Council of the European Union

Brussels, 11 December 2025
(OR. en)

16767/25
ADD 1

ENFOPOL 480
CRIMORG 259
IXIM 345
COPEN 419
DATAPROTECT 342
JAI 1908
SIRIS 16
SCHENGEN 108

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	11 December 2025
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2025) 404 final
Subject:	COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL evaluating and assessing the operational impact of the implementation of the tasks provided for in Regulation (EU) 2022/991, in particular in Article 4(1), point (t), Article 18(2), point (e), Article 18(6a), and Articles 18a, 26, 26a and 26b, with regard to Europol's objectives as well as the impact of those tasks on fundamental rights and freedoms as provided for by the Charter, pursuant to Article 68(3) of Regulation (EU) 2016/794

Delegations will find attached document SWD(2025) 404 final.

Encl.: SWD(2025) 404 final

EUROPEAN
COMMISSION

Brussels, 11.12.2025
SWD(2025) 404 final

COMMISSION STAFF WORKING DOCUMENT

Accompanying the document

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

evaluating and assessing the operational impact of the implementation of the tasks provided for in Regulation (EU) 2022/991, in particular in Article 4(1), point (t), Article 18(2), point (e), Article 18(6a), and Articles 18a, 26, 26a and 26b, with regard to Europol's objectives as well as the impact of those tasks on fundamental rights and freedoms as provided for by the Charter, pursuant to Article 68(3) of Regulation (EU) 2016/794

{COM(2025) 752 final}

Table of Contents

Index of boxes

Index of tables

Index of charts

Acronyms

CTA	Customs Threat Assessment
DG HOME	Directorate-General for Migration and Home Affairs of the European Commission
DPF	Data Protection Function
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSA	Digital Services Act, Regulation (EU) 2022/2065
ECTC	European Counter Terrorism Centre
EDPS	European Data Protection Supervisor
EIS	Europol Information System
ENU	Europol National Unit
EPPO	European Public Prosecutor Office
ER	Europol Regulation, Regulation (EU) 2016/794
ETR	Europol Tool Repository
EU CARES	EU Child Abuse Referral Service
EUDPR	EU Data Protection Regulation, Regulation (EU) 2018/1725
EU IRU	EU Internet Referral Unit
FR	Fundamental rights
FTE	Full-time Equivalent
FTF	Foreign Terrorist Fighter
FRO	Fundamental Rights Officer
GDPR	General Data Protection Regulation
HSP	Hosting Service Providers
ICT	Information and Communications Technology
IM(U)	Information Management (Unit)
IOCTA	Internet Organised Crime Threat Assessment
JOAC	Joint Operational Access Concept
LED	Law Enforcement Directive – Directive (EU) 2018/680
MS	Member State
NCMEC	National Centre for Missing and Exploited Children
NGO	Non-governmental Organisation
ODIN	Operational Data for Innovation (Europol's sandbox)
OTF	Operational Task Force
PERCI	Plateforme Européenne de Retraits de Contenus Illégaux sur Internet
SAC	Schengen Associated Country – Switzerland, Liechtenstein, Norway, Iceland
SIRENE	Supplementary Information REquest at the National Entries
SIS	Schengen Information System
SOCTA	Serious and Organized Crime Threat Assessment
TCO	Terrorist Content Online
TE-SAT	Terrorism Situation & Trend Report
TFEU	Treaty on the Functioning of the European Union

1. Background

The EU Agency for Law Enforcement Cooperation (Europol) began operations in 1999. Since then, it has played **a central role in combating cross-border serious crime and terrorism**, becoming a key driver of law enforcement cooperation in Europe. The security landscape has undergone drastic changes over the last thirty years, with a corresponding shift in the DNA of serious and organised crime.[1] Member States have new operational needs to address emerging threats effectively, and so their **expectations of Europol's support have** also **evolved**. Europol's mandate has therefore been replaced or amended several times to maintain and enhance the Agency's relevance.

The mandate, as set out in Regulation (EU) 2016/794[2] (the 'Europol Regulation', or 'ER'), was last amended in 2022 with the adoption of Regulation (EU) 2022/991[3] to address new security threats. The Europol Regulation was no longer fit for purpose in a new reality where criminals exploit the advantages brought about by **digital transformation**, **new technologies**, **globalisation**, and **mobility**.[4]

The **specific objectives** of Regulation (EU) 2022/991[5] were:

- enabling effective cooperation between **private parties** and law enforcement authorities to counter the abuse of cross-border services by criminals;
- enabling law enforcement to analyse **large and complex datasets** to detect cross-border links, in full compliance with fundamental rights;
- enabling Member States to use **new technologies** for law enforcement.

In addition, Regulation (EU) 2022/991 amended the data protection rules applicable to Europol to maintain a **high level of data protection,** striking a balance between the Agency's new powers to process personal data and individuals' privacy and personal data protection. It largely aligned the data protection rules applicable to Europol with those applicable to other Justice and Home Affairs (JHA) EU agencies and bodies under Chapter IX of Regulation (EU) 2018/1875 ('the EU Data Protection Regulation', or 'EUDPR'), and those applicable to Member States' law enforcement authorities ('competent authorities') under their national law transposing Directive (EU) 2016/680 (the 'Law Enforcement Directive' or 'LED')[6] to **facilitate the flow of information**.

The new powers and tasks would help Europol attaining its objectives 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' and 'endeavor to ensure a high level of security through measures to prevent and combat crime', in accordance with Article 88 Treaty on the Functioning of the European Union (TFEU) and Article 3 ER.

2. Scope of the evaluation and methodology

The evaluation has been carried out in compliance with the obligation for the Commission, pursuant to **Article 68(3) ER**, to evaluate and assess the operational impact of Europol's tasks

---

1 Europol, 2025 EU Serious and Organised Crime Threat Assessment (SOCTA) – The changing DNA of serious and organised crime, available online under https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf ('EU SOCTA 2025'). See also the Customs threat assessment (CTA) 2025, available online under https://www.douane.gouv.fr/sites/default/files/2025-07/03/Livret-CTA-UE-public_0.pdf.

2 OJ L 135, 24.5.2016, p. 53, ELI: http://data.europa.eu/eli/reg/2016/794/oj.

3 OJ L 169, 27.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/991/oj.

4 SWD(2020) 543 final of 9 December 2020, p. 37, https://eur-lex.europa.eu/resource.html?uri=cellar:1a4d9f40-3b02-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF.

5 *Ibidem.*

provided for in Regulation (EU) 2022/991 three years after it entered into force. The Commission received the mandate to: first, evaluate and assess the **operational impact** of some of the new rules for processing personal data, with regard to Europol's objectives, under Article 3 ER; secondly, assess the impact of those rules on **fundamental rights and freedoms** ('fundamental rights') as provided for in the Charter[6], and thirdly, carry out a **cost-benefit analysis** of the related data processing tasks.

In accordance with Article 68(3) ER, this evaluation of the Europol Regulation covers only the new, or amended, provisions of Article 4(1)(t) ER, Article 18(2)(e) and 33a ER, Articles 18(6a) and 18a ER as well as, Articles 26, 26a and 26b ER. In essence, it is limited to the new legal framework for the processing of personal data by Europol as regards the following tasks:

(a) **Schengen Information System (SIS) information alerts** on third-country nationals upon proposal by Europol;
(b) processing of personal data by Europol for **research and innovation** projects;
(c) analysis by Europol of **large and complex datasets (**better known in slang and technical jargon as '**big data**')[7] without data subject categorisation (DSC);
(d) exchange of personal data between Europol and **private parties**. [8]

To prepare the evaluation, the Commission services gathered information and feedback from **various sources**: reports by Europol on the implementation of the Europol Regulation, consultations of Europol staff at technical meetings with DG HOME staff and through written requests for information, consultations of Member States via a short questionnaire, and contributions provided spontaneously by other stakeholders. The evidence collected, although limited in scope[9], nonetheless allows to identify possible areas for improvement in Europol's legal mandate and its implementation.

Further information on the evidence base of the evaluation can be found in Annex I **Evidence base of the evaluation**, which describes in detail all sources used for the report, including the consultation activities. The tables in Annex II **Overview of costs and benefits (2022-2025)** summarise the costs and benefits of Europol's extended tasks. Annex III **Summary of Member States' replies** reports all statistics on the replies of the Member States to the short questionnaire and the comments provided by Member States in extensive form.

3. General context

3.1. External dimension - Article 4(1)(t) ER on SIS information alerts on third-country nationals upon proposal by Europol

Given the **global nature of serious crime and terrorism**, information held by third countries and international organisations about perpetrators and persons suspected of such crimes is increasingly relevant to the EU's internal security. The external dimension of EU law

6 Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391, ELI: http://data.europa.eu/eli/treaty/char_2012/oj.

7 EDPS, Opinion 7/2015, p. 7, available online under https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf. 'In general terms, as a common denominator of the various definitions available, 'big data' refers to the practice of combining huge volumes of diversely sourced information and analysing them, using more sophisticated algorithms to inform decisions. Big data relies not only on the increasing ability of technology to support the collection and storage of large amounts of data, but also on its ability to analyse, understand and take advantage of the full value of data (in particular using analytics applications)'.

8 For the purposes of the Europol Regulation, according to Article 2(f), 'private parties' means entities and bodies established under the law of a Member State or third country, in particular companies and firms, business associations, non-profit organisations and other legal persons that do not qualify as international organisations.

9 See Section 1 of Annex III.

enforcement cooperation has therefore become crucial for Member States, as has the **role of Europol in supporting Member States in their partnerships with third countries** or entities located in those countries. Further efforts will be **essential in the future** to strengthen global security.[10]

Regulation (EU) 2022/991 introduced already substantial amendments to the Europol Regulation in order to enhance the **external dimension of Europol's activities**, in particular facilitating the exchange of information with third countries[11] and requiring Europol to include a strategy for relations with third countries and international organisations in its multiannual programming and annual work programs.[12]

To maximise the usefulness of Europol's information obtained from trusted third countries and strengthen Europol's international role in the fight against serious crime and terrorism, Regulation (EU) 2018/1862 on the establishment, operation and use of SIS in the field of police cooperation and judicial cooperation in criminal matters [13] was amended in 2022[14], introducing a new category of alerts: the **information alerts in the interest of the Union**. At the same time, Regulation (EU) 2022/991 assigned as Europol a new task: to 'support […] Member States in processing data provided by third countries or international organisations to Europol on persons involved in terrorism or serious crime and to **propose the possible entry by the Member States**, at their discretion and subject to their verification and analysis of those data, **of information alerts on third-country nationals in the interest of the Union (information alerts) in the Schengen Information System (SIS)** …'.

Box 1 presents hypothetical scenarios that illustrate how these provisions are expected to help law enforcement in practice.

---

10 See ProtectEU: a European Internal Security Strategy, COM(2025) 148 final of 1 April 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0148.

11 See, for example, Article 25(4a) ER providing the possibility for Europol to transfer data to third countries upon a self-assessment of Europol that all the circumstances surrounding the transfer of personal data and has concluded that appropriate safeguards exist with regard to the protection of personal data and Article 25(5) ER extending the scope of the exceptional cases where Europol can ad hoc transfer in duly justified cases (categories of) data to third countries and international organisations.

12 Articles 12(2) ER.

13 Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312, 7.12.2018, p. 56, ELI: http://data.europa.eu/eli/reg/2018/1862/oj.

14 Regulation (EU) 2022/1190 of the European Parliament and of the Council of 6 July 2022 amending Regulation (EU) 2018/1862 as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union, OJ L 185, 12.7.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1190/oj.

Box 1 – Case scenarios for the application of Article 4(1)(t) ER

Case scenario I: Terrorism suspect linked to ISIS in Syria

US authorities provide to Europol information on a third-country national who is being detained in detention facilities in northeast Syria and based on the collected battlefield information, suspected of having committed terrorist offences, including membership of a terrorist organisation and involvement in terrorist acts. Europol analyses the information received, verifying that: (a) there is no alert on the suspect in the SIS, (b) the information meets the established threshold of quality, reliability, accuracy and relevance, and finally (c) the suspect in question intends to commit, is committing or may commit any of the offences listed in Annex I ER. This verification includes contacting the competent US authorities to obtain updates and confirmations as necessary. Europol makes available the information it holds to Member States and proposes entering an information alert in the SIS, which results in the suspected individual in question being subject to an 'information alert' which is available in real-time to end-users of SIS.

Case scenario II: Suspect of core international crime committed during the war in Ukraine

Ukraine provides Europol with information on an individual who is being investigated or even prosecuted in Ukraine for having committed a core international crime (genocide, crime against humanity or war crime) in the context of the war started by the Russian Federation. Europol conducts a thorough analysis of the information received, verifying that: (a) there is no alert on the suspect in the SIS, (b) the information meets the established threshold of quality, reliability, accuracy and relevance and finally (c) the suspect in question intends to commit, is committing or may commit any of the offences listed in Annex I ER. This verification includes contacting Ukraine to receive updates and confirmations as necessary. Europol makes available the information it holds to Member States and proposes entering an information alert in the SIS, which results in the suspected involvement of the third-country national in question being flagged to the SIS end-users due to participation in a core international crime.

Source: Europol, Response to DG HOME request for Information dated of 1 March 2025

The provisions of Article 4(1)(e) ER are complemented by the obligation of Member States to **inform**, within 12 months from Europol's proposal, **other Member States** and **Europol on the outcome** of the verification and analysis of the data and on whether an alert has been entered in the SIS, as well as by a **periodic reporting mechanism**. Member States are obliged to inform Europol of any information alerts entered in the SIS and of **any match or hit**[15] on such information alerts, with the possibility to **inform, through Europol, the third-country or international organisation** that provided the data leading to the entry of the information alert, of hits on such information alert, following the procedure set out in Regulation (EU) 2018/1862.

In fact, certain information, especially when the individual concerned is not an EU citizen and there is no relation with a national investigation, is shared by the third country only with Europol, which in turn processes the data and shares the analysis results with all Member States. The new provisions aimed to **maximise the exploitation of information** received by Europol from third countries by **facilitating accessibility to Europol data** for law enforcement authorities. It complements other measures, such as the European Search Portal (ESP) and the **interoperability framework**[16] between EU information systems for security, border, and migration management, to address the structural shortcomings related to these systems that impede the work of national authorities, notably border guards.

[15] A '**match**' means that a search has been conducted in SIS by an end-user and has revealed an alert entered into SIS by a Member State; and data concerning the alert in SIS match the search data. A '**hit**' is any match that has been confirmed by the end-user; or the competent authority in accordance with national procedures, where the match concerned was based on the comparison of biometric data; and further actions are requested.

[16] Regulation (EU) 2019/818; OJ L 135, 22.5.2019, p. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

The **SIS** was established in 1985 and implemented in 1995 as the primary compensatory measure for an area without internal borders under the **Schengen** architecture, to ensure a high level of security within the area of freedom, security, and justice. **Only Member States**, as well as the Schengen Associated Countries, can **enter alerts in the SIS**. However, consultation of the SIS is also possible for Europol and Frontex. Since March 2021, Member States have shared with Europol search matches[17] on SIS alerts related to terrorist offences. Europol then exchanges supplementary information with countries on SIS alerts related to terrorist offences through the SIRENE bureaux.

Today, the SIS is the most widely used database in Europe for law enforcement, border control, and migration. Therefore, it serves as a key additional dissemination channel, enabling outreach to a broader circle of law enforcement officers across borders, compared to similar and complementary international police databases, such as Europol's own information system (EIS) or the INTERPOL Information System (see Table 1). What is most important is that **all border guards** at the external borders not only have access to the Schengen Information System (SIS) but are also legally **required to consult it when conducting border checks under the Schengen Borders Code (SBC)**. The same obligation applies to the INTERPOL Stolen and Lost Travel Documents (SLTD) database, but not to the Europol Information System (EIS) and other watchlists.[18]

Table 1 – Comparison of the number of searches in the EU and international police databases

	Schengen Information System (SIS) Main users: 27 EU Member States, 4 SACs, Europol and Frontex – Police and other authorities	**Europol Information System (EIS)** Main users: 26 Europol Member States, EU agencies and bodies – Police	**INTERPOL databases** Main users: 196 INTERPOL member countries – Police
2019	6.6 billion	5.3 million	7.4 billion
2024	15 billion	12.7 million	3 billion

Source: eu-LISA, SIS Annual Reports; Europol, Consolidated Annual Activity Reports; INTERPOL, Annual Reports (see Annex I).

Note: It is essential to note that the circles of users differ, and in the case of INTERPOL, authorities from third countries are also included. The information included is the same to a certain extent. The number of searches in INTERPOL databases decreased by over 50% from 2023, from 7 billion to 3 billion.

3.2. Innovation - Articles 18(2)(e) and 33a ER on the processing of personal data by Europol for innovation and research projects

Technological developments present both enormous opportunities and considerable challenges to the EU's internal security[19] and have had such a profound impact on criminality as to alter even the deep nature, 'DNA', of serious and organised crime threats.[20] Criminals are quick to integrate new technologies into their operations, creating novel business models and refining their tactics. At the same time, these advancements offer **unprecedented opportunities for law enforcement**

17 See footnote 15 above.

18 Article 8(3)(a)(1) and (2) of Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 77, 23.3.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/399/oj.

19 Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024, available online under Internet Organised Crime Threat Assessment (IOCTA) 2024 | Europol.

20 Europol, EU SOCTA 2025, p. 19.

to enhance its capabilities. Therefore, research and innovation play a crucial role in internal security by developing solutions to counter emerging threats and to keep pace with the rapidly evolving forms and *modus operandi* of criminal networks, including those arising from the misuse of technology. The Union has invested, and will continue to invest, in the development of innovative tools through EU-funded security research and innovation, under ProtectEU, the European Internal Security Strategy.[21]

Established in late 2019, at the mandate of the Justice and Home Affairs ministers of the EU Member States, the **Europol Innovation Lab (EIL)**[22] aims to drive Europol's commitment to law enforcement innovation. Regulation (EU) 2022/991 introduced substantial amendments to the Europol Regulation to strengthen Europol's mandate for innovation, so as to both support the capabilities of the new Europol Innovation Lab (EIL) itself and promote synergies with other research and innovation activities at the EU level, including notably in the Commission, under the **EU Innovation Hub** for Internal Security[23].

A key precondition for developing reliable technologies for law enforcement to combat crime is the availability of high-quality datasets that allow their effectiveness to be empirically tested. Unreliable or biased datasets risk leading to poor technology.[24] Against this background, **Article 18(2) ER,** which regulates the purposes of information processing activities at Europol, was amended to enable Europol to **process (operational) personal data for research and innovation projects**. Articles 18(3a), 30(2) and (3), ER and Article 33a ER define the conditions for such processing.

Article 33a ER established strict safeguards to ensure that Europol processes data in accordance with the **principles of transparency, explainability, fairness, and accountability**. Article 33a(2), **letter (d)**, ER mandates in essence the establishment of a **sandbox environment**, by requiring that any personal data processed in the context of the project shall be temporarily copied to a **separate**, **isolated** and **protected data processing environment** within Europol for the sole purpose of carrying out that project. Data may be accessed only by specifically authorised Europol's staff and, subject to technical security measures, by specifically authorised staff of the competent authorities of the Member States and EU agencies. Data cannot be transmitted or transferred, nor can it lead to measures or decisions affecting the data subjects as a result of their processing. It must be erased once the project is concluded or the time limit for storing personal data has expired.

The administrative process ensures effective oversight by various actors of the use of this new possibility but also generates a significant administrative workload. Any project needs the **approval of Europol's executive director** subject to the completion of a **data protection impact assessment** (**DPIA**), the consultation of the fundamental rights officer (**FRO**) and the data protection officer (**DPO**), the information of the European data protection supervisor (**EDPS**) and Europol **management board** as well as the consent from the **data owner**, i.e. the entity having provided the personal data to Europol.[25]

3.3. Criminal investigations - Articles 18(6a) and 18a ER on the analysis by Europol of large and complex datasets ('big data')

In its role as the **EU criminal information hub**, Europol not only facilitates the collection and exchange of information but also helps **increase the effectiveness of investigations through advanced data analysis**, detecting links between criminal offences and criminal networks across

---

21 COM(2025) 148 final of 1 April 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0148, p. 9.

22 https://www.europol.europa.eu/how-we-work/innovation-lab.

23 See, in particular, Article 4(1)(v) and (w) ER.

24 SWD(2022) 543 final of 9 December 2020, p. 29.

25 Article 33a(2), letters (a) to (c), ER.

borders that are not visible at a national level. These capabilities support Member States by enriching the information available for their criminal investigations.

With the extensive and intensive use of technology, **large and complex datasets have become the new normal in all aspects of life**. Crime is no different: criminals use and rely on technology, but also hide behind it.[26] Investigations into organised crime or terrorism face the challenge of analysing terabytes of data, including audio, video, and machine-generated data seized during investigations. For example, in the joint investigation to dismantle the EncroChat network[27], investigators analysed millions of messages that criminals exchanged to plan serious crimes. Against this background, the availability of the necessary Information and Communication Technology (ICT) tools, expertise and resources to analyse large and complex datasets (known in technical jargon as 'big data') is key for law enforcement and judicial authorities.

At the end of 2020, the European data protection supervisor (EDPS) raised concerns about the conditions for the processing of big data by Europol. While the Europol Regulation did not impose any restrictions *per se* on the analysis of big data, it lacked structured provisions setting out proportionate conditions for analysing large and complex datasets received from Member States and other EU agencies and bodies.

The most **critical point** was the **compliance with the requirement of data subject categorisation (DSC)** of the storage of large and complex datasets in **Europol Information System** (EIS).[28]

The categorisation of the information received by Europol is **typically** already **done** by data providers, such as **Member States** or **EU bodies and agencies,** before they transfer the personal data.[29] Under EU law, they are all required to perform Data Subject Categorisation (DSC) for their own processing and investigations, regardless of the data transfer to Europol, and based on equivalent yet not identical rules to those of Europol (see Box 2). For large and complex datasets, manual processing is a resource-demanding and time-consuming exercise, though. Analysing the data in a single mobile phone can take, in a semi-automated way, up to three days, and even hundreds of mobile phones can be seized during an investigation.[30] The DSC **for big data** is **not always possible,** due to the sheer amount of data or the way data is (un)structured or a lack of resources, or it may otherwise manually **take too long**. The only possibility is to first analyse the data in more depth from an operational point of view, or to understand links, also in an automated way, by cross-checking available data.

The **practical impossibility** of swiftly and manually processing **large and complex datasets to perform data subject categorisation (DSC)** made it necessary to find a tailored solution to handle vast amounts of data in a manner compatible with the Europol Regulation, and more generally, with the Charter.

Box 2 – Data subject categorisation (DSC) requirements for Europol, competent authorities and other EU bodies and agencies

In the case of Europol, data subject categorisation is used to verify **whether a given dataset contains personal data belonging to the categories of data subjects listed in Annex II ER**.

26 Europol, EU SOCTA 2025, *passim*.

27 https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochatcommunications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized.

28 EDPS Decision on the own initiative inquiry on Europol's big data challenge of 5 December 2020, see EDPS Decision on the own initiative inquiry on Europol's big data challenge | European Data Protection Supervisor.

29 Member States transfer data to Europol via Europol's Secure Information Exchange Network Application (SIENA), and the Data Subject Categorisation is implemented as a mandatory field in SIENA.

30 See MS reply to Question 9 of the Short Questionnaire of 2 June 2025, Annex III.

Anne II is articulated into two parts:

Annex II, part A, includes an exhaustive list of categories of personal data and categories of data subjects whose data may be collected and processed to cross-check aimed at identifying connections or other relevant links between information related to: (i) persons who are **suspected of having committed or taken part in a criminal offence** in respect of which Europol is competent, or who have been convicted of such an offence; (ii) persons regarding whom there are **factual indications or reasonable grounds to believe that they will commit criminal offences** in respect of which Europol is competent]. They include:

- persons who, in accordance with the national law of the Member State concerned, are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence;
- persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences in respect of which Europol is competent.

Annex II, part B, is an exhaustive list of the categories of personal data and categories of data subjects whose data may be collected and processed for the purpose of analyses of a strategic or thematic nature, for the purpose of operational analyses or for the purpose of facilitating the exchange of information as referred to in points (b), (c) and (d) of Article 18(2). They include:

- persons who, pursuant to the national law of the Member State concerned, are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence;
- persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences in respect of which Europol is competent;
- persons who might be called on to testify in investigations in connection with the offences under consideration or in subsequent criminal proceedings;
- persons who have been the victims of one of the offences under consideration or with regard to whom certain facts give reason to believe that they could be the victims of such an offence;
- contacts and associates; and
- persons who can provide information on the criminal offences under consideration.

Under Article 6 of the Law Enforcement Directive[31] (LED), Member States' competent authorities have the same obligation but only, **where applicable and as far as possible**, to make a clear distinction between personal data of different categories of data subjects, such as: (a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence; (b) persons convicted of a criminal offence; (c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and (d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).

Identical provisions to Article 6 LED apply to the **European Public Prosecutor Office (EPPO)** under its mandate[32], i.e. the EPPO is obliged to comply with DSC requirements '**where applicable, and as far as possible**', and under Article 73 EUDPR.

Under its mandate, **Eurojust** may - **in exceptional cases, for a limited period of time which shall not exceed the time needed for the conclusion of the case in relation to which the data are processed** - also process operational personal data other than the personal data relating to the

[31] Directive (EU) 2016/680, OJ L 119, 4.5.2016, pp. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.

[32] Article 51 of Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31.10.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj.

circumstances of an offence, where such data are **immediately relevant to and are included in ongoing investigations which Eurojust is coordinating or helping to coordinate and when their processing is necessary**.[33]

The EDPS did not question, *per se,* the lawfulness of the processing of big data by Europol.[34] The concern was that, in the absence of a specific legal retention period for data without DSC, Europol applied the general **three-year retention period,** in accordance with Article 31(2) ER. In its decision of 3 January 2021[35], the **EDPS** concluded that it would be more proportionate to apply, **by analogy,** the shorter **six-month retention period** under Article 18(6) ER.[36]

Without legislative changes, the perceived **legal uncertainty** and the **short retention period** could have **negatively impacted Europol's capacity to provide analytical support with big data,** reducing the Agency's ability to detect cross-border links with other crimes and with known criminals and terrorists in different Member States.[37] To counter such risk, Regulation (EU) 2022/991 introduced specific conditions for the analysis of datasets without DSC.

Balancing personal data protection requirements with Europol's operational business continuity, to provide both more clarity and more flexibility, Regulation (EU) 2022/991 set out structured conditions for the application of DSC, providing for the rules to be applied by Europol for processing personal data received without prior DSC.

First, by way of derogation from the general rule, Article 18(6a) ER explicitly provides the possibility to process personal data received without DSC only for **up to 18 months**, with a possible extension of up to 36 months in justified cases, solely for the **purpose of completing the DSC**. Article 18(6a) ER does not make explicit reference to large and complex datasets but applies, more generally, the '**strict necessity**' test, *i.e.* the derogation applies when strictly necessary.

Second, by way of derogation from the general rule, Article 18a ER provided that Europol can process personal data received from a **competent authority,** the European Public Prosecutor's Office (**EPPO**) or **Eurojust**, where necessary for the support of an **ongoing criminal investigation**, without any need to perform the Data Subject Categorisation (DSC), if not already provided, and beyond the categories listed in the Europol Regulation. Europol can process the data through **operational analysis**, or in exceptional and duly justified cases, by **cross-checking** to identify connections or other relevant links. This derogation catered for the asymmetries between the rules on DSC applicable to Europol, on the one hand, and those for the competent authorities, the EPPO, and Eurojust, on the other hand.

---

33 Article 27(3) of Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, OJ L 295, 21.11.2018, p. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj (the 'Eurojust Regulation' or 'EJR').

34 See in particular EDPS statement at the JPSG meeting held in Paris on 28 February 2022: '[…] we have never used in any of our decisions any statement that the data was unlawfully processed by Europol by purpose. We spoke about the problem of the interpretation of the Regulation …'. recording online available at https://videos.assemblee-nationale.fr/video.11933410_621c93de8de70, see statements at 02:03:22 and 02:07:16, accessed on 30/06/25.

35 https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/edps-orders-europol-erase-data-concerning_en.

36 The six-months period was the result of an interpretation by analogy of the time limit under Article 18(6) ER ('Europol may temporarily process data for the purpose of determining whether such data are relevant to its tasks and, if so, for which of the purposes …. The time limit for the processing of such data shall not exceed six months from the receipt of those data'.). The new Articles 74a and Article 74b ER set out a new retention period also for data held by Europol at the date of entry into force of Regulation (EU) 2022/991, i.e. June 28, 2022, although received before. See also in this regard the pending action for invalidity brought by the EDPS before the Court of Justice, case C-698/23 P.

37 SWD(2020) 543 final of 9 December 2020, p. 28.

In addition, Article 18(5a) of the ER, in combination with Article 73 of the EUDPR, clarified the conditions of the general DSC: Europol is tasked, where applicable and as far as possible, with making a clear assignment of personal data to a specific category of data subjects. In practice, as a rule, Europol should determine the precise role in the criminal activity (for example, whether a person is a suspect, a victim or only a witness) for each person whose personal data will be processed and not in an aggregated way (for example, when it is established that an entire set of data is entirely relevant for a criminal investigations).

3.4. Cooperation with third parties - Articles 26, 26a and 26b ER on cooperation between Europol and private parties

Criminals increasingly abuse the (cross-border) services of private parties – internet-based services, as well as financial services, and classical telecom services – for their illegal activities. Consequently, **private parties hold a large amount of personal data relevant to criminal investigations**. In particular, the internet has created a public space that is in private hands, making it difficult to enforce rules online for law enforcement purposes as they do offline.[38]

Against this background, **cooperation between law enforcement authorities and private parties** has become **indispensable.** As set out in the ProtectEU strategy, it will be essential to reinforce partnerships with the private sector to facilitate the exchange of information. Police Chiefs have also called, in their joint statement on the future of Europol, for Europol to serve as a '**vital gateway for obtaining information from private entities**'.[39] The nature of the collaboration varies from sharing information to providing commercial open-source data, and from involvement in research and innovation projects to delivering services that support corporate functioning.[40] For example, in 2025, Europol successfully disrupted Lumma Stealer, the world's most significant infostealer threat, through cooperation with Microsoft, which had identified over 394 000 Windows computers globally infected by the Lumma malware.[41]

Regulation (EU) 2022/991 introduced **additional possibilities** for Europol to exchange personal data with private parties. Previously, Europol could receive personal data from private parties only via a Europol National Unit (ENU), or through pre-identified contact points or authorities of third countries or international organisations. The purpose of Europol's processing was limited to identifying the relevant ENU, or the third country and international organisation contact point or authority that could assume responsibility for the case.

The **amended provisions of Article 26 ER broadened Europol's task,** enabling it to comprehensively pre-process the data (including personal data). A primary purpose of the processing has remained to identify the concerned Europol National Unit (ENU). Europol is also permitted now to enrich the information with its own analysis to facilitate further processing of a case at the national level.

The new Article 26a introduces special conditions for **online crisis situations** and Article 26b ER addresses the **online dissemination of online child sexual abuse material**. In those cases, Europol may assist Member States by processing personal data directly received from private parties. In both cases, Europol may also transfer personal data to private parties on a case-by-case basis.

---

38 SWD(2020) 543 final of 9 December 2020, pp. 16-17.

39 See ProtectEU: a European Internal Security Strategy, COM(2025) 148 final of 1 April 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0148, p. 6, and

40 Europol, cooperation with private parties, 31 May 2023, EDOC #1306090v13. See also Milieu Consulting, study on the practice of direct exchanges with of personal data between Europol and private parties, Final Report, September 2020.

41 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma. Further examples are provided in the accompanying Staff Working Document.

Regulation (EU) 2022/991 included the possibility of using Europol's infrastructure for the exchange of information between competent authorities and private parties, as well as the ability for Europol to request that Member States obtain, in accordance with their national laws, personal data from private parties.

These provisions complement other initiatives, such as the Terrorist Content Online (TCO) Regulation[42] and the Digital Service Act (DSA)[43]. The objective to promote the involvement of private parties in the fight against crime and facilitate lawful access to data in line with 'the ambition of a change of culture in security' (**whole-of-society approach**) is also a key element of **ProtectEU**, a European Internal Security Strategy.[44]

Box 3 – Cooperation with private parties under the TCO Regulation and the Digital Services Act

In June 2021, the European Parliament and the Council adopted Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online (**TCO Regulation**). It aims to ensure that TCO available to the public is removed swiftly and, in a cooperative and coordinated manner among all EU Member States, Europol and hosting service providers (HSPs). The Regulation applies to all HSPs offering services in the EU, regardless of whether they are established in an EU Member State.

The TCO Regulation establishes rules and obligations for the competent authorities of Member States and HSPs to address the misuse of hosting services for the dissemination of TCO. One of the main provisions gives the competent authorities of Member States the power to issue removal orders (ROs), requiring HSPs to remove TCO or disable access to it in all EU Member States within one hour of receipt of an RO. According to **Article 14 TCO Regulation** on the 'cooperation between hosting service providers, competent authorities and Europol', competent authorities are to exchange information, coordinate and cooperate and, **where appropriate, with Europol, with regard to removal orders.** The TCO also asks **HSP to transmit information concerning terrorist content to Europol in relation to an imminent threat to life**, which can include personal data.[45]

The TCO Regulation became applicable in all EU Member States on 7 June 2022, shortly before Regulation (EU) 2022/991.

In October 2022, the European Parliament and the Council adopted Regulation (EU) 2022/2065 on a Single Market for Digital Services (**Digital Services Act - DSA**) to set harmonised new rules for all digital services that operate in the EU. The proposal puts forward measures for countering illegal content online and introduces under **Article 18 DSA** obligations for HSP to **report suspicions of criminal offences to the law enforcement or judicial authorities of the Member State(s) concerned**, once the HSP becomes aware of a threat to the life or safety of person or persons; should the Member State concerned be unclear, the HSP must report it to the authorities of the Member State in which the company is registered in the EU, **or to Europol**, or both.

The DSA entered into force on 16 November 2022, and its rules became fully applicable from February 2024.

3.5. Internal and external oversight on compliance with fundamental rights

Regulation (EU) 2022/991 reinforced the obligation for Europol under the Treaty on European Union (TEU)[46] to respect the fundamental rights and freedoms enshrined in the Charter and introduced new safeguards, including **enhanced oversight**, **to ensure compliance with fundamental rights and freedoms**.

42 Regulation (EU) 2021/784; OJ L 172, 17.5.2021, p. 79, ELI: http://data.europa.eu/eli/reg/2021/784/oj.
43 Regulation (EU) 2022/2065; OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.
44 See ProtectEU: a European Internal Security Strategy, COM(2025) 148 final of 1 April 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX: 52025DC0148, p. 2.
45 Article 14 TCO Regulation.
46 Article 6 and 51 TEU, in combination with Article 51(1) of the Charter.

In essence, Europol's new powers for the processing of personal data went hand in hand with the **alignment** of the Europol Regulation **with the data protection standards** under the **EUDPR**. In 2018, the EUDPR introduced data protection rules applicable to the EU Institutions and bodies, as close as possible to the modernised data protection rules adopted only two years before for the national public sector, as laid down in Regulation (EU) 2016/679[47] (the 'GDPR') and Directive (EU) 2016/680[48] (the 'LED'). The EUDPR aimed to **ensure a consistent approach to protecting and facilitating the free movement of personal data in the EU**. Chapter IX of the EUDPR, in the areas of law enforcement cooperation and judicial cooperation in criminal matters, did, however, not apply immediately to Europol pending a review of the need to propose changes to the Europol Regulation by 30 April 2022.[49]

The most important changes for Europol under the new data protection regime concern the amended or new provisions on the internal compliance ensured by the **data protection Officer (DPO)** and the extension of powers of the **European data protection supervisor (EDPS)**, including the need for **prior consultation of EDPS** (Article 39 ER), in combination with Article 90 EUDPR, and for **data protection impact assessment** (DPIA), and the **right of access** for the data subject (Article 36 ER), which gives the possibility for data subjects to exercise their data subject access rights directly to Europol also for data provided by Member States.

Box 4 – New conditions for the prior consultation of the EDPS

Under Regulation (EU) 2022/991, the oversight of the European data protection supervisor (EDPS) under Article 39 ER was strengthened, including by making mandatory for Europol to consult the EDPS **before any new type of processing** and:

(a) a data protection impact assessment […] indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or

(b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of the data subject.

At the same time, other conditions for a prior consultation of the EDPS introduced **some flexibility to ensure the proportionality** of the requirement of a prior consultation insofar as, first, 'specific risks'[50] should no longer suffice but that only '**high risks**' should trigger the need for prior consultation, second, the time for issuing a prior consultation opinion was reduced from four months[51] to the current maximum **2.5 months**[52], and, third, it is possible, in exceptional circumstances, for Europol **to launch processing operations after the prior consultation has been initiated** but **before the EDPS has delivered its opinion** in cases where the processing operations have substantial significance for the performance of Europol's tasks and are **particularly urgent and necessary** to prevent and combat an immediate threat of a crime or to protect vital interests of the data subject or another person[53]. In such cases, the written advice of the EDPS shall be taken into account retrospectively, and the way the processing is carried out is to be adjusted accordingly. The DPO is to be involved in assessing the urgency of such processing operations and to oversee the processing in question.

Through this legislative reform, the provision for prior consultation of the supervisor by Europol was **aligned** with the corresponding provision in **Article 28(1) LED**.

Source: Europol DPO, 2022 Annual Report, pp. 20-21

47 OJ L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

48 OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.

49 Articles 2(3) and 98 EUDPR.

50 Article 39(1) ER in the version in force before 28 June 2022.

51 Article 39(3) ER in the version in force before 28 June 2022.

52 Article 39(3), third subparagraph, ER, as amended in 2022, in combination with Article 90(4) EUDPR that foresees a regular period of 6 weeks from receipt of the request, that may be extended by a month.

53 Article 39(3), first subparagraph, ER.

Complementary to the new data protection safeguards was the establishment of the new position of a **Fundamental Rights Officer (FRO)**, under Article 41c ER, in line with the mandates of other Union agencies[54]. The FRO is *inter alia* entrusted to inform the Executive Director about possible violations of fundamental rights in the course of Europol's activities.

Additionally, **the democratic oversight and accountability** was **reinforced** through the political monitoring of Europol's activities by the **European Parliament and national parliaments**, as provided for under Article 88(2), second subparagraph, TFEU. Regulation (EU) 2022/991 strengthened the monitoring by the **Joint Parliamentary Scrutiny Group** (JPSG)[55], for example, by providing for the JPSG's mandatory consultation on the Europol's draft multiannual programming and work annual program, the possibility for the JPSG to address non-binding specific recommendations to Europol, and submit them to the European Parliament and national parliaments, and the establishment of a consultative forum to assist the JPSG, upon request, by providing independent advice on fundamental rights matters.

4. State of play of the operational implementation of Europol's new data protection powers and tasks provided for in Regulation (EU) 2022/991

4.1. Article 4(1)(t) ER on the Schengen Information System (SIS) information alerts on third-country nationals upon proposal by Europol

As of 30 June 2025, the possibility for Europol to propose to Member States the Schengen Information System (SIS) information alerts in accordance with **Article 4(1)(t) ER is not yet operational** as the technical implementation is ongoing.

In **2023**, Europol's Management Board adopted a decision to implement the legal requirements regarding the criteria for the possible proposal by Europol of Schengen Information System (SIS) information alerts on third-country nationals. In 2024, the Commission amended the SIS implementing decisions, incorporating the procedures for the information alert into the SIS framework.

However, the 2022 amendments to Regulation (EU) 2018/1862 also require technical adjustments to the Schengen Information System (SIS) by the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) for the Central System and implementation by Member States in their national systems. **Pending the notification by eu-LISA of the successful completion of all testing activities**, and the notifications on the completion of implementation by both eu-LISA and the Member States, as well as Europol, the Commission has not yet adopted the decision setting the date from which Member States may start entering information alerts on third-country nationals in the interest of the Union.[56] Europol is finalising the Data Protection Impact Assessment (DPIA) in view of the prior consultation of the EDPS[57] in the course of **2026,** as this is currently the expected date of entry into operation of these provisions.

Insofar as Article 4(1)(t) ER allows a wider availability and diffusion of Europol's information, the benefits are proportionate to the relevance of the information collected by the Agency. In this regard, this new task is arguably even more critical today than at the time of the adoption of Regulation (EU) 2022/991, thanks to the **ongoing cooperation between Europol and third countries, as well as the implementation of new projects**. For example, under the existing international agreement governing the exchange of personal data, **Europol maintains intensive and effective cooperation with the US**. The exchange of personal data is done in accordance

---

54 See e.g. Article 109 Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, OJ L 295, 14.11.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/1896/oj.

55 See https://www.europarl.europa.eu/relnatparl/en/eu-agencies-oversight/jpsg-on-europol.

56 See Articles 37a and 79(7) of Regulation (EU) 2018/1862, as amended by Regulation (EU) 2022/1190.

57 Europol, Reply to DG HOME follow-up Request for Information of 26 May 2025, p. 2.

with applicable legal frameworks, with full respect for fundamental rights and the EU's data protection standards. The US has shared a substantial volume of information with Europol concerning individuals suspected of involvement in terrorist activities. The US has also shared targeted data on specific categories of individuals suspected of involvement in terrorist activities.

The new task under Article 4(1)(t) ER will **strengthen Europol's capacity to receive, process, analyse, and share information with Member States**, not only from the US but also from other **third countries** and **international organisations**, in a more targeted manner. Europol has adopted a **new External Relations Strategy 2025+,** as part of its Single Programming Document for 2025-2027, aiming to enhance its cooperation with external partners more flexibly, while still based on the operational needs of Member States.[58] Between 2022 and 2024, the Commission continued to prioritise **negotiating international agreements** that enable the exchange of personal and non-personal data between Europol and competent authorities in third countries. The relevant Agreement with New Zealand entered into application on 15 August 2024. Following the Council's authorisation to open negotiations for international agreements with thirteen countries, the Commission aims to strengthen law enforcement cooperation with Europol's priority countries through these agreements.[59] Additionally, a cooperation agreement with INTERPOL is currently under negotiation.[60]

4.2. Article 18(2)(e) ER on processing of personal data by Europol for innovation and research projects

The implementation of Article 18(1)(e) regarding Europol's processing of personal data for innovation projects could not commence immediately upon the entry into force of Regulation (EU) 2022/991. As a **precondition** to the processing of personal data for research and innovation projects, **Europol set up a research and innovation 'sandbox' environment, named ODIN (Operational Data for Innovation)**, for the implementation of the safeguard under Article 33a(2)(d) ER.

Europol **completed the sandbox** environment in **2023,** and the development of the first tool using the sandbox was only recently completed. As explained by Europol[61], ODIN is an 'innovation pipeline' to validate potential new solutions swiftly. It allows for a safe and controlled data processing environment where Europol and law enforcement authorities can experiment with new ideas and technologies. It has significant potential benefits, enabling **faster learning and feedback cycles**, **enhancing collaboration** both within the Agency and with external partners, and facilitating co-creation, thereby fostering an agile mindset.

Europol also recalled that 'Member States are provided with benefits in particular through the use of **Europol's Tool Repository (ETR)**. The use of personal data for innovation/research purposes will further lead to the development of tailored and enhanced tooling to address the innovation needs of Member States'.

Box 5 below presents the first example of a project realised by Europol Innovation Lab (EIL), thanks to the possibility of using personal data under the new Article 18(1)(e) ER.

---

58 Europol, Europol Programming Document 2025–2027, adopted by the Management Board of Europol on 10 December 2024, available online under https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2025-2027.pdf.

59 European Commission, DG for Migration and Home Affairs, Annual Activity Report 2024, p. 38.

60 Council Decisions (EU) 2021/1312 and 2021/1313 of 19 July 2021 authorising the opening of negotiations for a cooperation agreement between the European Union and the International Criminal Police Organization (ICPO-INTERPOL), OJ L 287, 10.8.2021, pp. 2; ELI: http://data.europa.eu/eli/dec/2021/1312/oj and OJ L 287, 10.8.2021, pp. 6; ELI: http://data.europa.eu/eli/dec/2021/1313/oj

61 Europol, Reply to DG HOME follow-up request for information of 25 May 2025.

Box 5 – First project: The development of an audio denoising tool

Europol's Innovation Lab was contacted by national law enforcement authorities (LEAs) to support them in the development of a software prototype that allows the user to enhance the quality of audio data. The dataset available for training, evaluation, and testing is a set of audio recordings obtained in a law enforcement operational environment. The recordings capture the noise from the road, etc. The aim of the processing is to enhance voice data, e.g. in conversations.
The project aims at developing a prototype tool that assists LEAs' officers. If successful, the resulting prototype will be made available to Member States via the Europol Tool Repository (ETR).
The project investigates algorithms to improve the quality of the output to enable improvements in post-processing.
The goal of the project is to assess available algorithms on their ability to enhance the 'wanted' audio output, such as human speech.
The resulting output will be assessed for quality by a human. The user may need to adjust algorithm parameters, such as filtering settings or compression levels, to achieve the optimal output.

Source: Europol, Reply to DG HOME request for information of 1 March 2025

Europol has announced **three upcoming projects** for which consultations with the Europol Data Protection Function (DPF) and the Fundamental Rights Officer (FRO) are ongoing:

- Face deepfake detection
- Child Sexual Abuse Material (CSAM) Synthetic Image Detector (SID)
- Translation model to enable the translation of a rare language to European languages for law enforcement purposes.

4.3. Articles 18(6a) and 18a ER on the analysis by Europol of large and complex datasets ('big data') and remaining challenges with the Data Subject Categorisation (DSC)

Article 18(6a) ER and Article 18a ER applied to the processing, including notably the analysis of large and complex datasets by Europol, from the date of entry into force of Regulation (EU) 2022/991, on **28 June 2022**. The conditions were set out by Europol's Management Board, after consultation with the EDPS, in its decision of the same date. [62] This Management Board decision was, however, replaced by **a new decision** adopted on **21-22 March 2023**.[63]

Table 2 presents available statistics on the implementation of the new provisions for analysing large and complex datasets. The relevance of the provisions of **Article 18(6a)** is confirmed by the fact that Member States continued to ask Europol's support for the analysis of large and complex datasets without DSC.

Europol received a total number of **new contributions without DSC from Member States, amounting** to **653** (in 2023) and **597** (in 2024). The new provisions had *prima facie* no negative impact on Member States' engagement in carrying out the DSC[64] and indicating it in SIENA[65] when transferring data to Europol. There was no artificial short-term increase (shock) in contributions without DSC, and the number of cases under Article 18(6a) was **steady** compared

62 See Articles 18(6b) and 18a(5) ER.

63 See EDPS, Supervisory Opinion on Europol's Management Board Decisions adopted pursuant to Articles 11(1)(q), 18 and 18a of the Europol Regulation (Case 2022-0923), available online under https://www.edps.europa.eu/system/files/2023-01/22-11-17_edps_opinion_-_2022-0923_e-signed_en.pdf.

64 As stressed by a Member State, '[Member States] can clearly distinguish what kind of data [they] are dealing with, which can be very important in the investigation itself'.

65 Member States transfer data to Europol via Europol's Secure Information Exchange Network Application (SIENA) and the Data Subject Categorisation is implemented as a mandatory field in SIENA.

to equivalent cases before 28 June 2022. Between 2023 and 2024, the share of contributions without DSC decreased by a slight amount. The number of contributions without DSC is not insignificant, due to frequent investigations that seize large amounts of data. Yet, they accounted for a limited percentage, **less than 1%**, **of all contributions** accepted by Europol from Member states (0.85% in 2023 and 0.71% in 2024).

All 26 Member States sent contributions falling under the scope of Article 18(6a), **but to a different extent**. Additionally, Europol conducted the Data Subject Categorisation (DSC) of contributions received from other EU agencies and bodies, third countries, and other external partners.

Article 18a ER has been used for the first and only time in 2024 for a project with the participation of two Member States. The limited use of this Article confirms a proportionate approach to the use of those rules. It also confirms that the adoption of Article 18a proved justified.

Table 2 – Statistics on contributions provided by Member States without DSC

	Art. 18(6a) Nr of contrib.	**Art. 18a** Nr of contrib.	**Share of total MS contrib.** %	**MS sending contrib.**	**StDev**	**Average** Nr contrib. per million inhabitants
2023	653	0	0.85 pt	26	2.84	1.5
2024	597 ↓ -8.5%	2 ↑undefined	0.71 pt ↓ -16.5%	26	2.97 ↑ +4.6%	1 ↓ -33%

Source: DG HOME based on data from Europol Annual report on information provided by Member States in accordance with Article 7(11) Europol Regulation in 2023 and 2024, and information provided by Europol

Technical comment: Taking into account the very different sizes of the Member States, the data dispersion (in terms of standard deviation (StDev)) and the average number of contributions per Member State (MS), are calculated based on the number of contributions per inhabitant (million) in each MS. The standard Deviation and average also include the two cases of application of Article 18a ER. The value of the standard deviation is context dependent. In this case, a value of 3 indicates rather significant deviations from the average, or in other words, that data are spread close to the extreme values rather than around the average values.

In the first three years of implementation of the provisions introduced by Regulation (EU) 2022/991, Europol always respected the time limit of 18 months for the processing of per-sonal data without DSC. Europol remarked: 'The fact that the **18-month** timeframe has **not yet been exceeded** demonstrates how rigorously Europol handles the corresponding data review of the information Member States and operational cooperation partners entrust to it. However, the extended timeframe of 36 months remains crucial. Given the sensitive nature of the data concerned, the maximum limit of **36 months** serves as an essential **safeguard in terms of legal certainty** and **operational flexibility**, exclusively reserved for **complex investigations** which require **more time** for **the DSC determination**'.[66]

Member States **did not provide any statistics** about the operational results achieved thanks to the implementation of Articles 18(6a) and 18a ER but mentioned examples of major investigations carried out thanks to Europol's analysis of large and complex datasets, such as **EncroChat**, **Sky ECC**, and **Balkan-based criminal networks involved in cocaine trafficking**.

66 Europol, Reply to DG HOME follow-up request for information of 25 May 2025.

4.4. Articles 26, 26a and 26b ER on the exchange of personal data between Europol and private parties

Europol adopted the necessary measures for the timely implementation of the extended possibility to exchange personal data with private parties upon the entry into force of Regulation (EU) 2022/991. In **June 2025, it** adopted its **new strategy on cooperation with private parties.**[67] Based on the information provided by Europol, only Article 26b (3) ER is not applicable for the sharing of hashes is not applicable. Establishing proper processes and communication channels for this purpose is under consideration for the future.[68]

At the request of the Commission, Europol developed a technical solution in 2021 that facilitates the implementation of Regulation (EU) 2021/784 (the 'TCO' Regulation) by Member States. This solution provides a single system connecting all Member States with hosting service providers (HSPs). Known as **PERCI** (*Plateforme Européenne de Retraits des Contenus illégaux sur Internet*), this platform went live on 3 July 2023. It is managed by the European Union Internet Referral Unit ('EU IRU'), and it is used to issue and transmit removal orders.[69]

PERCI is not integrated in Europol Information System (EIS). Currently, there is also **no interplay** between **Articles 26, 26a, and 26b of the ER** and **PERCI**, because the platform only covers exchanges between Europol and private parties with the TCO Regulation as the legal basis. The situation will **change** with the development of a new workflow in PERCI to facilitate the transmission of the notifications stemming from **Article 18 DSA** from the service providers to Europol and the Member States. From a legal point of view, Article 18 DSA applies in combination with Article 26 ER. Europol signed a contribution agreement with the European Commission to initiate the development of an automated workflow in PERCI, supporting the implementation of the Digital Services Act (DSA) related orders in line with Article 18 DSA.[70]

EU-CARES is Europol's **service dedicated to the retrieval, enrichment and dissemination of child sexual abuse-related referrals reported by** Online Service Providers to the United States-based **National Centre for Missing and Exploited Children** (**NCMEC**). EU-CARES retrieves, through a dedicated interface with NCMEC, the content of each referral (textual and media information) concerning potential child sexual abuse-related offences affecting victims or suspects. Both the **media and textual information are processed and enriched with the information held by Europol**. After that, the package containing the original referral plus the compiled enriched information is disseminated to the relevant Member State. The information added to the referral supports the law enforcement authorities in prioritising the high number of referrals received by NCMEC, based on the criticality and importance of the potential offence. EU-CARES is the technical gateway between NCMEC and the connected countries. NCMEC is the provider of the data; thus, Europol cooperates with it to receive updates or address challenges related to the platform (e.g., new versions of the data model being deployed or expected outages in its service). However, the role of other private actors – namely, service providers that refer their information to NCMEC – is of great importance, as their information is crucial in detecting abusers and initiating investigations.[71]

---

67 EDOC#1437881v8b.

68 Europol, Reply to DG HOME follow-up request for information of 26 May 2025.

69 A review of the implementation of the TCO Regulation can be found in the Report on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, COM(2024) 64 of 14 February 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52024DC0064.

70 DG HOME internal information. See also Europol answer to written question from the Member of the European Parliament (MEP), Ms. Saskia Bricmont, to the Joint Parliamentary Scrutiny Group (JPSG) of 21 February 2025, available online under https://secure.ipex.eu/IPEXL-WEB/download/file/8a8629a89526e2e40195283a598f0001/Answer_to_JPSG_written_questions_MEP_Bricmont.pdf.

71 *Ibidem*.

Memoranda of Understanding **(MoUs)** are also an instrument for Europol to **foster strategic cooperation with private sector partners and academia** in countering cybercrime, serious and organised crime and terrorism. Although not legally binding, MoUs provide a framework for structured cooperation and guidelines for both parties to ensure a fruitful partnership in areas of common interest. While not providing the legal basis for the exchange of personal information, the MoU facilitates the exchange of knowledge, expertise, and non-personal information, enhances coordination of joint activities, and ensures visibility for both parties vis-à-vis their relevant stakeholders. The **majority of MoUs** were concluded today in the **areas of cybercrime, financial, and economic crimes**, underlining the importance of cooperation with private parties in tackling crime in these areas.

Table 3 reports available statistics on Europol's cooperation with private parties. In its first report pursuant to Article 16(11) ER in 2023, Europol noted that the exchange of information with private parties had not yet reached a material scale compared to day-to-day operational information sharing, analysis, and overall support activities delivered. While Article **26a** ER has **not been used so far**, cases of **cooperation** with private parties **under the other articles have already sharply increased** in 2024. Notably, this is the case for the submission of private party data to Europol's EFECC (European Financial & Economic Crime Centre), which has increased significantly since the entry into force of Regulation (EU) 2022/991, particularly from private companies and international foundations. These provide valuable intelligence generated by their expert investigative departments, which, after Europol's pre-processing, are passed on to the relevant Europol National Units (ENUs). It includes actionable intelligence for combating sports corruption, intellectual property rights infringements, and excise fraud.[72]

Table 3 – Statistics on the implementation of Articles 26, 26a and 26b ER

	Other **TCO**(1)	Other **URL**(2)	Art 26 ER **DSA**(3)	Art 26 ER **Other than DSA**	Art 26a ER **Online crises**	Art 26b ER **CSE**(4)
2023	11	4 261	169	26	0	[156 456[73]]
2024	22 ↑100%	11 421 ↑168%	508 ↑201%	285 ↑996%	0	605 316
(1) **TCO**: Received contributions under the TCO Regulation in the framework of PERCI						
(2) **URL**: Successful referrals to private parties in the framework of PERCI						
(3) **DSA**: Notifications handled under Art 18 DSA. Art 26 ER is providing the legal basis for the exchange of data referred to in Art 18 DSA.						
(4) **CSE**: Cyber Tips on Child Sexual Exploitation from private parties via EU CARES						

Source: Europol, 2023 Annual Reporting to the Europol Management Board (MB) on the exchange of data with private parties (Article 26(11) ER) and, for 2024, response to the follow-up request for information.

Member States **did not provide any statistics** about the operational results achieved thanks to the implementation of Articles 26, 26a and 26b ER. Despite limited practical experience,[74] Europol and Member States stressed the relevance of the new provisions. Cooperation with private parties proved crucial during the reporting period. These provisions also yielded tangible results, with successful criminal investigations, such as **Phobos and AKIRA**, or most recently, the '**Lumma Stealer**' case (see Box 6).

72 Europol, Cooperation with Private Parties, 31 May 2023, ref. EDOC #1306090v1.

73 Between 4 October 2023 and 31 December 2023. On 4 October 2023, EU CARES, a dedicated tool to exchange data on Child Sexual Exploitation (CSE) went live, since then private parties can directly forward data to Europol on CSE.

74 Five Member States only replied they had experience with the new provisions on cooperation with private parties. See MS replies to Question 1 of the Short Questionnaire of 2 June 2025, in Annex III below.

Box 6 – Europol and Microsoft disrupt world's largest infostealer Lumma

Lumma, the world's largest infostealer, was a sophisticated tool that enabled cybercriminals to collect sensitive data from compromised devices on a massive scale. Stolen credentials, financial data, and personal information were harvested and sold through a dedicated marketplace, making Lumma a central tool for identity theft and fraud worldwide. The Lumma marketplace operated as a hub for buying and selling malware, providing criminals with user-friendly access to advanced data-stealing capabilities. Its widespread use and accessibility made it a preferred choice for cybercriminals looking to exploit personal and financial data.

Between 16 March and 16 May 2025, Microsoft identified over 394 000 Windows computers globally infected by the Lumma malware. In a coordinated follow-up operation […], Microsoft's Digital Crimes Unit (DCU), Europol, and international partners have disrupted Lumma's technical infrastructure, cutting off communications between the malicious tool and victims. In addition, over 1 300 domains seized by or transferred to Microsoft, including 300 domains actioned by law enforcement with the support of Europol, will be redirected to Microsoft sinkholes.

Source: Europol, 5 June 2025: Europol and Microsoft disrupt world's largest infostealer Lumma | Europol

5. Evaluation of the operational impact of Europol's new personal data processing powers and tasks with regard to Europol's objectives under Article 3 ER

5.1. Article 4(1)(t) ER on the Schengen Information System (SIS) information alerts on third-country nationals upon proposal by Europol

At this stage, an evaluation of the tasks provided for in Article 4(1)(t) ER is not possible due to the delayed implementation of that article. At the same time, comments from Europol and Member States demonstrate ongoing support for the potential relevance and added value of these new personal data processing tasks.

During the consultation, both **Europol** and **Member States** expressed very positive views on the ***potential*** **benefits** of the **provisions on information alerts on third-country nationals, which would support law enforcement work,** and many of them also commented extensively on the **relevance** of this measure.[75] As explained by a Member State, 'third countries share information on non-EU subjects with Europol, these individuals are in many cases **unknown in the EU and cannot be linked to a national investigation or case**. Europol's role, with the possibility of proposing a Schengen Information System (SIS) alert, will **cover this gap**. Another Member State commented: 'Europol-initiated the Schengen Information System (SIS) alerts will provide **early warning on high-risk individuals** (e.g., terrorists, violent extremists, organised criminals). They will enable frontline law enforcement authorities (LEAs) units to act on threats not yet flagged by national authorities. They will support LEAs in **targeted checks**, **surveillance**, or **detentions based on intelligence-led Schengen Information System (SIS) alerts**. Enhances border control and internal security through real-time, EU-level risk indicators. Alerts [proposed] by Europol can highlight threats that LEAs may not yet be aware of, based on intelligence from third countries or EU partners. They will strengthen LEAs' **situational awareness at airports, seaports, public spaces, and events**'.

A Member State also stressed that 'Europol's right to propose the Schengen Information System (SIS) information alerts can enhance the capacity to combat cross-border crime and terrorism by leveraging Europol's unique position and analytical expertise. However, **strong safeguards for data protection and fundamental rights** must be enforced. Given the varying data protection standards and legal frameworks in third countries, a **cautious approach is necessary when acting upon or proposing alerts based on such information**'.

[75] See MS replies to Question 2 of the Short Questionnaire of 2 June 2025, Annex III.

Only three Member States referred to a **possible future extension of Europol's prerogatives**, which was proposed in 2020[76], and their comments show that this remains a **controversial matter**. One of them would indeed prefer 'Europol being able to input alerts directly into the Schengen Information System (SIS) rather than proposing it to Member States'. The others argue, to the contrary, that 'this would be an important change in principle as regards the tasking, as this would imply that Europol would also accompany the alert with an action to take. It would probably make more sense to wait for the implementation of the information alerts before trying to add to this possibility'. This matter, however, falls outside the scope of this evaluation and would necessitate amending the Europol Regulation and Regulation (EU) 2018/1862.

5.2. Article 18(2)(e) ER on processing of personal data by Europol for innovation and research projects

At this stage, an evaluation of the tasks provided for in Article 18(1)(e) ER is not possible due to the delayed implementation of those provisions. At the same time, comments from Europol and Member States demonstrate ongoing support for the potential relevance and added value of these new personal data processing tasks.

During the consultation[77], a Member State commented that 'the new mandate for research and innovation establishes Europol as a **central driver for developing the next generation of law enforcement tools** (Innovation Lab). It is a strategic, **long-term benefit for all Member States**'. A few other Member States provided similar comments, for example, one mentioning 'Research and innovation provide all Member States — including those with limited technical capacity — access to cutting-edge innovations developed in a centralised legal EU framework'. A Member State also stressed that 'Europol's support for innovation, in particular the **work of the Innovation Lab**, is **outstanding**'.

5.3. Articles 18(6a) and 18a ER on the analysis by Europol of large and complex datasets ('big data')

During the consultations, most comments provided by Europol and Member States concerned the provisions of Articles 18(6a) and 18a ER, which are the provisions with which they have the most experience.[78] They highlighted the benefits, relevance, and EU added value of Europol's power to analyse large and complex datasets, but also flagged certain **shortcomings in the current implementation of the new provisions that undermine their effectiveness**.

For Europol, '[its] ability […] to analyse large and complex datasets can increase the efficiency of Member States' criminal investigations, in particular where they face gaps in tools, processes or resources. In addition, Member States gain access to an increased criminal intelligence value through Europol's ability to **uncover hidden criminal structures and cross-border links that may not be visible to national authorities alone**. Overall, Europol's strengthened analytical capacity indirectly supports and enhances the investigative infrastructure of national law enforcement agencies, as well as the EU security interests overall, therefore supporting **cohesion across the EU** …'.[79]

Several Member States confirmed this view. For example, a Member State considers that '[t]he most significant, though least publicly visible, benefit comes from the new legal framework for processing large and complex datasets. This provision legally **solidifies Europol's role as the EU's central criminal information hub**. For the police, this means they can lawfully share vast quantities of data seized during major investigations—such as data from servers, computers,

---

76 See, in this regard, COM(2020) 791 of 9 December 2020, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0791:FIN:EN:PDF.

77 MS Replies to Question 4 of the Short Questionnaire of 2 June 2025. A few other MS also provided comments along the same lines, see MS Replies to the Short Questionnaire of 2 June 2025, Annex III.

78 See MS Replies to Question 1 of the Short Questionnaire of 2 June 2025, Annex III.

79 Europol, Reply to DG HOME follow-up request for information of 26 May 2025.

mobile phones, or extensive financial records—with Europol. Europol, in turn, can … legally use its superior analytical resources and advanced technologies to process this data, identify links, and extract actionable intelligence that might be beyond the capabilities of national units'.

Nonetheless, the **Data Subject Categorisation (DSC) requirement remains challenging**. Europol highlighted legal uncertainty around **Articles 18(6a) and 18a ER,** as well as their scope of application. For most Member States, the legal requirements for Data Subject Categorisation are, *per se,* sufficiently clear; however, the problem lies in their **practical implementation**.[80]

Under the guidance of the EDPS, Europol and its Management Board have generally followed a **conservative approach**, for example, as regards the application of the new Article 18(5a) ER that requires, '*where applicable and as far as possible*, to make a clear distinction between the personal data that relate to the different categories of data subjects listed in Annex II [of the Europol Regulation]'. Europol received datasets collected and provided by Member States that, based on judicial direction and respective warrants, were included personal data of persons involved in criminal activities that fall under Annex I ER. In other words, at Member State level, the judicial authorities had determined that **all data was relevant for the case and all data subjects are in one way or another connected to the crime(s)**. Member States considered that, in such cases, the DSC had been provided.[81] Europol would instead assume those cased to possibly fall under the **scope of Article 18(6a) or of Article 18a ER**.

In *very large* investigations, a restrictive interpretation increases the time and costs of the Data Subject Categorisation (DSC) to an extent that, according to some Member States, **may compromise the usefulness of data processing**. During the consultation, a Member State observed, for example, that '[w]hen dealing with large and complex data sets, the **challenges in categorisation,** having in mind the requirements which need to be met, are considerable. Besides the **time and resources (human, technical, and financial)** allocated to implement this task, there are cases where the available information is not complete and structured, or the **source may be non-standardised, resulting in difficulties concerning the identification of data subjects**. Thus, the progress of the investigations will be affected'. Some other Member States also voiced the **same** concerns.

At the same time, for a non-governmental Organisation (NGO), Europol's Management Board decision would have not even addressed all the recommendations by the European Data Protection Supervisor (EDPS) in its implementing decision and the implementation would not be strict enough: 'there is a significant chance that the way in which the provisions in the amended Europol Regulation regarding the processing of datasets lacking a DSC are currently being implemented by Europol does not sufficiently take into account the importance of maintaining a distinction between the categories of persons whose data are processed'.[82]

A Member State also remarked that '[**the negligible use of Article 18a ER**] **seems quite strange** as … the expectation was that this would be a flexible basis for Member States to use in case of important and big investigations. Yet this seems not to be the case'.

In this regard, the limited use of Article 18a ER may arguably reflect the exceptional character of the provisions. However, Europol[83] also recalled the restrictive interpretation by the EDPS in its opinion[84] of 17 November 2022. The EDPS sees Article 18a ER as a stand-alone provision which

---

80 See MS Replies to Question 9 of the Short Questionnaire of 2 June 2025, Annex III.

81 A Member State explains: '… which were always regarded as being data relating to criminals (so DSC was considered to be determined already)'.

82 Meijers Committee, Comment on Europol's Data Subject Categorisation based on the Amended Europol Regulation, May 2024, p. 4, available online at https://www.commissie-meijers.nl/wp-content/uploads/2024/05/CM-comment-Europol-DSC.pdf.

83 First technical meeting between DG Home and Europol staff, on 18 February 2025.

84 EDPS, Supervisory Opinion on Europol's Management Board Decisions adopted pursuant to Articles 11(1)(q), 18 and 18a of the Europol Regulation (Case 2022-0923), available online under

is meant to apply to specific cases ('**ongoing specific criminal investigations**') that require the processing of large and complex datasets, for which Europol is better placed to detect cross-border links, and thus under specific conditions laid down to that purpose by the co-legislators. Accordingly, the EDPS understands that this provision is intended to address extraordinary situations, such as those that prompted the creation of operational task forces (OTFs), including *Fraternité*, *EMMA*, *LIMIT*, [85] or *Greenlight*[86]. In those cases, Europol was provided by Member States with large amounts of information that, in the EDPS's view, fell automatically outside the scope of Article 18(6a) ER. The scope of Article 18a ER would not be defined by whether the datasets received are with or without DSC, but rather by the link to a specific ongoing criminal investigation at the request of the contributor. In practice, this means that **when Europol assigns a Data Subject Categorisation (DSC) and extracts the relevant information, the data cannot be further injected into the Europol Analysis System** under the relevant Analysis Project and processed under Article 18(2) ER as other personal data with DSC completed.[87] The use of the data remains limited to the purpose (investigation) for which it was provided and must be deleted as soon as the investigation is closed.

5.4. Articles 26, 26a and 26b ER on the exchange of personal data between Europol and private parties

During the consultations, Europol and Member States highlighted the benefits, relevance, and EU added value of Europol's cooperation with private parties but also flagged certain **shortcomings in the current implementation of the new provisions that undermine their effectiveness**.

For Europol, its **facilitator role in relation to private parties' cooperation can allow for targeted collaboration**, while enabling **deconfliction across the investigation process**. By positioning itself as a connector, Europol seeks to ensure the timely dissemination of crucial operational criminal intelligence, thereby empowering Member States to respond more effectively to emerging threats. Europol can further enrich the information received from a private party by conducting cross-checks or complementary operational analyses to identify links with ongoing criminal investigations in certain Member States or third countries. Furthermore, in the case of **PERCI**, the EU Platform for the takedown of illegal content online, the **Member States directly benefit from the use of Europol's infrastructure for exchanges** between the competent authorities of the Member States and private parties as per Article 26 (6c) ER.[88]

Several Member States provided positive comments. During the consultation, a Member State commented that 'many Member States have benefited from Europol signing ***Memoranda of Understanding*** **(MoU) with private parties that have improved cooperation'**. For another Member State: 'Once fully implemented, mechanisms for engagement with private entities could open new avenues for detecting and disrupting criminal activities online, particularly in cybercrime and child sexual abuse content'.

In the view of Europol, **challenges** remain in implementing cooperation with private parties. Operational staff at the national level may encounter difficulties with the use of Articles 26, 26a, and 26b ER due to their **length and complexity**.[89] In addition, Europol considers that the Agency

---

https://www.edps.europa.eu/system/files/2023-01/22-11-17_edps_opinion_-_2022-0923_e-signed_en.pdf.

85 Europol, OTF LIMIT, online under New major interventions to block encrypted communications of criminal networks | Europol.

86 Europol, OTF Greenlight/Trojan Shield, https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication.

87 Europol DPO, 2024 Annual Report, pp. 16-17.

88 Europol, Reply to DG HOME first request for information of 1 March 2025, p. 6, and Reply to DG HOME follow-up request for information of 26 May 2025.

89 Europol staff, technical meeting of 18 February 2025.

is perceived as a trusted partner by private parties. However, **private parties have expectations for potential reciprocal benefits in the cooperation**, and with respect to direct information exchange (rather than Member States as intermediary, in view of the provisions of Article 26(1) ER for day-to-day cooperation).[90] In certain domains, such as joint strategic cooperation on cryptography and quantum computing, the mutual benefit of collaboration between law enforcement and private parties is clear to both sides. In other crime areas, the **risks to a private party (to their business model, for example), or the time commitment, could outweigh the benefits for the private party**.[91]

Europol explained that the applicable **legal framework is increasingly scattered across multiple instruments** and includes a growing list of secondary EU legislation and implementing acts. It would be a **challenge for private parties to adapt to established procedures that accurately reflect the complex EU legal requirements**, especially in cases where they are based outside the EU and may be subject to different national laws (i.e. US).[92]

Inefficiencies may result from the **variety of communication channels used by private parties to transfer information to Europol, as well as the security requirements** for these channels more generally.

Also, in the future, Europol may face the challenge of assessing data from private parties that has been pre-processed using Artificial Intelligence applied by private parties. It may need to evaluate whether what has been provided is 'real' or AI-generated. Europol expects that this pre-processing will add complexity to the assessment of such data.

As main challenges, Member State also stressed that 'processing data from private parties under Articles 26, 26a and 26b ER **requires careful consideration of data protection principles and additional coordination with national authorities** … Once fully implemented, mechanisms for engagement with private entities could open **new avenues for detecting and disrupting criminal activities online**, particularly in cybercrime and child sexual abuse content' and, as indicated by another Member State, 'practical impact varies based on Member States' engagement and legal framework'.[93] Some Member States are also more cautious: 'Operational implementation on cooperation with private parties under Article 26 ER, although necessary in certain fields, **requires an in-depth reflection in light of recent international developments, with special caution on sharing of personal data**'.

6. Assessment of the Impact of the implementation of Europol's new personal data processing powers and tasks on fundamental rights

Article 68(3) ER requires the Commission to assess the impact on fundamental rights and freedoms as guaranteed by the Charter of the tasks provided for in the provisions introduced by Regulation (EU) 2022/991.

Available reports as well as the consultation of Member States indicate that Europol **implemented fundamental rights safeguards rigorously,** taking the responsibility to 'effectively transform the perceived dichotomy between policing and the protection of fundamental rights into a positive narrative'[94].

As regards compliance more specifically with the protection of personal data (Article 8 of the Charter), '**Europol's data protection framework is robust and rights-compliant'**: remarked a Member State, supported with similar views by Europol and other Member States.

---

90 Europol, Reply to DG HOME first request for information of 1 March 2025, p. 6.
91 *Ibidem*, p. 7.
92 *Ibidem.*
93 See replies of Member States to Question 3 of the Short Questionnaire of 2 June 2024, Annex III.
94 Europol FRO, 2023 and 2024 Annual Reports.

In 2024, Europol's Management Board adopted the revised DPO implementing rules as one of the implementing acts of Regulation (EU) 2022/991. Europol emphasised the **important role of its DPO** in disseminating knowledge of data protection and ensuring compliance with the new data protection rules.[95]

Generally, during the consultation, most Member States reported having limited experience with the new data protection rules.[96] Yet, several Member States, emphasised the **importance of aligning with the EUDPR for the achievement of Europol's objectives under Article 3 ER**. For one Member State, 'the alignment with Regulation 2018/1725 does not directly force an increase in data sharing — but it **removes key legal and procedural barriers**, promotes trust, and ensures that data flows are legally sound, secure, and rights-respecting. These improvements create a **more predictable and interoperable environment** for information exchange between Europol and Member States. Europol can now act as a trusted intermediary for information coming from private entities (e.g. telecom providers, financial services, tech platforms)'. Another Member State mentions that 'for instance, in an investigation into an organised group involved in drug trafficking, [they] were able to **quickly transmit personal data and related financial records** to Europol because the safeguards and procedures were clearly defined. **In the past, such exchanges were delayed due to differing interpretations of data processing rules**. Now, the harmonised framework allows faster cooperation without legal barriers'.[97]

Another Member State is more critical: 'part of the legal framework on this matter is now to be found in the EUDPR instead of the Europol Regulation, and some of the rules in there are different to a certain extent from the previous ones. However, we don't really see a lot of difference in the way these requests are processed in practice. […] we have the **impression that a changed interpretation of the legislation** (by the Courts and by the EDPS) has **a bigger influence on this than changes in the legislation itself**'.[98]

Europol and its Management Board implemented the new safeguards rigorously from the start, under the guidance of the EDPS. Some stakeholders argued that, with this conservative approach, Europol did not fully utilise the flexibility granted by the legislators.

Europol highlighted during the consultation some shortcomings in the implementation of the new data protection rules, which some Member States also confirmed. Besides the specific challenges presented by the Data Subject Categorisation (DSC), as explained under Section 4.1., Europol and some Member States identified notable legal uncertainty and a **need to streamline the implementation** as regards the data subject access rights and the prior consultation of the EDPS.[99]

Both Europol and six Member States[100] consider the implementation of the new **data subject access rights** as one of the most challenging areas since Europol is now competent to decide on requests even for data provided by the Member States. However, Europol relies on timely feedback from national authorities to process requests for access rights and some Member States complain that the **scope of the access provided by Europol** and the EDPS. Another issue raised by a **few** Member States is the **type of replies provided by Europol to access requests** even when the information itself is not disclosed. There is a risk in the view of Member States to jeopardise their investigations. .

For some Member States, the scope of the obligation to **consult the EDPS** and conduct **data protection impact assessments** (DPIA) stemming from overly restrictive interpretations of

95 Europol, Reply to DG HOME follow-up request for information of 25 May 2025.
96 See MS replies to Question 6 of the Short Questionnaire of 2 June 2024, Annex III.
97 See MS replies to Question 6 and 7 of the Short Questionnaire of 2 June 2025, Annex III.
98 MS Replies to Question 8 of the Short Questionnaire of 2 June 2025, Annex III.
99 See MS replies to Question 8 of the Short Questionnaire of 2 June 2025, Annex III.
100 See MS replies to Question 6 and 7 of the Short Questionnaire of 2 June 2025, Annex III.

Articles 39 ER and 90 EUDPR has generated disproportionate delays and administrative costs. This would be based on the **presumption that any new type of processing of operational personal data would be high risk**, regardless of the possible preventive measures taken to mitigate the risk. According to Europol and some Member States, this interpretation delays and undermines the benefit of data processing by increasing the costs thereof to a point that, according to a Member State: '[t]here is [a perceived] **reluctance to [invest in] innovative digital tools or experimental analysis models**, where Data Protection Impact Assessment (**DPIA**) **constraints outweigh the perceived benefit** [in the short term]'.[101]

Table 4 reports available statistics on the implementation of key areas where Regulation (EU) 2022/991 changed the fundamental rights safeguards.

Table 4 – Statistics on the implementation of key fundamental rights' safeguards

	Data subjects' access requests	Prior consultations of the EDPS	Reports on FR violations
2022	318	• EPRIS • VAT SIREN • Biometric Queries of the Schengen Information System (SIS) II • SIS II Dactyloscopic Searches • PERCI • Data Refinery	n.a.
2023	469 ↑ +47%	• NCMEC Automation* • QUEST+ • Data Refinery	0
2024	483 ↑ +3%	• Europol's Face Recognition Solution (NEO Face Watch) • IVAS BRAIN • IVAS GFMS • Joint operational analysis case (JOAC)	0

Source: Europol Consolidated Annual Activity Reports for 2022, 2023 and 2024.

Note: NCMEC Automation is the first prior consultation carried out under Regulation (EU) 2022/991

In June 2022, Europol's Management Board adopted its decision on the role, profile and organisational placement of the Fundamental Rights Officer (FRO) function, and **in December 2022,** designated the **first Fundamental Rights Officer (FRO) at Europol**. Under the motto 'Fundamental Rights at Europol, it takes all of us!', the FRO engaged in further developing the fundamental rights culture at the Agency.[102]

The **risk of fundamental rights violations** by Europol staff, **other than in the field of data protection**, is generally **moderate**. An area of divergence with law enforcement agencies is Europol's lack of executive powers. The only problematic cases are, therefore, on the one hand, staff deployed in the field, where violations of Article 1 Charter could for instance take place. or, on the other, the processing of data sent to the European Counter Terrorism Centre, which may not have been gathered in compliance with fundamental rights, for instance obtained under torture. The intelligence Europol sends in support of major investigations is always validated by the local judicial authorities, which guarantees compliance with fundamental rights. The new tasks provided for in Regulation (EU) 2022/991 present, therefore, a minimal risk. In its first two

101 Comment from a MS in its Reply to the Short Questionnaire of 2 June 2025.
102 Europol FRO, 2023 Annual Report.

years of activities, **no reports of fundamental rights violations** were presented by the FRO to the Executive Director since no complaints were lodged.[103]

7. Cost-benefit analysis of the operational implementation of Europol's new personal data processing powers and tasks

7.1. Costs

7.1.1. Article 4(1)(t) ER on the Schengen Information System (SIS) information alerts on third-country nationals upon proposal by Europol

For the provisions of Article 4(1)(t) ER, Europol has reported costs for about **EUR 1.4 million in total**, of which a part is for SIS-related activities in general. **HR costs** amounted to **EUR 685 250**, and **ICT** amounted to **EUR 710 000.**

Based on data provided by Europol[104], the staff effort of the Operation Directorate for the envisaged entry into operation of the Schengen Information System (SIS) information alerts, during 2022, 2023, 2024, and currently in 2025, was less than 1 Full Time Equivalent (FTE). The staff effort was higher for Europol's ICT Department, with 3-4 FTEs, during the period 2022-2024.

Table 5 – One-off costs for Article 4(1)(t) ER for HR

2022	2023	2024	2025
Operations Directorate			
EUR 28 500	EUR 30 500	EUR 31 500	EUR 32 750
ICT Department			
EUR 204 000	EUR 280 000	EUR 77 000	
Total			
EUR 232 500	**EUR 310 500**	**EUR 108 500**	**EUR 32 750**

Source: Europol, Reply to the follow-up request for information of 25 May 2025

In addition, between 2022 and 2024, a total of EUR 710 000 was allocated to the development of the Schengen Information System (SIS)/SIRENE, predominantly for contractor resources (see Table 6). The Schengen Information System (SIS)/SIRENE hardware and recurring costs are limited as the integration with the Schengen Information System (SIS) (hosted by eu-LISA) has been implemented with a set of small Application Programming Interfaces (APIs) which run on a shared platform with other (unrelated) services and applications. The projected commitments for 2025 amount to an estimated EUR 95 000 (no specific breakdown for the Schengen Information System (SIS) alerts is available). This amount represents only a small percentage of Europol's budget for the overall ICT workstream related to interoperability and biometrics.

Table 6 – One-off costs for Article 4(1)(t) ER (non-including HR)

2021	2022	2023	2024	2025
	EUR 130 000 Investments focused on software licensing	EUR 220 000 Additional contractor extensions for the Schengen Information System	EUR 120 000 Ongoing development and testing needs were met through contractor	

[103] Europol FRO, 2023 and 2024 Annual Reports.

[104] Europol's reply to DG HOME follow-up request for information of 25 May 2025.

		(SIS)/SIRENE for ensuring continuity in both testing and development	resources supporting the Schengen Information System (SIS)/SIRENE and ETIAS	
	EUR 240 000 Development of testing activities			
Total				
	EUR 370 000	**EUR 220 000**	**EUR 120 000**	

Source: Europol, Reply to the follow-up request for information of 25 May 2025

All costs so far were one-off costs for preparatory measures. Regarding the future costs after the expected **entry into operation of the new SIS alerts in Q1 2026**, Europol estimates an increase in HR (**2 FTEs)** to initiate the envisaged workflow. In **2027**, the number is estimated to increase by at least **1-2 additional FTEs**, to reach a **minimum of 3-4 FTEs**. Europol assumes that the work will increase progressively. Once the Schengen Information System (SIS) information alerts are in the system, hits will start to be reported to Europol. Follow-up on hits will be necessary, and a thorough data review process will need to be performed on all data continuously.

In their comments on Article 4(1)(t) ER, **three Member States**[105] stressed the **key role of the SIRENE Bureaux,** which are 'responsible for managing the exchange of information related to the Schengen Information System (SIS) alerts and will play a key role in this new process. When a "hit" occurs on a Europol-proposed alert in …, the SIRENE Bureau will coordinate the necessary follow-up actions and share relevant information with Europol and other Member States' and the importance that '[these provisions] **must not generate additional workload for the SIRENE Bureaux**, as in some Member States, the responsibility for making these entries lies with them'. The Commission services understand that no costs have been incurred so far, absent the operational implementation of Article 4(1)(t) ER, and an estimate of such costs is not possible. The costs might also vary across the Member States.

7.1.2. Articles 18(2)(e) and 33a ER on the processing of personal data by Europol for research and innovation projects

For the provisions of Article 18(2)(e) and 33a ER, Europol has reported costs for about **EUR 940 000** for the establishment of the sandbox. Costs for innovation projects are still not available and depend on the nature of the project. **HR costs** amounted to **EUR 160 000** and **ICT costs**, other than for HR, to **EUR 780 000.**

Based on the information provided by Europol[106], the costs included investments for the development and long-term sustainability of the sandbox, for an overall amount of EUR 780 000 (see Table 7). For 2025, there are no foreseen Sandbox investments in Europol's ICT. In terms of Staff for the establishment of the 'sandbox', the ICT infrastructure for future research and innovation, Europol's Information and Communication Technology (ICT) Department dedicated about 1 FTE in the period 2023-2024, amounting to EUR 160 000.

The Innovation Lab undertakes supportive work for the sandbox development within the Information Management Unit (IMU). Between 2022 and 2024, the Innovation Lab included up to 11 FTEs per year, with an overall cost of approximately EUR 5.7 million (which includes the supportive work for the sandbox development).

105 See MS comments to Question 2 of the Short Questionnaire of 2 June 2025, Annex III.

106 Europol, Reply to DG HOME follow-up request for information of 25 May 2025.

Table 7 – One-off costs for the development of the 'Sandbox' (non-including HR)

2022	2023	2024	2025
	EUR 205 000 hardware, including general equipment, for GPU equipment, and a proportional share of storage infrastructure	EUR 95 000 Sandbox project management	
	EUR 15 000 Software renewals and support	EUR 265 000 Application and architectural services	
	EUR 130 000 resource (including for project management)	EUR 70 000 Hardware and software renewal	
Total			
	EUR 350 000	**EUR 430 000**	

Source: Europol, Reply to DG HOME follow-up request for information of 25 May 2025

Annual recurring costs from 2025 onwards are estimated by Europol at **EUR 50 000**, of which EUR 40 000 for hardware maintenance (based on 15% of the total hardware investment) and EUR 15 000 for license renewals (until major developments of the sandbox are implemented, or a replacement is launched).

7.1.3. Articles 18(6a) and 18a ER on the analysis by Europol of large and complex datasets ('big data')

Except for the administrative costs stemming from the adoption of the Management Board decision, the amendment to Article 18(6a) ER did **not, per se,** generate **new direct costs,** as it provided clarifications on the retention period for large and complex datasets without Data Subject Categorisation (DSC). The implementation of Article 18(6a) ER did not have any impact on the actual scope of Europol's obligation to complete the DSC compared to the situation before the entry into force of Regulation (EU) 2022/991.

Table 8 reports the staff effort of the data quality and compliance team, which amounted to EUR 1.35 million in the reference period. Europol explained that an exact estimate of other costs incurred for the implementation of Article 18(6a) ER, notably in terms of the need for DSC, is not possible because they are indirect costs for the DSC assessment, which is incorporated in Europol's daily intake process of the Operations Directorate[107]. According to Europol, those indirect costs are significant and this view was supported by some Member States[108]. A Member State, for example, explained: 'currently it takes a Europol analyst three working days to process the information from one seized phone. In large investigations, we are often working with 100 phones from one member state alone'.

[107] By the end of 2024, there were 405 temporary agents (TAs) from competent authorities in post in the Operations Directorate (in 2023: 386, in 2022: 345). **A breakdown of the FTEs devoted to DSC is not available**.

[108] See MS replies to Question 9 of the Short Questionnaire of 2 June 2025, Annex III.

Table 8 – Costs for the implementation of Article 18(6a) ER for HR

2022	2023	2024	2025
Data quality and compliance team			
1.00 FTE	1.5 FTEs	2.50 FTEs	3.50 FTEs
Total			
EUR 145 000	**EUR 240 000**	**EUR 385 000**	**EUR 580 000**

Source: Europol, Reply to DG HOME follow-up request for information of 25 May 2025

The **one case** applying the **Article 18a ER** required a limited investment of **EUR 7 200** so far. Further costs and maintenance will depend on further development of this case. An estimation of the indirect costs is not possible.

7.1.4. Articles 26, 26a and 26b ER on the exchange of personal data between Europol and private parties

For the provisions of Article 26, 26a and 26b ER, Europol has reported costs for about **EUR 20 million**. **HR costs** amounted to over **EUR 5 million** and **ICT costs,** other than for HR, to over **EUR 15 million.**

The staff effort across Europol for developing new cooperation possibilities with private parties was approximately **1 FTE** in the period 2024-2025. In addition, the staff effort for Europol's ICT Department for PERCI was **31 FTEs** in the period 2022-2024, with a corresponding overall amount of **EUR 4.56 million**, and for EU CARES was **2 FTEs** in the period 2023-2024, with a corresponding overall amount of **EUR 290 000** (see Table 9 below).

Table 9 – Costs for the cooperation with private parties for HR

2022	2023	2024	2025
ICT Department – PERCI			
EUR 1 560 000	EUR 2 215 000	EUR 785 000	
ICT Department – EU CARE			
	EUR 200 100	EUR 91 000	
Other departments			
		EUR 155 000	EUR 200 000
Total			
EUR 1 560 000	**EUR 2 415 100**	**EUR 1 031 00**	**EUR 200 000**

Source: Europol, Reply to the follow-up request for information of 25 May 2025

Between 2021 and 2024, substantial investments were made in the **development and expansion of the PERCI platform**, focusing on strengthening infrastructure, cloud capabilities, and external contractor support, for an estimated **EUR 6.77 million** (see Table 10 below). The investments to support the **EU Child Abuse Referral Service (EU CARES)** between 2023 and 2025 amounted to EUR 205 000 (see Table 11 below).

Table 10 – One-off costs for the development of PERCI (non-including HR)

2021	2022	2023	2024	2025-2026
EUR 480 000 critical infrastructure,	EUR 2 560 000 for extensive contractor	EUR 715 000 cloud environment operations across	EUR 820 000 expert contractor resources (solution	EUR 1 200 000 investment for the implementation of

storage systems, and host machines	resources and extensions across ICT environments	development, testing, and production.	architecture, requirements engineering, and external support, etc)	Article 18 of the Digital Services Act (DSA) via the PERCI platform
EUR 240 000 cloud services and the related security tooling (including, based on EDPS requirements), and licensing for cloud on-premises services	EUR 520 000 cloud services, including platform licenses, log analytics, and business intelligence tooling	EUR 1 430 000 funded contractor renewals, as well as resource additions to meet demand		
		EUR 10 000 infrastructure and code security analysis tools		
Total				
EUR 720 000	**EUR 3 080 000**	**EUR 2 155 000**	**EUR 820 000**	**EUR 1 200 000**

Source: Europol, Reply to DG HOME follow-up request for information of 25 May 2025

Table 11 – One-off costs for the development of EU CARES (non-including HR)

2022	2023	2024	2025
	EUR 85 000 Investment	EUR 120 000 migration work between the NCMEC application and EU CARES	EUR 590 000 including supporting the testing and development for the EUCARES application.
			EUR 120 000 hardware and software-related costs are envisaged
Total			
	EUR 85 000	**EUR 120 000**	**EUR 710 000**

Source: Europol, Reply to the follow-up request for information of 25 May 2025

Europol expects **annual costs (recurring)** of **EUR 540 000**, primarily to cover Cloud provider costs to support the continuous operation and maintenance of key systems. In addition, for EU CARES, **recurrent costs** are estimated at EUR 85 000 (yearly), of which **EUR 45 000** for the maintenance of IVAS (Image and Video Analysis Solution) and EUR 38 000 (yearly) for overall maintenance (including software licences).

7.1.5. Internal and external oversight on compliance with fundamental rights

The **Data Protection Function (DPF)** currently has eight full-time equivalent members (FTEs)**,** including one FTE member for the Data Protection Officer (DPO) and one FTE member for the **Fundamental Rights Officer (FRO)** (see Table 12 below).

Table 12 – Costs for the FRO and the DPF for HR

2022	2023	2024	2025
Fundamental Rights Officer (FRO)			
	EUR 233 200	EUR 224 200	EUR 278 100
Data Protection Function (DPF)			

EUR 1 010 000	EUR 1 300 000	EUR 1 458 500	EUR 1 530 500
Total			
EUR 1 010 000	**EUR 1 533 150**	**EUR 1 682 700**	**EUR 1 808 750**

Source: Europol, Reply to the follow-up request for information of 25 May 2025

In addition, **60 FTEs** of Europol staff are estimated to be involved on an **annual basis** in activities generated by **assurance/supervisory bodies and oversight/advisory entities**. Europol committed **25 FTEs** to efforts in responding to **data protection supervision and corresponding assurance actions**. This includes follow-up on EDPS recommendations, as well as work generated in the context of prior consultations for operational data processing. Accordingly, out of the **25 FTEs** dealing with data protection, **16 FTEs** are related to specific EDPS response activities.[109]

From an overall perspective, the preparatory work, in particular the discussion, preparation and adoption of relevant legal instruments by the Europol Management Board is hard to quantify (given the involvement of multiple stakeholders at various phases). The work involved at least **2 FTEs from Europol's Corporate Law Team**.

7.2. Benefits

7.2.1. Article 4(1)(t) ER on the Schengen Information System (SIS) information alerts on third-country nationals upon proposal by Europol

The provisions of Article 4(1)(t) ER were not operational during the reporting period. Therefore, they have **not yet generated any actual benefits**. However, during the consultation, **several Member States reiterated the important benefits *expected*** from Europol's proposals for the Schengen Information System (SIS) alerts and the relevance of Article 4(1)(t) ER for Europol's objectives.[110]

The main expected benefits mentioned by Europol and Member States include the increased security provided thanks to wider dissemination to all Member States' border guards of information on high-risks individuals (terrorists, violent extremists, organised criminals) unknown to Member States and the facilitation of targeted checks, surveillance, or detentions based on intelligence-the Schengen Information System (SIS) alerts as well as improved situational awareness at airports seaports, public spaces and events.

7.2.2. Articles 18(2)(e) and 33a ER on the processing of personal data by Europol for innovation and research projects

Due to the time necessary to set up the sandbox, **only one project** could be developed during the reporting period, making use of the new provisions under Article 18(2)(e) ER. The project was launched very recently. Therefore, it **has not yet generated any tangible benefits**. However, during the consultation, Europol and several Member States reiterated the **important benefits *expected*** by stressing the relevance of Article 18(2)(e) ER.

The main expected benefits, as mentioned by Europol and Member States, include the **development of tailored and enhanced police tools to address the innovation needs of Member States**. For Europol, there are also significant potential benefits in terms of **efficiency gains in the long run**, as avoiding duplication of efforts across different Member States can lead to substantial improvements.

---

109 Europol, dedicated resource estimate exercise, reported to the Europol Management Board in March 2022.

110 See MS replies to Question 2 of the Short Questionnaire of 2 June 2025, Annex III.

7.2.3. Articles 18(6a) and 18a ER on the analysis by Europol of large and complex datasets ('big data')

Europol and several Member States emphasised in their comments that analysing large and complex datasets is highly valuable for Member States' competent authorities.

The new provisions of **Article 18(6a) ER merely facilitated this task**, already lawfully carried out by Europol, by providing legal certainty and a more extended retention period than that imposed by the European Data Protection Supervisor (EDPS) interpretation of the Europol Regulation. A Member State notes that '[… they] **didn't experience any particular problems before the EDPS opinion**. So, the new provisions have brought a clear legal basis but have **not drastically changed the possibility to send data to Europol**'.

The main benefits mentioned by Europol and Member States include, thanks to **increased legal certainty and appropriate conditions**, enhanced support to Member States' investigations by the improved capacity of Europol to analyse large and complex datasets. **Efficiency gains** result from the fact that Europol carries out analysis for the benefit of all Member States.

7.2.4. Articles 26, 26a and 26b ER on the exchange of personal data between Europol and private parties

The feedback from all stakeholders who provided comments indicates that cooperation with private parties has been **vital in disrupting crime across various areas**, including cybercrime, terrorism, financial crime, and others.

Europol and seven Member States submitted that, over the reporting period, the new provisions on the exchange with private parties generated significant and tangible benefits for national law enforcement authorities and supported several investigations. The main advantages are described as **targeted and enhanced collaboration** with private parties and **deconfliction** across the Member States' investigation process.

Member States did not provide any statistics on operational results but mentioned examples of major investigations carried out with the support of Europol's new task, such as **Phobos, AKIRA**, and, most recently, **Lumma**.

7.2.5. Internal and external oversight on compliance with fundamental rights

For Europol, Member States benefit from the support provided by Europol's Data Protection Function (DPF) and Fundamental Rights Officer (FRO) by **ensuring compliance with fundamental rights, including data protection, across Europol's operational tasks and objectives as specified in the Europol Regulation**.

During the consultation, Member States generally indicated that they had little to no practical experience with the new data protection safeguards.[111]

Some Member States submitted nonetheless that the alignment with Regulation (EU) 2018/1725 **facilitates the flow of information between Europol and the Member States**.[112] A Member State observes: '[t]he alignment with the said regulation safeguards allows personal data to be handled securely and in compliance with the EU legal framework. Thus, within the context of police cooperation, **trust is enhanced**. Member States are **exchanging information easily and in a timely manner**'. For another Member State, this does **not directly force an increase** in data sharing, but it removes **key legal and procedural barriers**, promotes trust, and ensures that **data flows are legally sound, secure, and rights-respecting**. These improvements create a **more predictable and interoperable environment** for information exchange between Europol and

111 All comments provided by Member States are reported in Annex III.

112 See MS replies to Questions 6 and 7 of the Short Questionnaire of 2 June 2025, Annex III.

Member States. Europol can now act as a trusted intermediary for information coming from private entities (e.g. telecom providers, financial services, tech platforms)'.[113]

7.3. Cost-benefit analysis

Given the very early stage of operational implementation of the new data protection powers and tasks, and the limited practical experience, it is **premature to draw any valuable conclusions about the new provisions based on a cost-benefit analysis.**

The data collected indicates that the costs incurred so far were generally one-off costs associated with the start of implementation. They included notably HR resources to comply with requirements stemming from the Europol Regulation about governance, internal and external oversight, to commence the operational implementation of new tasks or to adapt to the new provisions. They included, however, also significant financial investments, particularly in ICT, which were necessary for the development of the 'Sandbox', 'EU CARES' and 'PERCI'. In this regard, some Member States stressed that 'it is important that Europol provides the necessary ICT resources to provide and further develop the tools for the implementation of the new possibilities of Regulation (EU) 2022/991'.

[113] All comments provided by Member States are reported in Annex III.

Distribution of estimated resources between ICT and HR

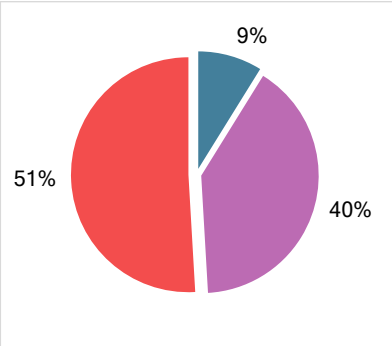

Chart 1 – Main categories of costs for the implementation of Article 4(1)(e) ER

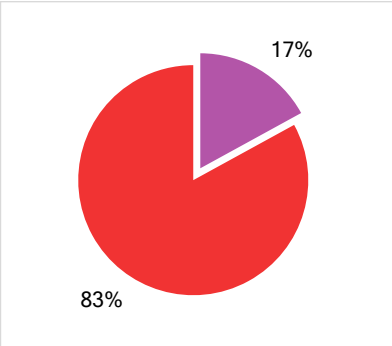

Chart 2 – Main categories of costs for the implementation of Articles 18(2)(t) and 33a ER

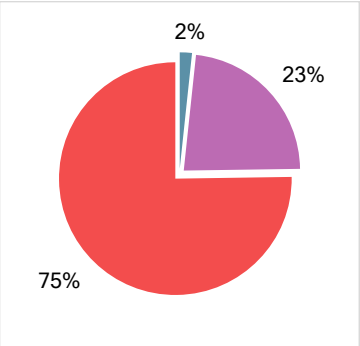

Chart 3 – Main categories of costs for the implementation of Articles 26, 26a and 26b ER

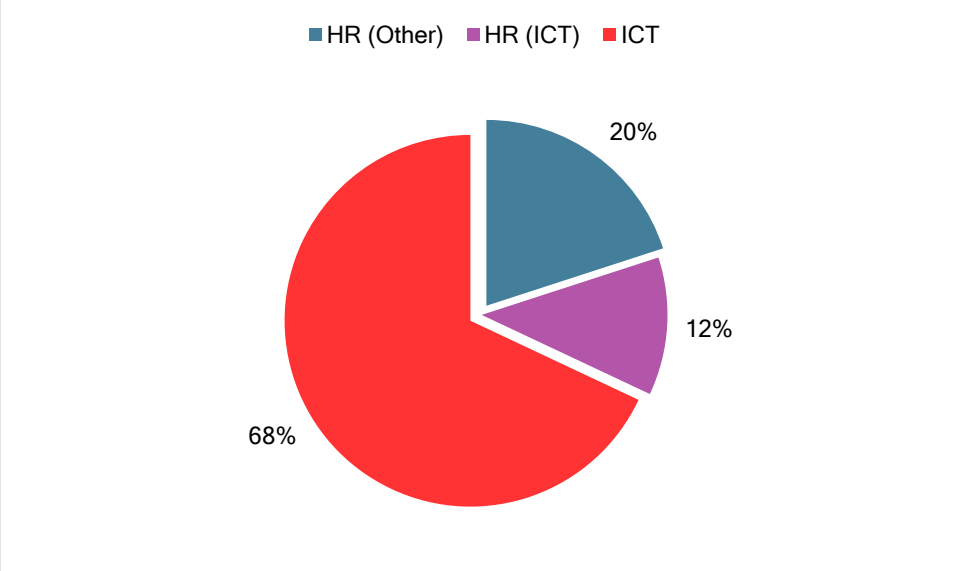

Chart 4 – Main categories of costs for the implementation of the new personal data processing tasks

Recurrent costs, on the contrary, were **quite limited**; however, they **cannot be considered indicative of future expenses,** given that the operational scale and complexity of the implementation have not yet reached their full potential.

Significant indirect costs were indicated only as regards Article 18(6a) ER for performing the Data Subject Categorisation (DSC). Although these costs are related to the implementation of Article 18(6a) ER, they are **not *new* costs,** given that Europol was already processing and analysing large and complex datasets before 28 June 2022, and the new provisions did not introduce stricter conditions. In the long run, savings or efficiency gains may be assumed where Europol's support benefits all Member States due to scale effects over a longer period.

At the same time, the **benefits achieved**, or expected, thanks to the new tasks cannot be monetised, and are **hardly quantifiable in terms of operational results** over a short period. It is worth stressing that, in some instances, implementation has been minimal due to delays in operationalising specific provisions. A **rather long period is generally necessary to gain deeper insight into the operational results of new tools in criminal investigations**, including prosecution, due to the length of investigations and judicial proceedings. Individual activities can also not be measured continuously, for example, with respect to the Data Subject Categorisation (DSC) assignment. Despite the absence of statistics, the longer practice with analysing big data

and cooperation with private parties shows that they may provide an essential contribution to investigations. The cases cited by Member States corroborate this conclusion.

All in all, a cost-benefit analysis of the implementation of some tasks (Article 4(1)(t) ER and Article 18(1)(e) ER) provided for in Regulation (EU) 2022/991 is premature at this stage. For the other tasks (Articles 18(6a) and 18a ER and Articles 26, 26a and 26b ER), there seems to be agreement among stakeholders that the benefits of the analysis of large and complex datasets and of the cooperation of private parties outweigh the costs, and their use may justify additional dedicated resources.

The comments of Europol and some Member States suggest that, nonetheless, **possible inefficiencies** stemming from the implementation of the new provisions need to be addressed within the existing governance, administration, and data protection framework, which undermines their operational impact by delaying or limiting their use. Some Member States attributed notably significant costs to the decision to follow a conservative approach in implementing new oversight rules, rather than **making proportionate use of the flexibility provided by the Europol Regulation**. This would be the case notably for the Data Subject Categorisation under Article 18(6a) and 18a ER, and the data protection impact assessments and prior consultation of the EDPS under Article 39 ER and Articles 89 and 90 EUDPR. A Member State argues, for example, '[w]e do have a strong impression that the EDPS demands prior consultation more often than the national supervisory authorities do. And since the conditions in **Article 90 EUDPR** and in Article **28 LED** are virtually identical, such **diverging interpretations of the necessity for prior consultation** seem **arbitrary to a certain extent**. In practice, this leads to delays when Europol needs to set up new processing systems, hampering the effective implementation of the new possibilities created by the 2022 amendment and hampering the provision of agile services to the Member States.

The Commission services see a need to collect further evidence to assess and evaluate the indicated shortcomings in the context of the evaluation[114] to be carried out pursuant to Article 68(1) ER.

Finally, savings may be possible by streamlining the current implementation of horizontal governance and oversight mechanisms, which, according to the data collected, require a significant amount of staff effort. An analysis of Europol's working methods in this regard is, however, **outside the scope of the evaluation under Article 68(3) ER** and will be undertaken in the framework of the evaluation to be carried out pursuant to Article 68(1) ER.

8. Conclusions and ways forward

The evaluation carried out by the Commission services allows taking stock of the progress made with the operational implementation of key provisions of Regulation (EU) 2022/991 three years after it entered into force.

A key finding of the evaluation was that **the start of operational implementation of the new tasks was significantly delayed** by preparatory measures at governance, technical, and administrative levels, in addition to operational-level needs, such as setting up new ICT structures in some instances. However, on 29 June 2025, all provisions were operational except for Article 4(1)(t) ER, which should become operational in 2026.

As regards the processing by Europol of personal data for research and innovation pursuant to Article 18(2)(e) ER, due to the limited period of operational implementation, sufficient quantitative data is not yet available. At the same time, some qualitative positive comments by Europol and Member States on the effectiveness, relevance, and EU added value are not corroborated by actual practical experience.

[114] See Article 68(1) ER and Section 8 below of this SWD.

As regards Europol's analysis of large and complex datasets (Articles 18(6a) and 18a ER) and the exchange of personal data between Europol and private parties (Articles 26, 26a and 26b ER), both Europol and several Member States provided overall **very positive feedback** about their benefits and relevance as well as their EU added value, corroborated by some concrete examples of successful investigations. Europol has made a significant investment in the development of ICT platforms dedicated to cooperation with private parties, and the analysis of large and complex datasets can also require substantial human resources. **Constraints to a broader use of these tools may result from limited resources in the future**.

The evaluation did **not find evidence of a negative impact** of the extension of Europol's tasks **on fundamental rights and freedoms**. On the contrary, Europol currently has a robust and solid legal data protection framework in place, which ensures sufficient safeguards for potential increased use of its new tasks. According to several Member States, this framework also facilitates the flow of information.

To draw any conclusions from a comparison of costs incurred and benefits generated is premature for most of the provisions analysed due to the late state of implementation. Quantifying the monetary benefits of investigative tools is generally a daunting task, but in this case, the main finding is that the benefits of most provisions have not materialised yet.

At the same time, Member States pointed to certain shortcomings of a too cautious implementation of the data protection rules by Europol and its Management Board, under the guidance of the EDPS, and suggest that appropriate use should be made of the flexibility left by the co-legislators to maximise the effectiveness and efficiency of Europol's tasks provided for in Regulation (EU) 2022/991 and ensure their relevance and profitability in the long term.

Stakeholders identified some areas for improvement for the new tasks to maximise the expected benefits, notably as regards:

- the costs and time for the Data Subject Categorisation (DSC);
- the costs and time related to the prior data protection impact assessment and prior consultation of the EDPS carried out by default, even in the presence of measures mitigating the risk;
- divergencies in the handling of data subjects' access requests between Europol and national authorities;
- complexity and scenario-based compartmentalisation of the provisions on cooperation with private parties.

The co-legislators mandated this evaluation of the Europol Regulation at a very early stage of implementation to contribute to the evaluation of the Europol Regulation to be carried out before any revision of the Europol Regulation according to the Better Regulation Guidelines or, in any event at the latest by 29 June 2027, pursuant to Article 68(1) ER.

In its **ProtectEU**, the European Internal Security Strategy[115], the Commission announced that it will propose an ambitious overhaul of Europol's mandate to address escalating security challenges. In compliance with its Better Regulation Guidelines[116], the Commission launched preparations to evaluate the Europol Regulation and Europol's working methods, paving the way for a Commission **proposal in 2026 to make the Agency more operational, as set out in the Political guidelines**.[117] In July 2025, the Commission published the call for evidence[118] and contracted an external study to

115 ProtectEU: a European Internal Security Strategy, p. 10.

116 See https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox_en.

117 Ursula von der Leyen, Political Guidelines for the next European Commission 2024−2029, e6cd4328-673c-4e7a-8683-f63ffb2cf648_en

118 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14638-Law-enforcement-cooperation-new-Europol-regulation-proposal-en.

support the evaluation of the Europol Regulation and the impact assessment for the new proposal. The evaluation of the Europol Regulation carried out for the purposes of preparing this report is intended to contribute to that evaluation.

Annex I
Evidence base of the evaluation

Reports and other publications

(before 2020)

(1) EDPS, Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, https://www.edps.europa.eu/sites/default/files/publication/16-09-23_bigdata_opinion_en.pdf

(2) Europol, ECTC Case Study: Paris - 13 November 2015, available online under ECTC infographic PUBLIC

(3) Europol, Operation EMMA, online under Operation Emma - Dismantling EncroChat, an encrypted phone network widely used by criminal networks | Europol

(4) Europol, Press release: 800 criminals arrested in biggest ever law enforcement operation against encrypted communication, https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

(2020)

(5) European Commission, Commission Staff Working Document - Impact Assessment accompanying the proposal for a 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, SWD(2020) 543 final of 9.12.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020SC0543

(2021)

(6) EDPS Opinion 4/2021 on the Proposal for Amendment of the Europol Regulation, https://www.edps.europa.eu/system/files/2021-03/21-03-08_opinion_europol_reform_en.pdf

(2022)

(7) European Commission, Communication to the European Parliament and the Council - First Report on the application of the Data Protection Regulation for European Union institutions, bodies, offices and agencies (Regulation (EU) 2018/1725), COM(2022) 530 final of 14.10.2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022DC0530

(8) Europol Data Protection Officer (DPO), 2022 Annual Report

(9) Europol, 2022 Consolidated Annual Activity Report (CAAR), https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated%20Annual%20Activity%20Report%202022.PDF

(10) Europol, Operation Emma (Dismantling EncroChat, an encrypted phone network widely used by criminal networks), https://www.europol.europa.eu/operations-services-and-innovation/ operations/operation-emma

(11) EDPS, Supervisory Opinion of 17 November 2022 on Europol's Management Board Decision adopted pursuant to Articles 11(1)(q), 18 and 8a of the Europol Regulation (Case 2022-0923)

(12) Europol, OTF Greenlinght, Episode 2: Operation Greenlight Part 1 - The International Sting - The Europol Podcast | Europol

(2023)

(13) eu-LISA, 2023 the Schengen Information System (SIS) Annual Statistics

(14) Europol, 2023 Annual Report in accordance with Article 7(11) Europol Regulation on information provided by Member States
(15) Europol, 2023 Annual reporting to the Europol Management Board (MB) on the exchange of data with private parties (Art. 26(11) Europol Regulation)
(16) Europol, 2023 Consolidated Annual Activity Report (CAAR), https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated-Annual-Activity-Report-2023.PDF
(17) Europol Fundamental Rights Officer (FRO), 2023 Annual Report
(18) Europol Data Protection Officer (DPO), 2023 Annual Report
(19) EU Internet Referral Unit, 2023 Transparency Report

(2024)

(20) European Commission, Report on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, COM(2024) 64 final of 14.2.2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0064
(21) European Commission, DG Migration and Home Affairs, Annual Activity Report 2024
(22) Europol, 2024 Annual Report in accordance with Article 7(11) Europol Regulation on information provided by Member States
(23) Europol, 2024 Consolidated Annual Activity Report (CAAR), https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF
(24) Europol Fundamental Rights Officer (FRO), 2024 Annual Report
(25) Europol Data Protection Officer (DPO), 2024 Annual Report
(26) Meijers Committee, Comment on Europol's Data Subject Categorisation based on the Amended Europol Regulation, May 2024, available online at https://www.commissie-meijers.nl/wp-content/uploads/2024/05/CM-comment-Europol-DSC.pdf
(27) Europol, Press release: Violent Albanian criminal group linked to corruption disrupted via SKY ECC analysis, available online under https://www.europol.europa.eu/media-press/newsroom/news/violent-albanian-criminal-group-linked-to-corruption-disrupted-sky-ecc-analysis

(2025)

(28) Europol, OTF GRIMM, online under Operational Taskforce GRIMM - Sweden-led taskforce tackling violence-as-a-service and the recruitment of young perpetrators into serious and organised crime. | Europol
(29) Europol, Press release: Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown, https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown
(30) Europol, Press release: Europol and Microsoft disrupt world's largest infostealer Lumma, https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma

Technical Meetings between DG Home and Europol staff

(31) First technical meeting between DG Home and Europol staff, on 18 February 2025 in The Hague
(32) Second technical meeting between DG Home and Europol staff, on 3 April 2025 in The Hague

Replies to written request for information and questionnaires

(33) Europol, Reply of 2 April 2025 to DG HOME first Request for information of 1 March 2025
(34) Europol, Reply of 15 June 2025 to DG HOME follow-up Request for Information of 26 May 2025
(35) Member States' (MS) Replies to the Short questionnaire of 2 June 2025, submitted June-July 2025

Legal Acts

(36) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53, ELI: http://data.europa.eu/eli/reg/2016/ 794/oj
(37) Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS), OJ L 236, 19.9.2018, p. 72, ELI: http://data.europa.eu/eli/reg/2018/1241/oj
(38) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj
(39) Regulation (EU) 2021/1133 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the Visa Information System, OJ L 248, 13.7.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/1133/oj
(40) Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, OJ L 172, 17.5.2021, p. 79, ELI: http://data.europa.eu/eli/reg/2021/784/oj
(41) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj
(42) Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 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 in research and innovation, OJ L 169, 27.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/991/oj
(43) Regulation (EU) 2022/1190 of the European Parliament and of the Council of 6 July 2022 amending Regulation (EU) 2018/1862 as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union, OJ L 185, 12.7.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1190/oj

Annex II
Overview of costs and benefits (2022-2025)

Overview of costs						
		SIS Alerts Article 4(1)(t) ER	**R&I** Article 18(1)(e) ER	**Big data** Article 18(6a) ER Article 18a ER	**Private parties** Article 26 ER Article 26a ER Article 26b ER	**Oversight**
Cost description						
Direct costs for Europol	**One-off**	Development of the Schengen Information System (SIS)/SIRENE Operational Unit **0.5 FTE**< per year in 2022-2024 **2 FTEs** in 2025 ICT **3-4 FTEs per year** in 2022-2024 **= EUR 685 250** + **EUR 805 000** overall between 2022-2025	Developments of the 'Sandbox' ICT staff **1 FTE >** per year in 2022-2024 = **EUR 160 000** + **EUR 780 000** for ICT and other costs between 2023-2024	Negligible	Development of PERCI **30> FTEs** in total for 2022-2024 **= EUR 3.2 million** + **[EUR 725 000** in 2021] **EUR 3 million** in 2022 **EUR 2 million** in 2023 **EUR 820 000** in 2024 **EUR 1.2 million**[119] in 2025-2026 (DSA) Development of EU CARES **2 FTEs** in total for 2022-2024 **= EUR 291 100** + **EUR 85 000** in 2023 **EUR 120 000** in 2024 **EUR 710 000** in 2025	Law Team: **2 FTEs** > between 2023-2025 For all provisions, the adoption of MB decisions and other implementing acts and measures required a staff effort also of other different internal services. An estimation is not possible, see below.
	Recurrent	Not implemented yet	Maintenance of the 'Sandbox' **EUR 55 000** per year IMU staff – an estimation not possible.[120]	Data quality and compliance team **1 FTE** in 2022 **1.5 FTE** in 2023 **2.5 FTE** in 2024 **3.5 FTE** in 2025	Maintenance of PERCI **EUR 540 000** per year	A breakdown of the costs related exclusively to the tasks provided for in Regulation (EU) 2022/991 is not available

[119] Financed by the Commission (DG CNECT) via a contribution agreement.

				= **EUR 1 350 000** Projects under Art 18a no cases in 2022, 2023 and 2024 **EUR 7 200** for one project in 2025		DPF/FRO **8 FTEs** at the DPF **= EUR 5.3 million** **1 FTE** at the FRO **= EUR 735 500** Data protection supervision tasks **25 FTEs** (16 FTEs are related to specific EDPS response activities) **35 FTEs** are devoted to governance and oversight activities
Indirect costs for Europol		None	None	DSC under Art 18(6a) staff costs **very significant**, but an estimation is not possible. These are however not new costs.	None	None
Costs for MS		Additional **workload for the SIRENE Bureau**, and costs necessary for the reprocessing of the national the Schengen Information System (SIS) source systems, the Schengen Information System (SIS) searching tools, new SIRENE workflow. Estimation not possible and may differ across MS.	Unknown	**Savings for MS** by **not carrying out the DSC** for certain contribution where it would be very burdensome. However, savings are not very significant since MS in over 99% of the cases carry out the DSC.	Unknown	Unknown

[120] Supportive work for the Sandbox development is carried out by the Innovation Lab in the Information Management Unit (IMU). Between 2022 and 2024, the Innovation Lab included up to 11 FTEs per year, with an overall cost of approx. EUR 5 700 million (which includes the supportive work for the Sandbox development).

Overview of benefits					
	SIS Alerts Article 4(1)(t) ER	**R&I** Article 18(1)(e) ER	**Big data** Article 18(6a) ER Article 18a ER	**Private parties** Article 26 ER Article 26a ER Article 26b ER	**Oversight**
Benefits description					
Member States (Competent Authorities)	Improved dissemination to all MS border guards of information on high-risks individuals (terrorists, violent extremists, organised criminals) unknown to MS Facilitation of targeted checks, surveillance, or detentions based on intelligence-the Schengen Information System (SIS) alerts Improved situational awareness at airports seaports, public spaces and events	Tailored and enhanced police tools to address the innovation needs of Member States' competent authorities, made available via Europol Tool Repository (ETR)[6] Efficiency gains, where the development of innovation tools is coordinated by Europol for the benefit of all Member States	Increased legal certainty and enhanced support to Member States investigations (non-quantifiable) Support to several successful investigations (no statistics available) Efficiency gains, since analysis is carried out by Europol for the benefit of all Member States	More targeted and enhanced collaboration with private parties Support to several successful investigations (no statistics available) Deconfliction across MS investigation process Efficiency gains expected, as Europol can act as the connector between Member States and private parties (in the longer run)	Enhanced compliance with fundamental rights thanks to FRO and DPO Facilitation of flow of information between Europol and MS thanks to harmonised processing conditions and increased trust
Citizen/SMEs and other private actors	Indirect benefits in terms of increased security	Indirect benefits in terms of increased security	Indirect benefits in terms of increased security	Indirect benefits in terms of increased security	Indirect benefit in terms of increased security and better personal data protection

Note: Articles 4(1)(t), 18(1)(e), 18a and 26a ER were not used over the reporting period or only at a very late stage. Therefore, the indicated benefits are not actual benefits but expected benefits.

Annex III
Summary of Member States' replies

Short questionnaire on the operational implementation of Europol's tasks provided for in Regulation (EU) 2022/991

1. Survey and response rate

The Commission services sent a short questionnaire to the 27[121] Member States, on 2 June 2025, which included **nine questions** regrouped under three topics:

a. Operational impact of the implementation of the 'new tasks' (Questions 1, 2 and 3)
b. Cost-benefit analysis (Questions 4 and 5)
c. Implementation of the Personal Data Protection Safeguards (Questions 6, 7, 8 and 9)

The **response rate** was not **very high** despite the broad **participation of Member States**. A total of **24** Member States **completed the questionnaire** (**89%**), but respondents left a significant number of questions unanswered or indicated that they were unable to assess. It yields an **aggregated response rate of 51%**.[122] This outcome is **consistent with the limited practical experience** with the tasks provided for in Regulation (EU) 2022/991 and new data protection rules (see Chart 7 and Chart 16). Only one Member State indicated that the reason it was unable to provide a reply was the **short timeframe for feedback**. All in all, these data suggest that the **evaluation was premature** to evaluate the implementation of (some) tasks from the perspective of the Member States.

Response Rate

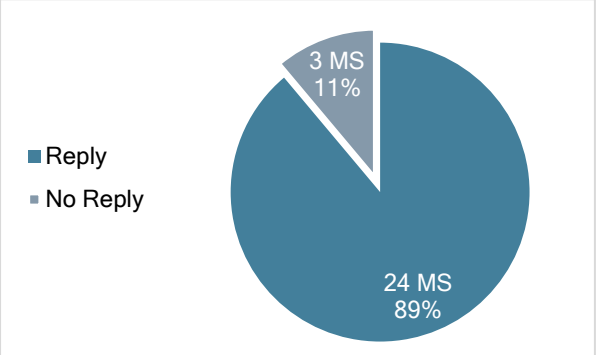

Chart 5 – Number of MS that replied

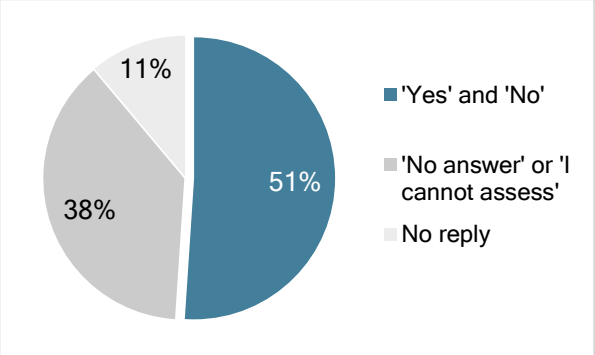

Chart 6 – Response rate as % of questions replied

2. Operational impact of the implementation of the new tasks

The first part of the questionnaire, which addressed the operational implementation of tasks provided for in Regulation (EU) 2022/991, included three questions.

---

121 Notwithstanding its special status, Denmark provided its feedback limited to the cooperation of Europol with private parties pursuant to the new Articles 26 and 26b ER, in combination with Article 18 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

122 This value is slightly overestimated. The response rate is calculated without including the questions asking for a rating that received very few replies.

Question 1

Do you have any experience with the support of Europol in relation to its new tasks since the entry into force of Regulation (EU) 2022/911?

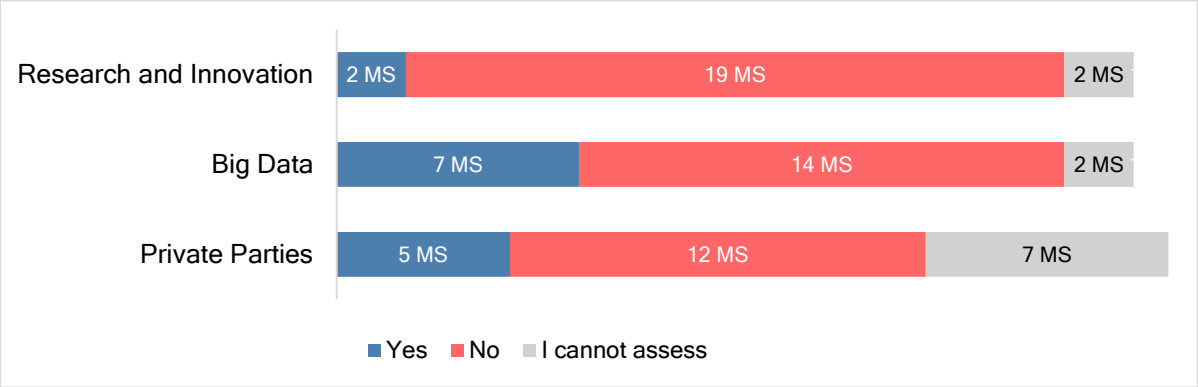

Chart 7 – MS experience with the new tasks (Q1.a)

Please rate your overall experience with the implementation of the new tasks, on a scale from 1 (very limited) to 5 (very good)

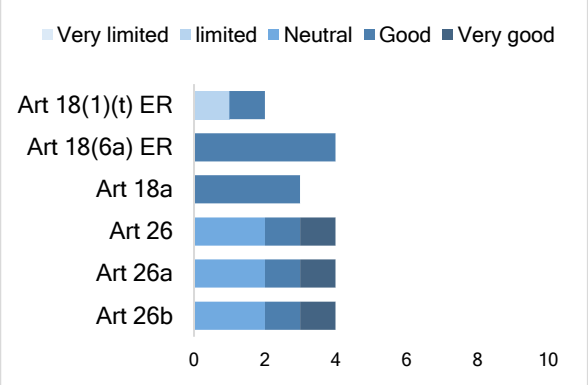

Chart 8 – Rating of MS experience with the new tasks (Q1.b)

Based on their replies, **nearly all respondents lack experience with,** or are **unable to assess,** at least one of the new tasks.[123] 'Due to lengthy consultations with stakeholders, it took a long time before these instruments could become fully operational', as observed by a Member State. Only four or fewer Member States provided a rating, so the outcome is not very indicative.

Several (7) Member States reported they had **experience** with the provisions of Articles 18(6a) and 18a ER on the **analysis of large and complex Datasets** (so-called 'big data'). A Member State says '[t]he Foreign Terrorist Fighters (FTF) lists provided by third parties, and which contained a huge dataset, were **handled professionally** by Europol's European Counter Terrorism Centre (ECTC) and the data processing as well as the analysis they created, supported the Member States. In the analysis of large and complex datasets, it is challenging to properly carry out data subject categorisation and prove the link to the perpetrator, which Europol can support'. Another Member States refer to '[a] massive volume of virtual wallets, transactions, virtual wallet users, IP-addresses, media access control (MAC) addresses, and phone numbers [shared with Europol for further processing]' and 'to the support […] provided in different Operational Task Forces (OTF) focusing on organised crime, child sexual abuse and violence as a service. The information has been obtained from, e.g. encrypted chats, closed online forums, seized hardware (phones, computers, …)'. A Member State stressed that 'it is also difficult to give any concrete examples as most data – legally that is to be considered as non-DSC data - in this context was

[123] Due to its status as a third country towards Europol, Denmark is concerned by the new provisions on private parties only in combination with Article 18 DSA, that applies to Denmark as it falls beyond the scope of Denmark opt-out.

delivered in the context of **SKY ECC and other similar investigations** which were always regarded as being data relating to criminals (so DSC was considered to be determined already)'.

Some (5) Member States replied that they have experience with Articles 26, 26a and 26b ER on the exchange of personal data with private parties and their comments **were overall positive**. Two of them specified that their experience is related to Article 18 of Regulation (EU) 2022/2065[124] on a Single Market For Digital Services ('Digital Services Act', or 'DSA') and one with the Regulation (EU) 2021/784[125] on addressing the dissemination of terrorist content online (TCO). A Member State recalls that 'Europol supported the […] activities in international operations, including **Phobos**[126] and **AKIRA**, which dealt with ransomware attacks. Through the transfer of data on disks by officers, Europol placed images of the servers on the Low Frequency Effect (LFE) and the data was analysed […]. Europol has sent several notifications under Article 18 DSA from private parties to their Point of Contact, but the number of investigations supported is unknown. The experience of the third Member State regarding Terrorist Content Online (TCO) is that **internet providers are deeply engaged** in the fight against terrorism, and they have sent their indications of terrorism-related content, including personal data. They can provide strong assistance in identifying suspects and support the investigations. Europol forwarded data received from private parties, which Europol analysed in the initial stage, identified the country to which it was linked and then forwarded to the competent country. In particular, **Europol provided support for online crises, including primary checks on entities**. […] Regulation (EU) 2022/991 enhanced the effectiveness of Europol and assists Europol to take over more burden from the Member States, at the same time, this commitment of Europol contributes to the investigations of the Member States'. **Only one Member State** is, instead, **rather critical**: 'Unfortunately, the occasional scarcity of information in the notifications received from private parties, and **the inability of Europol to create information from that void**, prevents the colleagues in Europol from providing an added value in the information supply chain'.

Regarding Article 18(1)(e) on 'research and innovation', **two** Member States replied positively to Question 1. Still, their experience is in reality limited to the **development of Europol's 'sandbox'**: '[the] Police has supported Europol in their development of the so-called 'Sandbox' by sharing national experiences of developing machine learning tools'. Another Member State also affirms that '[… it] participates in the activities of the European Clearing Board, during which [they] have been informed about the development of the Europol sandbox platform [and are] convinced that this platform **will be instrumental in testing projects**. However, they have no practical experience in this field'. A Member State notes negatively that, 'regarding the processing of personal data for research and innovation projects, Europol developed a minimal viable product (MVP) of the sandbox. **The MVP does not (yet) allow the exchange of personal data with the Member States**'. Another explains: 'Since there was only one new R&I project created by Europol and we have not yet practically cooperated in that regard; it is difficult for [them] to assess at this time. Also, they do not have any experience in the recently created Europol sandbox'.

---

124 OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.

125 OJ L 172, 17.5.2021, p. 79, ELI: http://data.europa.eu/eli/reg/2021/784/oj.

126 https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown.

Question 2

Do you consider that the possibility of Europol to propose SIS alerts in the interest of the Union will support your activities?

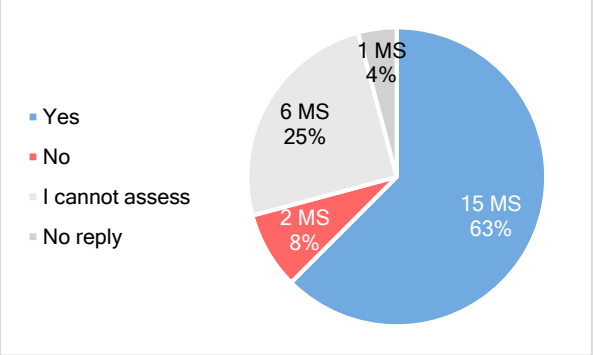

Chart 9 – Expected Benefits of the new SIS information alerts upon proposal by Europol (Q2)

Although not yet operational, **15 Member States** (**63%** of the respondents) confirmed the relevance of the provisions on Europol's **proposal for SIS information alerts on third-country nationals for their future work**. Other Member States (**29%** of the respondents) indicated that they were unable to assess, and one Member State did not reply. Two Member States replied negatively; however, as explained further below, their explanations were inconsistent with the question.

Member States articulated extensively and very positively in their comments on the expected benefits of the SIS information alerts on third-country nationals upon proposal by Europol, and one Member State also added that 'any way to contribute to better investigation or preventive work by the police is **welcome and urgently needed**'. A Member State affirms: 'Third countries share information on their nationals with Europol, these individuals are in many cases **unknown in the EU and cannot be linked to a national investigation or case**. Europol's role, with the possibility of proposing an SIS alert, will **cover this gap**'. In the same vein, other comments stress that '[t]he centralisation of the agenda of information coming from third countries and parties should bring higher effectiveness and also allow a **complete picture** of the matter' and '[t]he added value [of the new provisions thanks to] Europol's ability to consolidate and analyse intelligence from third countries and international organisations, which might not otherwise be accessible to national authorities. Europol's proposals can help … identify persons of interest who may not yet be known … but who pose a potential risk within the Schengen area'. For another Member State, 'Europol-initiated SIS alerts will provide **early warning on high-risk individuals** (e.g., terrorists, violent extremists, organised criminals). They will enable frontline [police] units to act on threats not yet flagged by national authorities. [They will support] Law Enforcement Authorities in **targeted checks**, **surveillance**, or **detentions based on intelligence-led SIS alerts**, enhance border control and internal security through real-time, EU-level risk indicators. Alerts inserted (sic!) by Europol can highlight threats that Law Enforcement Authorities may not yet be aware of, based on intelligence from Third Countries or EU partners. They will strengthen police **situational awareness at airports, seaports, public spaces, and events**'. A Member State recalls the role played already today by Europol in processing information from third countries: 'due to the work which Europol's European Counter Terrorism Centre (ECTC) carried out regarding the huge Foreign Terrorist Fighters (FTF) lists, – the transliteration of FTF names, the clarifications of biometric data –, Member States were able to conduct investigations and implement the necessary measures (insert SIS alerts)'.

Some Member States also highlight the main **crime areas concerned**. According to a Member State, 'the implementation of the new provisions is considered very beneficial for tracking movements of suspects across the EU's external borders [and can be expected] to be used in the context of **terrorism**, **migrant smuggling**, and **human trafficking**'. Another Member State observes '… the benefits are multiple: **Enhanced Border Security**: having their strategic

location on the EU's eastern flank, the ability to receive alerts on high-risk individuals from non-EU countries is essential. This will strengthen border control measures and help prevent the entry of persons who may pose a threat to national or European security. Improved Counter-Terrorism Efforts: The primary impetus for this new regulation was the need to track the movements of foreign terrorist fighters better. A **More Effective Fight Against Organised Crime**: The scope of these alerts extends beyond terrorism to include a wide range of serious, cross-border crimes. This will support the … police in combating everything from drug trafficking and human smuggling to cybercrime and financial fraud …'. Similarly, a further comment reads: '… the possibility for Europol to propose SIS alerts in the interest of the Union will support our activities. This mechanism enhances **cross-border cooperation** and strengthens our capacity to identify and respond to serious threats posed by third-country nationals involved in **terrorism or organised crime**.

A Member State stressed the shortcomings of SIS information alerts compared to SIS alerts for entry refusal[127]: 'From a security perspective, entering SIS alerts for "**Refusal of the entry into the Schengen area**" is considered to be the **most effective way to prevent the entry** of individuals into the Schengen area who may pose a potential threat to public security and order. Other categories of SIS alerts … may also be considered as an alternative but are probably less effective than alerts for the refusal of the entry. For instance, there are Member States that have a **significantly higher national threshold for entering alerts for refusal of entry and can therefore only use the information alert.** In this sense, a benefit is expected in terms of "**burden-sharing**". Since the information alert is not yet operational and no experience values are available, it is also not possible to say with certainty how the benefit will concretely manifest itself'.

Two Member States replied **negatively** to Question 2. In their comments, Member States refer rather to the **direct entry of SIS information alerts by Europol,** though. They do not raise objections to the actual provisions of Article 4(1)(t) ER. One of them states that '[it remains] **very reluctant** to grant Europol the possibility to issue alerts themselves as this would be an **important change in principle as regards the tasking, as this would imply that Europol would also accompany the alert with an action to take**. It would probably be better to test the implementation of the information alerts before trying to add to this possibility.' The other Member State: 'opposes granting Europol the possibility to insert information alerts in SIS, which is an **empowerment of Europol's supervisory powers vis-à-vis individuals and does not address operational challenges**. This mechanism would not allow for the effective detection of individuals reported during checks or for effective measures to be taken against them. Thus, it would create many difficulties: (i) risk of telescoping with the operational follow-up put in place by the Member States on targeted individuals and confusion around the respective responsibilities of Europol and national services, both on the ground (lack of precise action) and in the investigation process; (ii) difficulties in securing data, which may ultimately lead to a lack of readability of the SIS (incorrect or approximate names or dates of birth, missing aliases, etc.). In the light of these factors and in a comprehensive manner, the decision to insert a SIS alert and, where appropriate, the selection of the article selected are choices which must remain in the hands of the Member States alone'. One Member State, on the contrary, would **prefer 'Europol being able to input alerts directly into SIS** rather than proposing it to Member States'.

---

[127] According to Article 6(1)(d) of Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), '[f]or intended stays on the territory of the Member States of a duration of no more than 90 days in any 180-day period, which entails considering the 180-day period preceding each day of stay, the entry conditions for third-country nationals shall be the following: … (d) they are not persons for whom an alert has been issued in the SIS for the purposes of refusing entry'. In other words, SIS alerts for entry refusal triggers automatically a denial to enter the Schengen area, while a SIS information alert leaves margin of discretion to the border authorities and requires further assessment.

A **Member State** comments more cautiously that 'Europol's right to propose SIS information alerts can enhance the capacity to combat cross-border crime and terrorism by leveraging Europol's unique position and analytical expertise' but also recalls that 'it's **important that strong safeguards for data protection and fundamental rights are enforced**. Given the varying data protection standards and legal frameworks in third countries, a **cautious approach is necessary** when acting upon or proposing alerts based on such information'.

Two Member States point to the **key role of the SIRENE Bureaux** that are 'responsible for managing the exchange of information related to SIS alerts [and] will play a key role in this new process. When a "hit" occurs on a Europol-proposed alert […], the SIRENE Bureau will coordinate the necessary follow-up actions and share relevant information with Europol and other Member States'. It is considered important that '[these provisions] **must not generate additional workload for the SIRENE Bureau**, as in some Member States, the responsibility for making these entries lies with them'. As another Member State further details '... the implementation of Article 4(1)(t) ER will mean (or already means) the costs and resources necessary for the reprocessing of the national source systems for the SIS, all the searching tools into the SIS, as well as the change of SIRENE Workflow. ... Europol is not providing any support in this regard. Vice-versa, [Member States] support Europol in running SIRENE tests for implementing necessary changes'.

Question 3

Do you consider that the conditions set out in the 2022 Amending Regulation for the new tasks are overall adequate, sufficiently clear and easy to implement?

Based on your experience, if any, please rate the complexity of the new provisions and rules from an operational point of view on a scale from 1 (very complex) to 5 (sufficiently clear)

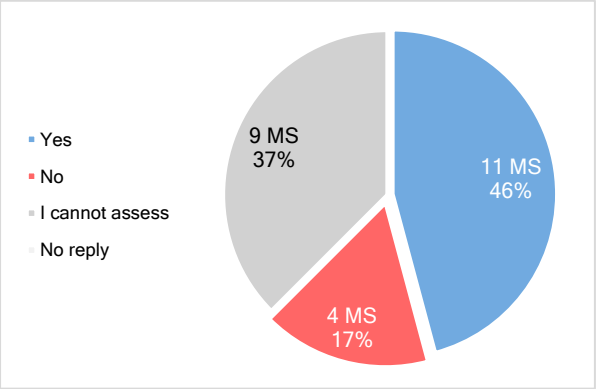

Chart 10 – Clarity of new tasks' conditions (Q3.a)

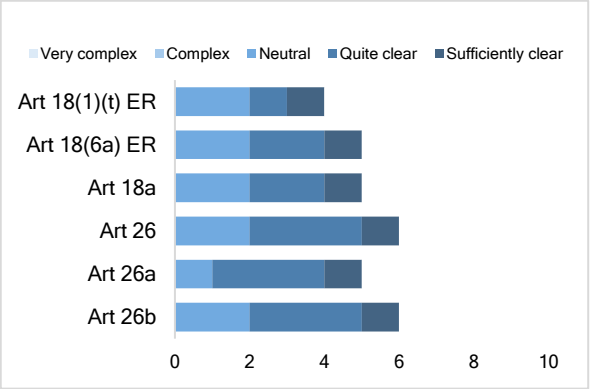

Chart 11 – Rating of the new tasks' clarity (Q3.b)

Many respondents (**46%, 11** Member States) consider the conditions for the exercise of the new provisions **sufficiently clear** and **easy to implement**. One Member State comments: '[t]he provisions of [Regulation (EU) 2022/991] are sufficiently clear and, although their real-life applicability is not immediate, we feel confident that when instances prompting their application occur, we would be in the position to make use of the provisions in a lawful and useful manner'.

However, the rating of the **clarity of the provisions** is **not high** (**3.8** points out of 5), and comments indicate **areas for improvement**. A Member State writes: 'challenges may arise regarding data management and accountability, respect of fundamental rights and privacy protection, allocation of Europol human resources and technical tools, cooperation with third countries'. For another Member State, 'processing data from private parties under Articles 26, 26a and 26b ER requires careful consideration of **data protection principles** and **additional coordination with national authorities**. In the context of [research and innovation] projects, the legal framework is sufficiently clear, and the procedural steps are manageable'.

For **a few** (4) Member States, the current conditions are **not appropriate**. For one of them, 'based on its experience, […] the new provisions carry a certain degree of complexity. To obtain further clarity, it was necessary to carry out **extensive and lengthy discussions between Europol and Member States and prepare further guidelines and legal decisions**. Some of those provisions are not yet in place because the level of maturity has not yet been achieved. [Articles 18(6a) and 18a ER] could benefit from a rewording in light of the experience achieved since 2022, dealing with [data without Data Subject Categorisation] and the opinions set by EDPS, aiming to achieve a better balance between data protection requisites and police cooperation. [The provisions on **SIS Alerts** under Article 4(1)(t) ER and on **research and innovation** under Article 18(1)(e) ER are] clear and adequate, but **require strong governance**, particularly when involving personal data or sensitive technologies. [The provisions on **big data** under Articles 18(6a) and 18a ER are] adequate and mostly clear but **technically demanding**. Practical implementation requires strong capabilities and safeguards. [The provisions on **private parties** under Articles 26, 26a and 26b ER are] sound and generally clear, but **practical impact varies based on Member States' engagement and legal framework**'. Another Member State explains: 'It's difficult to assess the complexity when **we have not made use of most of the new possibilities at this stage**. We still have questions about the reasons exactly why, and for some issues, we will liaise bilaterally with Europol. As we have not participated to any R&I project, we have not used the new finality in article 18 (1)(e) ER. This being said, we are not sure if there would be a need to do this as this would depend on a project that would need specific data that is not yet available for Europol and/or an implementation (depending on the wishes of the individual Member State) by Europol where an additional finality would be added to information that was sent with another finality'.

Other Member States did not provide an assessment nor comments.

3. Cost-benefit analysis

The second part of the questionnaire included two questions.

Question 4

Have you made use of the support provided by Europol and was such support beneficial for your activities?

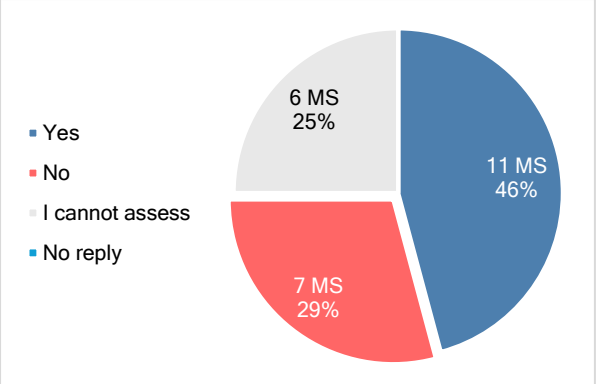

Chart 12 – Benefits of the new tasks (Q4.a)

Please rate the relevance of the support of Europol under the new provisions from an operational point of view on a scale from 1 (very limited) to 5 (very important).

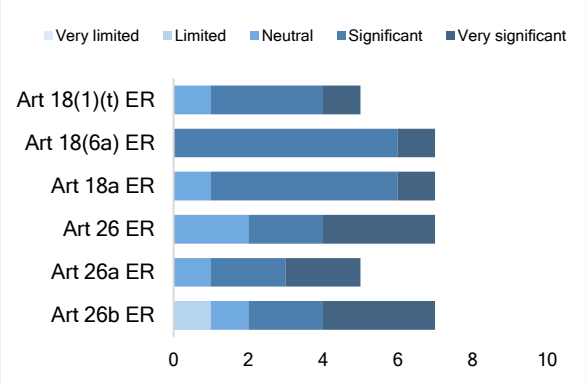

Chart 13 – Rating of the relevance of the new tasks (Q4.b)

Slightly less than half of respondents (**46%**, **11** Member States) consider that **they benefited from the new forms of support**. Most respondents indicated that they cannot assess the benefits of the new tasks (25%) or that they have not utilised the new forms of support and therefore have not benefited so far (29%). This outcome is consistent with the answers to Question 1 (see Chart 7). A Member State explains that '[it has not faced yet any investigation that required this

particular support'. The rating of the relevance ranges from neutral to very significant, but the number of replies is limited (six or fewer).

On the new provisions on the analysis of large and complex datasets, one Member State observes that '[… they] didn't experience any particular problems before the EDPS opinion. So, in itself, the **new provisions have brought a clear legal basis** but have **not changed the possibility drastically** to send data to Europol'.

A Member State notes that '**[s]mall countries** in particular are aware that [they] **do not have the technical or human resources** to conduct certain larger, more complex investigations on [their] own, which is why Europol's support is essential in such cases'. Also **bigger Member States** commented, however, that '[t]here are so far only very few experiences in practice, yet. However, [they] **value the support of Europol and the new possibilities from [Regulation (EU) 2022/911]**' and 'while [Regulation (EU) 2022/991] is still in a relatively early phase of implementation, its new provisions regarding big data, cooperation with private parties, and research and innovation are already providing **tangible benefits** to the […] Police'. For a Member State, 'the new tasks are clear and support Member States, but the processing of personal data for research and innovation projects has not given added value to our work so far. The SIS alerts and the **private parties' contributions were supporting significantly their operational work**, and the intelligence gathering. For another Member State, 'in a broad sense, the new tasks brought EU added value, especially those concerning big data, as Member States Law Enforcement Authorities lack full analytical resources to deal with those challenges. However, the full potential of these new tasks is yet to be achieved. Operational implementation of **cooperation with private parties under Article 26, although necessary in certain fields, requires an in-depth reflection in light of recent international developments**, with special caution on the sharing of personal data. The implementation of Europol's new tasks under the [Regulation (EU) 2022/991] unlocks capabilities that are only achievable through collective EU action. It ensures that all Member States — regardless of size or capacity — benefit from shared intelligence, innovation, and operational coordination. These enhancements strengthen EU internal security as a whole, delivering clear added value beyond what national authorities could achieve on their own: SIS alerts ensure timely, EU-wide visibility of threats that may otherwise go undetected. Research and innovation (Article 18(1)(e) ER) provides all Member States - including those with limited technical capacity - access to cutting-edge innovations developed in a centralised legal EU framework. Big data Processing (Article 18(6a) and 18a ER) provides central oversight and data protection safeguards, ensuring that big data processing complies with fundamental rights and EU standards. Individual Member States lack both the legal authority and technical capacity to process such multi-source datasets at this scale. Private party cooperation (Arts. 26, 26a, 26b) establishes a single, trusted EU-level channel for cooperation with global tech companies, financial institutions, and service providers'.

On **research and innovation**, a Member State explains 'The new mandate for research and innovation establishes Europol as a central driver for developing the next generation of law enforcement tools (Innovation Lab). This is a strategic, **long-term benefit for all Member States**'. Another Member State notes that 'Europol's support for innovation, in particular the **work of the Innovation Lab**, is **outstanding**. However, [the Member State] has not yet experienced the results of the "sandbox" platform'.

Regarding **cooperation with private parties**, '[…] it can facilitate and coordinate requests, leveraging its established relationships and expertise to expedite access to **crucial digital evidence**. This is particularly beneficial for […] investigations with a cross-border digital footprint'. Another Member State notes that 'the main benefit of the support is the large capacity of Europol's European Counter Terrorism Centre (ECTC) in processing data from Third or Private Parties. The ECTC can commit professionally the dataset analysis and due to this work the Member States, and they can carry out the investigations and map out the networks of

terrorists. The new tasks are of great importance in the course of investigations. **The handling of data from the private sector has opened up new possibilities.**'

Most beneficial would still be according to a Member State the processing of **large and complex datasets**. 'The most significant, though least publicly visible, benefit comes from the new legal framework for processing large and complex datasets. This provision legally **solidifies Europol's role as the EU's central criminal information hub**. For [the] Police, this means they can lawfully share vast quantities of data seized during major investigations - such as data from servers, computers, mobile phones, or extensive financial records - with Europol. Europol, in turn, can […] legally use its superior analytical resources and advanced technologies to process this data, identify links, and extract actionable intelligence that might be beyond the capabilities of national units'.

A Member State comments that '[t]he support provided by Europol under its new competences has been particularly valuable in investigations related to drug trafficking, organised crime groups, and the processing of encrypted data. In drug-related cases, especially those with a cross-border dimension, Europol provides **analytical support** that helps **link activities observed in different Member States**. Europol's infrastructure also **enables fast information exchange on suspects, vehicles, and trafficking routes**. In organised crime group investigations, Europol's data processing capacity helps identify criminal structures, roles within the network, and logistical chains. This is **crucial for coordinated and targeted action by Member States**. When working with large and complex datasets, including encrypted data, Europol's technical tools and experts support the decryption, classification, and analysis of information, which is often not feasible at the national level due to time and resource constraints. In such cases, Europol significantly **accelerates the investigation process**, **reduces duplication of efforts between Member States**, and provides added value that national authorities could not achieve on their own'.

Question 5

Do you consider that the support provided by Europol with the implementation of its new tasks also delivers EU added value, or in other words provides benefits beyond what would be possible by Member States acting independently?

Please rate the EU added value of the new provisions on a scale from 1 (no added-value) to 5 (significant added-value).

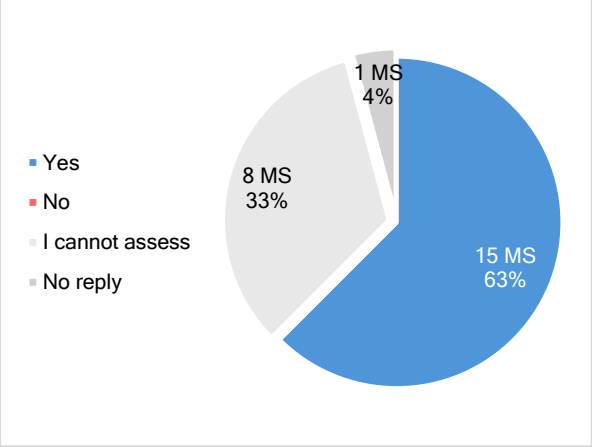

Chart 14 – Added value of the new tasks (Q5.a)

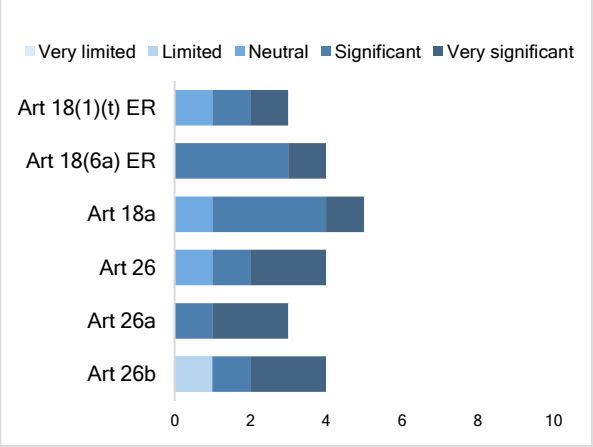

Chart 15 – Rating of the added value of the new tasks (Q5.b)

All respondents providing a view (**15** Member States) indicated that the tasks provided for in Regulation (EU) 2022/991 provided **EU added value**. The very few Member States providing a rating assessed the added value on average as **high** (**4** out of 5).

The EU added value is given, for a Member State, from '[t]he existence of **common tools**, **secure communication platforms for exchanging information**, **analytical capabilities** and **expertise** [that] have positive impact on the operational and analytical capacity of any Member State […] Europol is in a strategic position in that it is **privy to the most holistic picture possible of the data available at an EU wide level**, allowing it the best position to benefit to the utmost of Europol's support'. For another Member State: 'The support provided by Europol under its new tasks clearly delivers EU added value, offering benefits that could not be achieved by Member States acting independently. Examples of activities that would **not be possible at the national level alone** include: **cross-border analysis of encrypted communications** (e.g. from **EncroChat** or **Sky ECC)**. Europol provides unique technical capabilities and joint coordination across multiple jurisdictions, which individual Member States do not possess on their own. Real-time deconfliction and linking of intelligence related to organised crime groups operating simultaneously in several Member States (e.g. **Balkan-based criminal networks involved in cocaine trafficking**[128]). Without Europol's centralised database and analytical capacity, crucial connections would be missed. With the processing and *triaging* of large datasets from private parties (e.g. social media platforms or tech companies during online crisis situations). Europol facilitates secure data flows and coordinates responses that go beyond national legal and technical capacities. Immediate alerts and operational coordination through the Europol command centre during joint action days (e.g. EMPACT operations), enabling simultaneous arrests and seizures in multiple countries. Support in online child sexual abuse investigations: Europol acts as a central hub for matching fragmented information from multiple Member States and private parties, reducing duplication and speeding up victim identification. These examples highlight how Europol's role goes beyond national possibilities and provides a central intelligence and coordination function that significantly enhances collective EU security'.

A Member State comments: '[t]he new tasks are clear and support the Member States, but the processing of personal data for research and innovation project has not given EU added value to our work so far. The […] **private parties contributions were supporting significantly our operational work, and the intelligence gathering**'. For other Member States 'Europol's new tasks, have strengthened its role as an analytical and coordination hub, which realistically improves the operational activities of the police, especially in cases requiring international cooperation, analysis of large datasets or cooperation with the private sector. Some Member States lack **sufficient tools and staff** to process **complex and large amounts of data**. In the same vein, other Member States write: 'While the full operational potential of Europol's new tasks is yet to be realised, their future implementation is expected to deliver significant added value at the EU level. In particular, **enhanced cross-border coordination will become increasingly important as criminal networks continue to operate across jurisdictions**. Europol's central role can ensure more efficient joint responses. In the area of research and innovation, the continued **development of AI-driven tools and data analytics,** in collaboration with Europol, will enable Member States to benefit from shared technological advancements and **avoid duplication of efforts**. With the expected rise in the use of large and complex datasets, Europol's capabilities can **help standardise data analysis approaches and strengthen interoperability between national systems**. Once fully implemented, mechanisms for engagement with private entities could **open new avenues for detecting and disrupting criminal activities online**, particularly in **cybercrime** and **child sexual abuse content**', and 'Regarding research and information, it is our understanding that some Member States lack this possibility. Regarding "big data", it is our understanding that the storage time is longer than in many other Member States. Regarding private parties, it is our understanding that **many Member States** have **benefited from Europol's signing of Memoranda of Understanding (MoU)** with Private Parties that have improved cooperation'.

---

128 Europol, press release: 37 arrested as violent Balkan criminal cell is taken down - Ringleader orchestrated gang's criminal activities from behind bars | Europol.

4. Implementation of the Personal Data Protection Safeguards

The third part of the questionnaire on the implementation of the new personal data protection safeguards included three questions.

Question 6

Do you have any experience with the implementation by Europol of the new data protection safeguards resulting from the alignment with Regulation (EU) 2018/1725[129]?

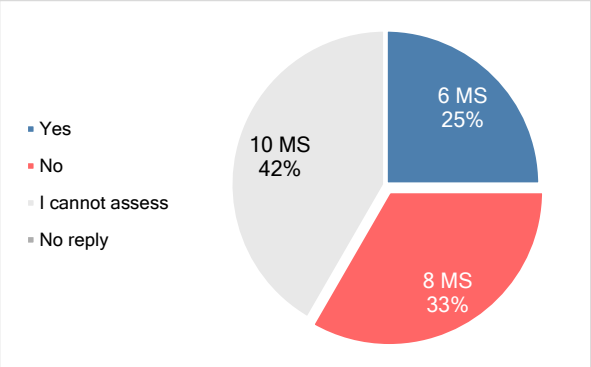

Chart 16 – Experience with new data protection rules (Q6)

Question 7

Do you consider that the alignment with Regulation (EU) 2018/1725 facilitated the flow of information between Europol and the Member States?

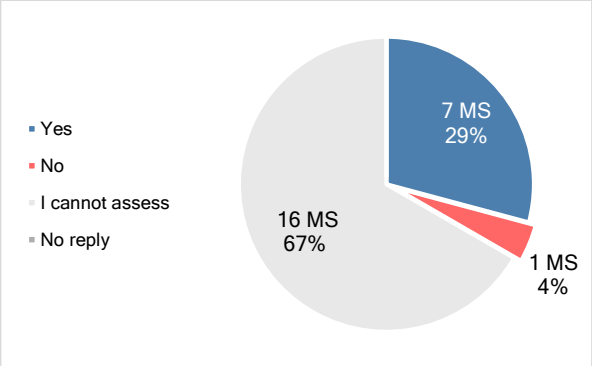

Chart 17 – Benefits of new data protection rules (Q7)

The vast majority of respondents (**67%**, **16** Member States) did not feel in a position to reply to Question 6. Only **some respondents** (**25%**, **6** Member States) indicated having **experience with the new data protection safeguards**, which is in line with the replies to Question 1 on the more general experience with the new tasks.

Question 7 also had a limited response rate (33%). Nearly all Member States (**7** out of 8) that expressed a view consider that **the alignment with Regulation (EU) 2018/1725 facilitated the flow of information between Europol and the Member States**. A Member State observes in particular: '[t]he alignment with the said regulation safeguards allows personal data being handled securely and in compliance with EU legal framework. Thus, within the context of police cooperation, **trust is enhanced** and Member States are **exchanging information easily and in a timely manner**'. For another Member State, 'the alignment with Regulation (EU) 2018/1725 has significantly facilitated the flow of information between Europol and Member States. For instance, in an investigation into an organised group involved in drug trafficking, we were able to quickly transmit personal data and related financial records to Europol because the safeguards

[129] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj.

and procedures were clearly defined. In the past, such exchanges were delayed due to differing interpretations of data processing rules. Now, the **harmonised framework allows faster cooperation without legal barriers**'. In the same vein, another Member State notes '[t]he alignment with Regulation (EU) 2018/1725 does **not directly force an increase in data sharing** - but it removes key legal and procedural barriers, promotes trust, and ensures that data flows are legally sound, secure, and rights-respecting. These improvements create a **more predictable and interoperable environment** for information exchange between Europol and Member States. Europol can now act as a trusted intermediary for information coming from private entities (e.g. telecom providers, financial services, tech platforms)'.

One Member State replied negatively and explained 'We have experience with these new safeguards, albeit only to a limited extent. **Most of our experience relates to access requests from data subjects** received by Europol, which concern data provided by [the Member State]. Part of the legal framework on this matter is now to be found in the EUDPR instead of the Europol Regulation, and some of the rules in there are different to a certain extent than the previous ones. However, **we don't really see a lot of difference in the way these requests are processed in practice**. In particular, the grounds for refusal of access have somewhat changed in theory, but in practice, such refusals are motivated on the same grounds as before, as our motivation always fits under both the previous and the current grounds for refusal. Europol's DPF is constantly adapting these procedures to the changing legal framework, and we have the impression that **changed interpretation of the legislation** (by the courts, by the EDPS, …) has a **bigger influence on this than changes in the legislation itself**'.

Question 8

Do you consider that there are any remaining obstacles in the implementation of data protection safeguards by Europol that should be addressed to facilitate cooperation, and make Europol more efficient and effective to offer solutions for Member States?

If your reply is yes, in which areas in particular:

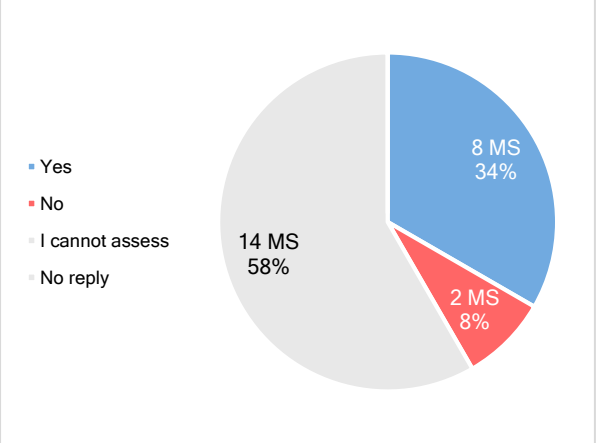

Chart 18 – Shortcomings of the implementation of the new data protection rules (Q8.a)

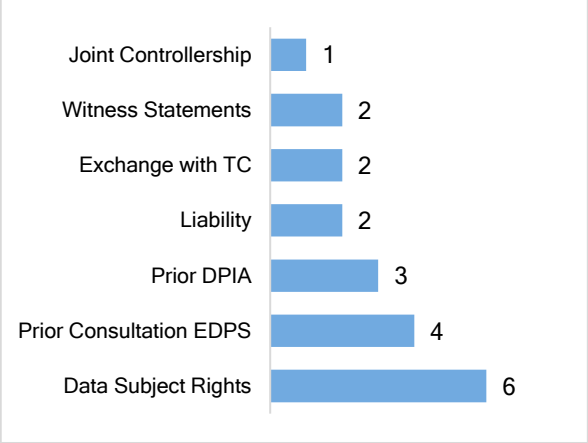

Chart 19 – Main areas for improvement in the implementation of the new data protection rules (Q8.b)

Only **two Member States** expressed the view that there are **no remaining obstacles**. One of them mentioned that 'in January 2025, it received a notification from Europol Data Protection Supervisor (EDPS), which contained a data subject access request submitted to Europol. The information exchange and the cooperation with Europol […] functioned properly. **Communication between Member States and Europol has become even more efficient**, with the possibility to cooperate through additional data categories.'

Most respondents (**54%, 13** Member States) consider that there are **areas for improvement regarding** the **implementation of data protection safeguards**. 'Despite significant improvements and a **robust legal framework**, there are **some remaining obstacles** in the implementation of data protection safeguards by Europol that, if addressed, could further facilitate cooperation, enhance efficiency, and make Europol even more effective in supporting Member States'. A Member State lists the main challenges as it follows: 'While Europol's data protection framework is robust and rights-compliant, remaining legal and operational uncertainties can create real obstacles to cooperation. To strengthen Europol's ability to support Member States, **targeted improvements are needed** — including **faster oversight mechanisms**, clear **liability rules**, flexibility in **third-country exchanges**, and solutions for **judicial usability of Europol products**'.

Most comments focus on difficulties with the current oversight. A Member State notes: 'there is reluctance to share covert surveillance data, intelligence from sensitive national sources, or data linked to ongoing investigations where **timely restriction of rights** is not guaranteed or large, unstructured datasets requiring urgent action, where the European Data Protection Supervisor (**EDPS**) **consultation could delay response**. There is reluctance to produce innovative digital tools or experimental analysis models, where Data Protection Impact Assessment (**DPIA**) **constraints outweigh the perceived benefit**. For a Member State, 'if the European Data Protection Supervisor (**EDPS**) can grant **access to data subjects** although the national data protection authority denied access there is a risk of jeopardising investigations'. Another Member State notes: 'It is a standard practice in Member States to give the same answer in cases where there are no data present on the requester as in cases where there are data present, but the requester cannot get access. Usually, in Member States, in both cases, a reply such as 'there are no data to which you legally have access' is given, to avoid data subjects drawing conclusions from potentially diverging answers in both cases. However, **because of the way the EDPS interprets certain rules there have been issues with the possibility to apply this practice by Europol** as well, for access requests on data in the Europol systems. This might lead to investigations being seriously hampered because of such access requests, which is not at all the goals of the legislation'. The same Member State comments: 'We do have a strong impression that the EDPS demands prior consultation more often than the national supervisory authorities do. And since the conditions in Article **90 EUDPR** and in Article **28 LED** are literally the same, such **diverging interpretations of the necessity for prior consultation** seem **arbitrary to a certain extent**. In practice this leads to delays when Europol needs to set up new processing systems, hampering the effective implementation of the new possibilities created by the 2022 amendment and hampering the provision of agile services for the MS'.

Some Member States flag, for example, issues in relation to the obstacles faced in relation to the development of **Joint Operational Access Concept** (**JOAC**), one of them explaining 'the **prior consultation procedures with EDPS are too long** and impact on the operational support of Europol, as the launch of Joint Operational Access Concept (JOAC)'. Another Member State argues that 'currently there are still issues with the demand for **joint controllership** for joint analysis by the EDPS. In anticipation of the formal response, it's difficult to predict, but it could very well be that the **formal position of the EDPS might lead to further complications in implementing yet again a new operational form of cooperation** and […] that the EDPS will also ask to **apply this to OTF's and JIT's**'.

'The processing of large and complex datasets where data subjects are not immediately categorised (suspects, victims, witnesses, etc.) has been a major point of contention between Europol and the European Data Protection Supervisor (EDPS). While [Regulation (EU) 2022/991] aimed to provide a legal basis for this, **the operational reality of managing and rapidly categorising vast, incoming data streams remains challenging**'.

In relation to third countries, two Member States note the need to strict safeguard mentioning that 'processing of third-country intelligence or strategic data from partners outside the EU needs **clear onward-sharing mechanisms**' and '[i]t's important that strong **safeguards for data protection and fundamental rights** are enforced. Given the varying data protection standards and legal frameworks in **Third Countries**, a **cautious approach is necessary** when acting upon or proposing alerts based on such information'.

As another challenge, a Member State recalls: 'Personal data of **vulnerable individuals** (witnesses, informants, minors) are not shared unless clear safeguards and liability limits are in place. It is difficult to use Europol analytical products in judicial proceedings without certainty that their **staff can testify, or the product is admissible**'.

Question 9

What is your experience with complying with the requirement to determine the categories of personal data and categories of data subjects included in large datasets before processing the personal data (so-called Data Subject Categorisation)?

Could you please rate below the estimated costs for Data Subject Categorisation from 1 (negligible) to 5 (very high)

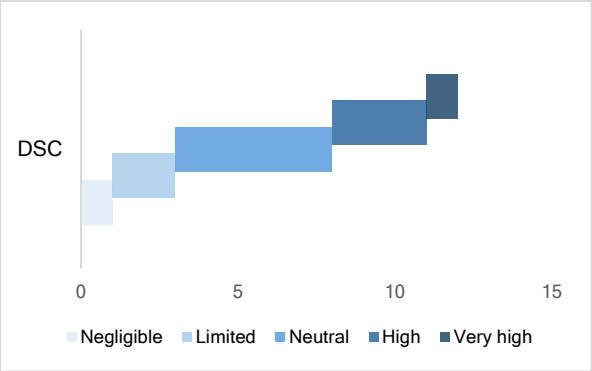

Chart 20 – Rating of the costs generated by the DSC (Q9.a)

Do you consider that the legal requirements for Data Subject Categorisation are sufficiently clear from an operational point of view?

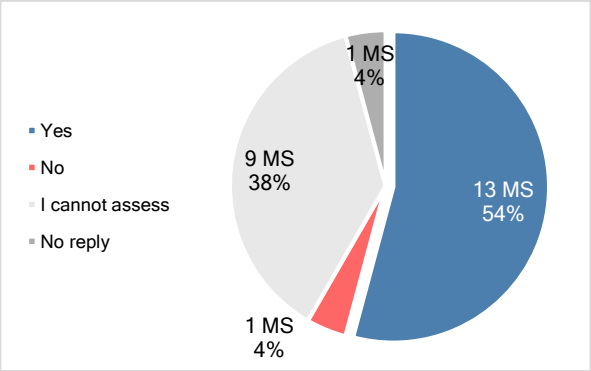

Chart 21 – Clarity of the requirement of the DSC (Q9.b)

For **half of the respondents** (**55%**, **12** Member States), the **provisions on the Data Subject Categorisation (DSC) are sufficiently clear**. Other respondents did not provide any assessment, except for one Member Stats for which there is a lack of clarity. The ratings of the costs were provided by over 10 Member States, showing quite divergent views.

One Member State explains: 'Now, during the work itself, we can clearly distinguish what kind of data we are dealing with, which can be very important in the investigation itself'. Another Member State '… find[s] the Data Subject Categorisation (DSC) easy to use, due to the fact the DSC validation is **implemented in SIENA as a mandatory field**, furthermore we have had the benefit of on-the-spot support in an investigation'. Similarly, another Member State notes that '[t]he Data Subject Categorisation requirements are clear and understandable from the operational point of view, because it is indispensable to link the person(s) to a certain case or investigation in order to be handled by Europol. **In the vast majority of the cases** […]**, the DSC is completed [by the Member State]**'. However, that same Member State also stresses that '[f]rom a practical point of view, when sending SIENA messages, it is necessary to pay attention to the categorisation of the data subjects and its consequent use. **In a complex investigation,** this can be **challenging for up to hundreds of entities involved**, both from a **Member State and Europol** analytical perspective'.

Some Member States consider the costs and challenges not negligible. The comments of three other Member States are fairly, if not very, critical: the first one writes: 'When dealing with large

and complex data sets the **challenges in categorisation** having in mind the requirements which need to be met are **considerable**. Besides the **time and resources (human, technical, financial)** allocated to implement this task, there are cases where the available information is not complete and structured whereas the **source may be non-standardised resulting in difficulties concerning the identification of data subjects**. Thus, the progress / course of the investigations will be affected'. For the second one: 'The new rules are generally understandable and provide a solid legal framework. However, some aspects are operationally demanding. The introduction of Data Subject Categorisation (DSC), while conceptually clear, proves **time-consuming** and **burdensome in practice, particularly** when dealing with **data that do not fall under predefined categories**'. The third Member States argues: 'Overall, the conditions set out in [Regulation (EU) 2022/991] are adequate and reasonably clear from a legal and conceptual point of view. However, the most challenging aspect from an operational perspective is the requirement to determine the categories of personal data and data subjects prior to processing large and complex datasets (for example, Data Subject Categorisation under Articles 18(6a) and 18a ER). This requirement imposes a **high administrative** and **analytical burden**, particularly when data is received from diverse sources (for example, Private Parties or Third Countries) and needs to be cross-checked quickly for ongoing investigations. The **18-month (extendable) temporary processing window is often insufficient in practice for large-scale cases involving encrypted or fragmented data**. Additionally, the obligation to functionally separate unclassified personal data, combined with the necessary interaction with the European Data Protection Supervisor (EDPS), adds a layer of complexity that can delay operational workflows in time-sensitive criminal investigations. A **more flexible or staged categorisation approach** would significantly improve implementation efficiency.'

A Member State provides a very articulated legal analysis:

'The provisions seem clear, but they do not solve the 'Big Data Challenge'. The challenge seems to be more related to how Europol can assess data as Data Subject Categorisation (DSC) completed (aggregated or individually) and how it can use Artificial Intelligence (AI) to process big data.

Overall, we are aware of Europol's challenge of processing all relevant data in a specific project in time, while accounting for all relevant data protection safeguards (the "**big data challenge**"). This is **also a challenge for many national law enforcement agencies**, although **the extent seems to vary depending on** how the **Law Enforcement Directive has been implemented in national legislation**, and how the national supervising authorities are interpreting the legal framework. In our experience, **Article 18(6a) ER has mitigated some of the big data challenge** for Europol by providing the opportunity of processing data temporarily for a 18+18-month period. However, **it does not solve the whole problem**. The reason, in our experience, is, among other things, the extensive demands for **manual verification** when Europol uses machine learning tools to process data, and the EDPS's interpretation of **how Europol should assess a big data set as DSC is completed** (DSC referring to Data Subject Category). The demand for manual verification at Europol seems to apply to all individual hits that are identified by machine learning tools for the purpose of cross-checking names and numbers, etc (i.e. processing according to Article 18(2)(a) ER). The practice seems to stem from **Europol's AI policy**, which in turn refers to an article in the previous Europol regulation that is now deleted. As the practice is still in place, we suspect, but have not been able to verify, that the manual verification requirement is related to the Artificial Intelligence (AI) Regulation. The challenge with the practice is that it slows down the processes substantially. Currently, it takes a Europol analyst **three working days to process the information from one seized phone**. In large investigations, we are often working with 100 phones from one member state alone. In summary, **the demand for manual verifications makes the management of big data impossible**. Another challenge is the **EDPS' disqualification of assessing large datasets as data subject completed (DSC) on an aggregated level**. If Europol is to comply with the EDPS requirements in this regard, it would

mean that it cannot assess, for instance, the content of a phone that has been seized from a suspect as 'DSC-completed' unless each piece of information in the phone (contacts, phone calls, messages, etc.) is assessed individually by being processed against an existing analysis project. This is, first of all, extremely time and resource-consuming, but perhaps more importantly**, there is also a serious risk of missing important connections** that can be crucial for identifying additional suspects or even preventing serious crimes. On national level, the possibility of assessing data sets as DSC completed on an aggregated level have been crucial to identify links that otherwise would have been missed and prevent crime. Also, the time period needed to identify a person behind an account has been drastically reduced, which has been one of the successes behind the reduced numbers of attacks […] recently. […] This is a **complex issue**, but it is **a key challenge that needs to be addressed if Europol is to remain a relevant operational partner and information hub**. The regulatory framework needs to be revised to encompass the complex big data reality that law enforcement is facing.

The interpretation of the European Data Protection Supervisor (EDPS) of these questions, right or wrong, makes the **management of big data close to impossible**'.

5. General comments

The questionnaire left the possibility to provide additional comments (Question 10) and some Member States provided also some generic comments on:

A. Cooperation between Member States and Europol

A Member State writes: 'Our overall experience with the implementation of Europol's new tasks has been positive, especially in the following areas: **On-the-spot operational support**: Europol's assistance during joint investigation teams and on-the-ground actions has been professional and well-coordinated. The presence of their experts enabled quicker cross-checking, cross-border analysis, and secure information exchange among Member States. **Use of technical tools**: Europol's analytical platforms have proven very helpful, especially when dealing with unstructured data (e.g. emails, documents, log files), enabling faster identification of relevant patterns and links in investigations. Implementation of data protection safeguards: While the legal requirements are strict, they have helped build mutual trust'.

Another Member State reports that 'In 2024, [its department that contributes to judicial investigations related to the fight against terrorism, violent extremism, and cybercrime] exchanged […] messages with Europol. These messages concerned screening requests or **OSINT** search queries on data communicated as part of judicial investigations, contributions to strategic questionnaires, and participation in operational meetings such as Referral Action Days, Terrorist Identification Task Forces, Operational Task Forces, and technical sprints. In 2024, the [same department] called on Europol to deploy a "mobile office" allowing several Europol officers to visit [its] premises to support the Directorate's efforts in connection with [a major sport event].'

B. Europol's capabilities under the current mandate

One Member State believes that: 'Europol's **current mandate provides sufficient scope** for the Agency **to strengthen and develop its police cooperation capabilities in these areas**. The priority is therefore to be able to exploit all the opportunities offered by its current mandate. However, an **independent evaluation is essential** before considering a targeted revision of the mandate'.

The same Member State also encourages **Europol to improve its analytical capabilities**. 'When a screening report and/or an Open-Source Intelligence (**OSINT**) query is requested from Europol, the [its] authorities undertake to provide feedback on the information provided: the possibility of prosecuting the information, the clarity and precision of the report, compliance with instructions, etc. The Agency can still improve in this area by **strengthening the training of its agents and its tools**. The other area [for] improvement for Europol is that of **biometric data**, which is still

poorly understood by the Agency at the dawn of implementing interoperability. The Agency is particularly **struggling to ensure the reliability of data when it is transmitted by third countries**'.

For another Member State: '[i]t is **important** that **Europol provides the necessary IT resources** in order to provide and further develop the tools for the implementation of the new possibilities of [Regulation (EU) 2022/991]'.

C. Need to develop new solutions like the 'Joint Operational Access Concept' (JOAC)

A Member State comments that **'**Faced with the increasing volumes of data, we need a data protection framework that enables law enforcement to process data effectively. This includes the **use of Artificial Intelligence (AI) and new technology to process big and unstructured data sets without unnecessary demands for manual verifications**.

These are major challenges for Europol today:

To find a more sustainable and long-term solution, we want to build on the […] **'Joint Operational Access Concept' (JOAC)** initiative to be able to conduct these operations remotely by storing our data at Europol and processing it together with other member states from afar. In short, **we want to be able to conduct the same kind of operations that we do at Europol, but without being dependent on expensive staff transfers. We want to move the information, not the staff**'.

Currently, it takes a Europol analyst **three days to process the data from one seized phone**. In large investigations, we are often working with 100 phones from one member state alone. Unless the conditions for how law enforcement can process data are changed, it is only **a matter of time before we lose the little advantage that we currently have on organised crime**.

Another pressing challenge in most major cross-border operations is the **need to process data jointly with other Member States and with Europol**. Currently, we can only conduct these joint processing operations (so-called **data sprints**) by moving our analysts to Europol or to a Member State. Understandably, **this is very costly**, and when it comes to Europol, we also have the pressing housing challenge.