EUROPEAN
COMMISSION

Brussels, 11.12.2025
COM(2025) 752 final

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

{SWD(2025) 404 final}

1. Scope of the evaluation

Since it began operating in 1999, **the EU Agency for Law Enforcement Cooperation (Europol)** has played **a central role in combating serious cross-border crime and terrorism**, becoming a key driver of law enforcement cooperation in Europe. The security landscape has undergone drastic changes over the last 30 years with a corresponding shift in the DNA of serious and organised crime.[1] Member States have new operational needs in addressing emerging threats effectively, and 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.

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

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

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

This report has been adopted in compliance with the Commission's obligation under **Article 68(3) ER**, to evaluate[7] and assess the operational impact of Europol's tasks as set out in Regulation (EU) 2022/991 three years after it entered into force. As mandated by the co-legislators, the Commission has: firstly, evaluated and assessed the **operational impact** of some of the new rules for processing personal data, in relation to Europol's objectives, under

---

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.*

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

7 This evaluation carried out in compliance with Article 68(3) ER is not the evaluation to be carried out according to the Better Regulation Guidelines in view of a possible proposal for a revision of the Europol Regulation. See also Section 4 below.

Article 3 ER (namely: support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating criminal offences falling under Europol's mandate); secondly, assessed the impact of those rules on **fundamental rights and freedoms** ('fundamental rights') as enshrined in the Charter[8], and thirdly, carried out a **cost-benefit analysis** of the related data processing tasks.

To prepare the review, the Commission services gathered information and feedback from various sources and held ad hoc consultations with Europol and the Member States. The accompanying **staff working document** provides a detailed description of the general context and methodology of the review, as well as a comprehensive account of the sources of evidence and consultations corroborating the main findings summarised in this report.

2. General context

In accordance with Article 68(3) ER, this Commission's report covers selected provisions of Regulation (EU) 2022/991, focusing on five key aspects of Europol's work.

(1) External dimension: Article 4(1)(t) ER on Schengen Information System (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 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.[9]

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[10] and requiring Europol to include a strategy for relations with third countries and international organisations in its multiannual programming and annual work programs.[11]

Article 4(1)(t) ER assigned a new task to Europol: to support Member States in processing data on individuals involved in terrorism or serious crime provided by third countries or international organisations. This includes **proposing to Member States the possible entry of information alerts on third-country nationals in the interest of the Union into the Schengen Information System (SIS)**. This new category of information alerts was introduced in 2022[12], following an amendment to Regulation (EU) 2018/1862 on the use of SIS in the field of police cooperation and judicial cooperation in criminal matters[13].

Certain information, especially when the individual concerned is not an EU citizen and there is no relation with a national case, is shared by the third country only with Europol, which

---

8 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.

9 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.

10 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.

11 Articles 12(2) ER.

12 Regulation (EU) 2022/1190; OJ L 185, 12.7.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1190/oj.

13 Regulation (EU) 2018/1862; OJ L 312, 7.12.2018, p. 56, ELI: http://data.europa.eu/eli/reg/2018/1862/oj.

processes the data and shares its analysis results with all Member States. The aim of the new provisions was to **maximise the exploitation of information** received by Europol from third countries by making it more accessible than if it were available only through Europol's own system. It complemented other measures, such as the European Search Portal (ESP) and the interoperability framework[14] between EU information systems for security, border and migration management, addressing the structural shortcomings related to those systems that impede the work of national authorities and notably border guards.

SIS is seen as a **key additional dissemination channel**: it is the most widely used database in Europe for law enforcement, border control, and migration. In 2024, over 15 billion searches were performed in SIS, compared with approximately 14 million searches in the Europol Information System (EIS) and fewer than 3 billion searches (worldwide) in the 19 INTERPOL databases, which are the two other leading information systems for competent authorities.[15]

(2) Innovation: Articles 18(2)(e) and 33a ER on 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[16] and have had such a profound impact on criminality as to alter even the deep nature, 'DNA', of serious and organised crime threats.[17] 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 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.[18]

Established in late 2019, at the mandate of the JHA ministers of the EU Member States, the **Europol Innovation Lab (EIL)**[19] 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 EIL's potential 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[20].

Article 18(2) ER on the purposes of information processing activities was amended to enable Europol to **process operational personal data** also **for research and innovation projects**. The availability of high-quality datasets to enable the empirical testing of the validity of new

---

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

15 eu-LISA 2024 SIS Annual Report, available online under https://www.eulisa.europa.eu/sites/default/files/documents/sis-annual-report-2024.pdf, Europol, Consolidated Annual Activity Report (CAAR) 2024, available online under https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF, and https://www.interpol.int/How-we-work/Databases.

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

17 Europol, EU SOCTA 2025, p. 19.

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

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

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

tools is widely regarded as a key precondition for developing technologies. By contrast, unreliable or biased datasets for testing may lead to producing poor technologies.[21]

Tailored data protection safeguards for such processing were laid down in Articles 18(3a), 30(2) and (3), and **33a ER**. The latter Article required the establishment of a **sandbox environment** by stipulating that any personal data processed in the context of a project must be temporarily copied into a separate, isolated, and protected data processing environment within Europol to be used solely for that project.

(3) Criminal investigations: Articles 18(6a) and 18a ER on the conditions for the processing of personal data received without Data Subject Categorisation (DSC)

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**, and by detecting links between criminal offences and criminal networks across 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**, including crime.[22] Investigations into organised crime or terrorism have started to face the challenge of analysing large volumes of electronically stored data, often amounting to terabytes, including audio, video, and machine-generated data seized during investigations. For example, in the joint investigation to dismantle the EncroChat network[23], 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'[24]) is key for law enforcement and judicial authorities.

While the Europol Regulation adopted in 2016 did not impose restrictions as such on the analysis of big data, it lacked structured provisions setting out the conditions for analysing this type of data. The most **critical point** was the **DSC requirement**. DSC refers to the need to screen the datasets to sort out personal data according to different categories, exhaustively listed in Annex II.A. and Annex II.B. to the Europol Regulation, before proceeding to the actual processing of the data for investigative purposes, including before cross-checking data to detect links or carrying out analyses of a strategic or thematic nature or operational analyses.[25] The relevant categories are linked to different types of involvement in criminal investigations, including (i) suspects, potential future offenders; as well as (ii) contacts, associates, victims, witnesses, and informants associated with criminal activities. Generally, Europol cannot process, nor even store, the personal data of individuals who do not fall under any of these categories.

---

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

22 Europol, EU SOCTA 2025, *passim*.

23 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.

24 EDPS, Opinion 7/2015, p. 7, available at 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)'.

25 See Article 18(2) ER.

Data providers, such as **Member States** or **EU bodies and agencies, typically** already perform the DSC before transferring the personal data to Europol.[26] Under EU law, they are all required to perform 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[27]. For large and complex datasets, manual pre-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. The DSC **for big data** is **not always possible,** given the sheer volume of the datasets, the way data is (un)structured, the lack of resources, or the excessive **manual effort required**. In practice, the only possibility is to first analyse the data in more depth from an operational point of view, or to detect links, also in a semi-automated way, by cross-checking available data.

Regulation (EU) 2022/991 clarified the conditions for DSC to provide **legal certainty** regarding the processing of large and complex datasets. Europol and the European Data Protection Supervisor (EDPS) had differing interpretations of the letter and spirit of the Europol Regulation regarding the applicable data retention period. According to Europol, that period should be three years; according to the EDPS, it should be six months.[28] New provisions were also necessary to provide **additional flexibility**, striking a proper balance between data protection and security aspects.

Article 18(5a) of the ER, in combination with Article 73 of the EUDPR, first clarified further the general principle of the DSC under Article 18(2) and Annex II. 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 at an aggregated level for all persons in a datafile to be processed, or part of it, (for example, by simply establishing that all persons mentioned are involved in a criminal activity falling under its mandate based on an examination of the general circumstances that generated the datafile) before personal data can be processed.

Article 18(6a) ER explicitly allows the processing of personal data received without DSC for **up to 18 months**, which can be extended for up to 36 months in justified cases, solely for the **purpose of completing the DSC**. Article 18(6a) ER does not explicitly refer to large and complex datasets but, more generally, requires a '**strict necessity**' test.

Article 18a ER provides a derogation by enabling Europol to process personal data received from a **competent authority,** the European Public Prosecutor's Office (**EPPO**) or **Eurojust**, where necessary to support an **ongoing criminal investigation**, without the need to perform DSC, if this has not already been carried out, and beyond the categories of data subjects 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 was designed to address the differences between the rules on

---

[26] Member States transfer data to Europol via its Secure Information Exchange Network Application (SIENA), where DSC is implemented as a mandatory field.

[27] See, for example, Article 6 of Directive (EU) 2016/680 (the 'Law Enforcement Directive' as regards indirectly competent authorities); OJ L 119, 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj; Article 51 of Council Regulation (EU) 2017/1939 (the 'EPPO Regulation'); OJ L 283, 31.10.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj; Article 27(3) of Regulation (EU) 2018/1727 (the 'Eurojust Regulation'); OJ L 295, 21.11.2018, p. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj.

[28] https://www.edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf.

DSC applicable to Europol and those applicable to the competent authorities, the EPPO, and Eurojust.

(4) Cooperation with third parties: Articles 26, 26a and 26b ER on the exchange of personal data between Europol and private parties

Criminals increasingly abuse the (cross-border) services of private parties – internet-based, financial and classical telecom services. 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 effectively in private hands, which makes it difficult to enforce rules online for law enforcement purposes as effectively as offline.[29]

Against this background, **cooperation between law enforcement authorities and private parties** has become **indispensable.** As set out in **ProtectEU**, the European Internal Security Strategy, it will be essential to reinforce partnerships with the private sector to facilitate the exchange of information.[30] Police Chiefs have also called, in their joint statement on the future of Europol[31], for Europol to serve as a '**vital gateway for obtaining information from private entities**'. The nature of this collaboration ranges from sharing information and providing commercial open-source data, to engaging in research and innovation projects and delivering services that support corporate functioning.[32] 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.[33]

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

In addition to the horizontal provisions of Article 26 ER, Articles 26a ER introduced rules for **online crisis situations** and Article 26b addressed the **dissemination of child sexual abuse material online**. In those cases, Europol may assist Member States by processing personal data received directly from private parties. Europol may also transmit personal data to private parties on a case-by-case basis.

Regulation (EU) 2022/991 introduced the possibility of using Europol's infrastructure for the exchange of information between competent authorities and private parties, as well as the

---

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

30 See ProtectEU: a European Internal Security Strategy, p. 6.

31 https://prezydencja.policja.pl/ppl/aktualnosci/260402,Wspolna-Deklaracja-Europejskich-Szefow-Policji-w-sprawie-przyszlosci-Europolu-Jo.html.

32 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.

33 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.

ability for Europol to request that Member States obtain, in accordance with their national laws, personal data from private parties.

These provisions were adopted in coherence with other initiatives, such as the Terrorist Content Online (TCO) Regulation[34] and the Digital Services Act (DSA)[35]. Further measures enhancing the involvement of private parties in the fight against crime and facilitating lawful access to data are envisaged to realise 'the ambition of a change of culture in security' (**whole-of-society approach**) under under the **ProtectEU**, the European Internal Security Strategy.[36]

(5) Internal and external oversight on Europol's compliance with fundamental rights

Regulation (EU) 2022/991 emphasises Europol's obligation to respect fundamental rights under the provisions defining Europol's tasks and enhanced related safeguards, notably by **strengthening the internal and external oversight of the Agency**.

In the area of data protection, the alignment of the Europol Regulation with the data protection safeguards under the EUDPR implied introducing new rules for the oversight by the **data protection officer** (DPO) and the **European Data Protection Supervisor** (EDPS). For example, the obligation to provide a data protection impact assessment (DPIA) and prior consultation with the EDPS have become systematic for any new type of processing. Regulation (EU) 2022/991 also introduced a new competence of Europol for access rights requests. Before, the national competent authorities were responsible to handle access rights requests if Member States were the data providers.

Regulation (EU) 2022/991 also established a **new position of fundamental rights officer** (FRO) at Europol, who is *inter alia* entrusted to inform Europol's executive director about possible violations of fundamental rights in the course of the Agency's activities.

Additionally, **democratic oversight and accountability** were **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, of the Treaty on the Functioning of the European Union (TFEU). Regulation (EU) 2022/991 strengthened the monitoring by the **Joint Parliamentary Scrutiny Group** (JPSG).[37] For example, it provided 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.

3. Main findings of the evaluation

3.1. State of play of the operational implementation of Europol's new personal data processing powers and tasks

Regulation (EU) 2022/991 entered **into force on 28 June 2022**. However, its operational implementation depended on various governance, technical, and administrative measures, as well as operational requirements, such as setting up new ICT structures in some cases.

Three years later, **nearly all the provisions** listed in Article 68(3) of Regulation (EU) 2022/991 **have become operational**. The provisions related to the analysis of large and complex datasets (Articles 18(6a) and 18a ER) and cooperation with private parties (Articles 26, 26a, and 26b

34 Regulation (EU) 2021/784; OJ L 172, 17.5.2021, p. 79, ELI: http://data.europa.eu/eli/reg/2021/784/oj.
35 Regulation (EU) 2022/2065; OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.
36 See ProtectEU: a European Internal Security Strategy, p. 2.
37 See https://www.europarl.europa.eu/relnatparl/en/eu-agencies-oversight/jpsg-on-europol.

ER) started applying as of 28 June 2022, or shortly after that. The processing of personal data for research and innovation projects (Article 18(2)(e) ER) started in 2023 after the sandbox environment, named ODIN, was set up to comply with the specific data protection requirements under Article 33a ER. By 29 June 2025, the possibility for Europol to propose **SIS information alerts** to Member States in accordance with Article 4(1)(t) ER had not yet become operational, as the technical implementation of the new type of alert is still ongoing. Entry into operation is **expected in 2026**.

3.2. Evaluation of the operational impact of Europol's new personal data processing powers and tasks on the Agency's objectives under Article 3 ER

As regards the operational impact of Europol's new personal data processing powers and tasks, the consultation indicated that **Member States maintain overall a favourable view** of their relevance, effectiveness, and added value, and Europol's support to their competent authorities in the related areas.[38]

The investigative powers covered by this evaluation are not used continuously or systematically to process data for monitoring purposes; some are even exceptional in nature, while others are used more regularly on a needs basis in investigations. The **operational use of the new provisions** over the reference period **differed significantly** in **quantitative terms,** depending on the different technical features and legal conditions associated with the new provisions.

Europol received a **non-negligible** number of **new contributions without DSC** from Member States under Article 18(6a) ER, amounting to 653 in 2023 and 597 in 2024. There was no short-term increase in contributions without DSC, and the number of cases where Article 18(6a) was applied remained **steady** compared to equivalent cases in the period before 28 June 2022. The new provisions had no negative impact on Member States' engagement in carrying out the DSC[39] either. Between 2023 and 2024, the share of contributions without DSC accounted for **less than 1% of all contributions** accepted by Europol from Member States (0.85% in 2023 and 0.71% in 2024). Since June 2022, Europol has consistently completed the DSC within 18 months, without utilising the extended 36-month time period. Europol and six Member States emphasised that, despite the improved legal certainty, the **administrative burden remained significant** for both Europol and the competent authorities due to the effort required to comply with the categorisation of personal data by individual involvement in the criminal offence. This requirement is implemented very strictly by Europol[40].

Europol reported that the exchange of information with **private parties** was still negligible in 2023, as only 26 cases of Article 26 ER implementation were recorded (in addition to the cases falling under the Digital Service Act).[41] However, in **2024**, statistics showed a **sharp increase to 284** (nearly +1 000%) cases involving cooperation with private parties under Article 26 ER. This was particularly the case for data from private companies to investigate **financial and economic crimes**. Europol also made significant use of Article 26b ER in the fight against Child Sexual Exploitation (CSE), where cooperation with private parties was already very substantial before. In both cases, the data also includes cooperation that was possible under the

---

38 See evidence presented under Section 5 of the staff work document accompanying this Report, and particularly Europol's submissions and the MS replies to Questions 2, 4 and 5 of the Short Questionnaire of 2 June 2025, in Annex III to the staff working document.

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

40 See Sub-Section 7.1.3. the staff work document accompanying this Report and MS replies to Question 9 of the Short Questionnaire of 2 June 2025, in Annex III to the staff working document.

41 Europol, 2023 Report pursuant to Article 16(11) ER.

previous legal framework. The available data do not disclose to what extent these new cases fall under the new provisions or an increased use of existing possibilities.

In **2025**, Europol adopted a **new strategy** to further enhance cooperation with private parties. In addition, measures have been taken to upgrade Europol's ICT infrastructure available to competent authorities for the exchange of information with private parties. In **2023**, Europol launched the *Plateforme Européenne de Retraits de Contenus Illégaux sur Internet* (**PERCI**) to facilitate the implementation of the TCO Regulation and, in the future, possibly also Article 18 DSA, as well as the *EU Child Abuse Referral Service* **(EU CARES)**. PERCI is not incorporated within the Europol Information System (EIS)[42].

Other provisions were **not utilised** at all (Article 26a ER), despite being operational, **or** were applied **only exceptionally** (one case where Article 18a ER was used in 2024 and one project realised with the processing of personal data under Article 18(1)(t) ER in 2025, with three new projects already in the pipeline).

Due to the limited period of operational implementation of the provisions introduced by Regulation (EU) 2022/991 and the lengthy nature of criminal investigations and judicial proceedings, Member States were unable to provide quantitative data on the impact of those provisions in operational terms. They offered instead some examples of successful investigations that demonstrate the **tangible benefits of the new investigative possibilities in real-life situations** for the provisions already in use, namely such as EncroChat, Sky ECC, Balkan-based criminal networks involved in cocaine trafficking or Lumma Stealer.

Europol and eight Member States also flagged a few **areas for improvement** to maximise the efficient and coherent use of the new legal framework and enhance Europol's role in the future. There are concerns, notably by Europol, that the excessive complexity, fragmentation, and length of the legal provisions may discourage practitioners or private parties from using the new available instruments. Member States' comments rather concern the manner in which Europol restrictively implements data protection safeguards under the oversight of the EDPS, which risks undermining the effectiveness and added value of certain provisions.

3.3. Assessment of the impact of Europol's new personal data processing powers and tasks on fundamental rights

The Commission did **not** find **any** evidence of **negative impact on fundamental rights** resulting from the operational use of the new powers for processing personal data from the limited use made so far of the new personal data processing powers.

In addition to implementing the specific data protection requirements associated with the new personal data processing powers, Europol has progressively taken all necessary measures to implement the new horizontal oversight mechanisms related to fundamental rights.

In 2024, Europol's Management Board adopted the revised DPO implementing rules as one of the last necessary implementing acts related to the new data protection regime. The evidence collected suggests that Europol and its Management Board have also ensured, in cooperation with Europol's DPO and the EDPS, a **rigorous implementation of the new data protection safeguards** introduced in 2022. That approach has prima facie effectively prevented any negative impact or interference from the initial use of the new personal date processing powers with individuals' rights to privacy and personal data protection. According to Member States, Europol currently has a **robust legal data protection framework** in place, which ensures sufficient safeguards for the potential increased use of its new powers. Seven Member States also stressed that this framework **facilitates the flow of information** by increasing trust,

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

although there is still scope for improvement. Only one Member States expressed a negative view.[43]

Besides the specific **challenges** related to the DSC, Europol and four Member States mentioned as areas for improvement the costs and time associated with the **Data Protection Impact Assessment** (DPIA) and **prior consultation of** the EDPS, which are in practice carried out by default. A further challenge raised by six Member States is the handling by Europol of **data subjects' access requests**, for which now it is competent even when a Member State is the data owner.

The **first Fundamental Rights Officer** was appointed in December **2022**. In the first two years of his mandate, he has **not** received nor presented **any complaints** to the executive director. The JPSG has continued to monitor Europol's activities closely and did not issue any recommendations since the new provisions took effect. The European Parliament set up the **JPSG Consultative Forum for Fundamental Rights** in February **2024**.

3.4. Cost-benefit analysis of Europol's new personal data processing powers and tasks

Given the early stage of implementation of the provisions introduced by Regulation (EU) 2022/991 and the limited experience with them, it is **premature** for the Commission to draw meaningful conclusions about the new provisions from a **cost-benefit analysis**.

The Commission services have collected information from Europol on the costs incurred to date in connection with the operational implementation of Regulation (EU) 2022/991, for the provisions under review. These costs totalled approximately **EUR 25 million** (about 5% of the total allocation to Europol[44]) between 2022 and 2025, primarily comprising one-off costs. Member States have not incurred any relevant new costs specifically linked to Regulation (EU) 2022/991 to date.

Most costs (almost EUR 17 million) were comprised of significant investments in the **development of new ICT structures,** implementing provisions on research and innovation (the sandbox ODIN), and for information systems to exchange personal data with private parties (PERCI and EU CARES). Costs for **human resources (HR)**, both related to ICT and operations, accounted for approximately one-third of the overall expenses (about EUR 8 million). HR will represent the **main recurring costs in the long run**.

It is worth noting that the EUR 8 million mentioned above do not include HR costs for the Information Management Unit (IMU) or the resources associated with (previous and new) oversight measures that have a horizontal character, and for which a disaggregation at the level of implementation of specific provisions is not possible. The costs for such resources are not negligible. For example, in 2023, **60 full-time equivalents (FTEs)** (nearly **5%** of Europol staff) were estimated to be involved in activities in **assurance/supervisory bodies and oversight/advisory entities**. Europol assigned 25 FTEs to efforts in responding to data protection supervision and corresponding assurance actions. This includes follow-up on the EDPS recommendations, as well as work generated in the context of prior consultations for operational data processing. Sixteen of these 25 FTEs are specifically engaged in activities related to EDPS requirements. As of June 2025, Europol has a dedicated team of eight full-time staff members in the field of data protection, including the DPO.

---

43 See MS replies to Question 9 of the Short Questionnaire of 2 June 2025, in Annex III to the accompanying staff working document.

44 In the same period of time the budget allocated to Europol amounted overall to approximatively **EUR 860 million** (increasing progressively from EUR 192 million in 2022 to EUR 241 million in 2025). For more details see the accompanying staff working document.

According to Europol and fifteen Member States, the **benefits** of the new personal data processing powers and tasks, in particular analysing large and complex datasets, as well as cooperating with private parties, are expected to be significant and **outweigh the associated costs**. No Member State was of different view. Some efficiency gains are reasonably expected in the long run, thanks to economies of scale effects and decreasing marginal costs. A Member State 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', which was also supported by two other Member States and other stakeholders.[45]

In the view of Europol and five Member States, possible implementation **inefficiencies** also need to be addressed within the **existing governance, administration, and data protection framework** to avoid undermining the operational impact of the new personal data processing tasks by delaying or restricting their use. Five Member States questioned a too cautious implementation of the data protection rules by Europol and its Management Board, under the guidance of the EDPS. They suggest that the flexibility granted by the co-legislators should be utilised adequately to maximise the effectiveness and efficiency of Europol's tasks and ensure their relevance and long-term profitability.

An evaluation of Europol's working methods and potential areas for simplification is outside the scope of the report under Article 68(3) ER and will be carried out within the framework of the evaluation under Article 68(1) ER.

4. Conclusions and way forwards

All in all, the preliminary main findings of the Commission are that Member States maintain **their support for the role played by Europol** in the key areas where it currently assists Member States with its **new personal data processing tasks**. However, to **maximise the benefits** of the new personal data processing powers, in the view of some stakeholders, there is a need to **address possible inefficiencies**, notably within the existing governance, administration, and data protection framework. It would be also useful to mitigate the **complexity and fragmentation** of the legal framework that may discourage practitioners from making use of the new possibilities.

Generally, the Commission did not find evidence that the new rules had a **negative impact on fundamental rights,** in particular thanks to robust data protection safeguards, which also facilitate the flow of information by increasing partners' trust. For some Member States, the Agency privileged a conservative approach, while **adequate use should be made of the flexibility granted by the co-legislators** as regards the Data Subject Categorisation, the data protection impact assessment, prior consultation with the Europol Data Protection Supervisor, the handling of access rights' requests.

Given the generally short implementation period of the new personal data protection rules provided for by Regulation (EU) 2022/991, the evidence collected are however not conclusive on all questions.

In its **ProtectEU**, the European Internal Security Strategy[46], the Commission announced that it will propose an ambitious overhaul of Europol's mandate to address escalating security

---

45 See evidence presented under Section 5 of the staff work document accompanying this Report, and particularly Europol's submissions and the MS replies to Questions 2, 4 and 5 of the Short Questionnaire of 2 June 2025, in Annex III to the staff working document and Joint Statement of European Police Chiefs on the Future of Europol.

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

challenges. In compliance with its Better Regulation Guidelines[47], 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**.[48] In July 2025, the Commission published the call for evidence[49] and contracted an external study to 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.

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

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

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