deployments - Number of data protection incidents reported/EDPS decisions	
Enable Member States to use new technologies for law enforcement	- Enable Europol to process personal data, including high volumes of personal data, as part of fostering innovation - Europol will participate in the management of research in areas relevant for law enforcement	- Amount of personal data processed for the purpose of innovation - Number of tools for law enforcement created - Level of end users' satisfaction with Europol's products and services and with how Europol's work contributed to achieve operational outcomes - Number of data protection incidents reported/EDPS decisions	Europol's data EDPS

Table 6: Overview of monitoring and evaluation

277 https://www.europol.europa.eu/activities-services/services-support
278 https://www.europol.europa.eu/activities-services/services-support/forensics

10. LIST OF ANNEXES

- Annex 1: Procedural information
- Annex 2: Stakeholder consultation
- Annex 3: Who is affected by the initiative and how?
- Annex 4: Past performance of Regulation (EU) 2016/794
- Annex 5: Detailed assessment of the policy options in terms of their limitations on the exercise of Fundamental Rights
- Annex 6: Europol and the Schengen Information System
- Annex 7: Europol's cooperation with third countries
- Annex 8: Europol's capacity to request the initiation of criminal investigations
- Annex 9: Policy options discarded at an early stage
- Annex 10: Questionnaire
- Annex 11: Replies to the questionnaire