Executive summary

Introduction

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 52 of Regulation (EU) 2018/1725 (hereinafter referred to as 'Regulation 2018/1725')[1] responsible under Article 43 of Regulation (EU) 2016/794 (hereinafter referred to as 'the Europol Regulation' or 'ER' abbreviated) [2] for:

- Monitoring and ensuring the application of the provisions of the Europol Regulation, of Regulation 2018/1725 and of any other EU act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by Europol;
- Advising Europol and data subjects on all matters concerning the processing of personal data.

To these ends, the EDPS fulfils the duties provided for in Article 43(2) and exercises the powers granted in Article 43(4) of the Europol Regulation. Among his powers to investigate, the EDPS can carry out investigations in the form of data protection inspections. The power to inspect is one of the tools established to monitor and ensure compliance with Europol's legal framework.

The inspection at Europol was part of the EDPS annual audit plan for 2025. The formal Decision was communicated to Europol by means of an Announcement Letter dated 12 May 2025. The fieldwork was carried out on 2 and 3 July 2025 at Europol's premises, Eisenhowerlaan 73 2517 KK in The Hague, The Netherlands.

Scope of the inspection

The EDPS 2025 inspection focused on the following topics that were selected after assessing different criteria including the current developments at Europol and the risks to the data subjects' fundamental rights and freedoms originating from the processing operations selected.

[1] 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 repealing Regulation (EC) No 45/201 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.

[2] 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 as amended by 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, PE/8/2022/REV/1, OJ L 169, 27.6.2022, p. 1–42.

1. **Europol's use of the Schengen Information System (SIS)** in order to verify compliance with Regulation (EU) 2018/1862 (the SIS Regulation for law enforcement). This part of the inspection looked at how the agency is being informed of hits regarding terrorism-related alerts, as this requirement to copy Europol on SIS terrorism hits has already come up in the context of complaint investigations. The inspection also followed up on prior consultation opinions issued by the EDPS regarding Europol's alphanumeric and biometric searches of SIS. Finally, the inspection checked whether adequate logging was in place for SIS operations by using the common inspection plan for SIS logging developed by Member States and the EDPS jointly in the framework of the Coordinated Supervision Committee (CSC).[3]

2. The inspection verified whether **Europol's implementation of the [redacted] solution for facial recognition** is in line with the requirements of Article 30 ER regarding the processing of biometric data, including an assessment of the implementation of strict necessity and proportionality. The inspection assessed whether Europol has properly implemented controls for the risks associated with the use of this technology, including the risk of false positive matches and the potential for bias in the algorithm used, and whether the agency has implemented adequate safeguards to ensure the accuracy and reliability of the facial recognition system in accordance with the European Data Protection Board's Guidelines on the use of facial recognition technology in the area of law enforcement, and the EDPS's prior consultation opinion on Europol's Face Recognition Solution.

3. Regarding **transfers of personal data to third countries and international organisations,** the inspection verified whether Europol's implementation of the legal framework is in line with the specific requirements set out in Article 25 ER, which sets out the circumstances in presence of which each type of means for data transfers available to Europol should or may be used. The inspection also verified whether the data processing operations carried out in relation to the two notifications received by the EDPS in October 2024 with regard to Europol's exceptional transfers to third countries under Article 25(5) ER were in line with the legal framework. In addition, the EDPS checked exchanges with the Ecuadorian authorities in the context of the working arrangement establishing cooperative relations between the Ministry of Interior of the Republic of Ecuador and Europol.

4. The **exchange of personal data with private parties** is an area of increasing operational relevance for Europol. As new data exchange possibilities have been introduced by the latest ER amendments, the inspection verified the agency's compliance with the legal requirements and limitations set out under Articles 26, 26a,

[3] The Coordinated Supervision Committee (CSC) is a group of national supervisory authorities and the European Data Protection Supervisor (EDPS) to ensure coordinated supervision of large-scale IT systems and of EU bodies, offices and agencies, in accordance with Article 62 of Regulation (EU) 2018/1725 or with the EU legal act establishing the large scale IT system or the EU body, office or agency.

and 26b ER. The inspection scrutinised the workflows currently in place to receive and process data received from private parties, as well as to transmit or transfer information to the latter, and assessed whether Europol's guidelines for dealing with personal data exchanges with private companies are in line with the ER provisions governing operational cooperation with private sector.

Key findings of the inspection

1. **Use of the Schengen Information System and SIRENE by Europol**

The inspection revealed that the processes at the SIRENE office and for SIS searches are mature and do not raise significant concerns from a data protection perspective. However, self-monitoring processes are insufficient due to the lack of resources available for proactive monitoring of SIS operations. As a result, self-monitoring by Europol is largely reactive, a concern that will intensify once the information alerts, under Article 48 of the SIS Regulation, go live.

2. **[redacted], Europol's central facial recognition solution**

Regarding [redacted], the inspection team found that the peer review process conducted by trained facial reviewers and biometric experts did not raise any specific issue. However, Europol still has to migrate a sizeable number of facial images from [redacted], the old facial recognition solution, to [redacted]. At the time of the inspection, both systems were indeed used in parallel, which means that Europol was still generating operational leads using an older facial recognition model running on facial images that do not meet Europol's current quality requirements. The team also observed that, despite its recommendation to implement a matching threshold and/or a ranking cap to limit the number of likely candidates displayed after a search, [redacted] still always returns 50 candidates. The inspection team also noted that the logs generated by [redacted] did not keep track of the matching score nor of the order in which the likely candidates were presented to the user. Besides, the team noticed that the default configuration of [redacted] logging system only recorded the last 250.000 entries, rather than those from the last three years. Lastly, Europol could not demonstrate the trail of logs related to deletion of facial images in [redacted] after the data retention of the respective case had expired.

3. **Transfers of personal data to third countries and international organisations**

The inspection showed that Europol has in place policies and processes to implement the transfers' regime provided in Article 25 of the Europol Regulation. However, there are still some shortcomings that need to be addressed. Indicatively:

- The definition of *'transfer of personal data*' is too restrictive and does not include direct access to Europol's databases,

- The provision regarding transfers based on '*appropriate safeguards*' has never been used (Article 25(4a) ER was added in the latest amendment to facilitate transfers to third countries),
- There is lack of concrete guidance regarding:
    - the assessment of the circumstances surrounding data transfers under the new transfer mechanism provided in Article 25(4a) ER,
    - the balancing of individual rights with public interests,
    - the accountability obligations of Europol - in particular with regard to their obligation to inform the EDPS on transfers under the new mechanism of Article 25(4a) ER (how often, what should be included etc).

4. Exchanges of personal data with private parties

The inspection showed that as of July 2025, Europol's data-processing regimes under Articles 26, 26a, and 26b of the Europol Regulation are not yet fully implemented. Several issues have been identified, including:

- Lack of clear and updated guidance on using [redacted] to perform referrals to online service providers so that these exchanges of information are compliant with the Europol legal framework,
- Unclarity as regards the justification and necessity of special procedures to process personal data received from Hosting Service Providers pursuant to Article 14(5) TCO, and Article 18 DSA, and inconsistencies between the process description developed for such purpose, and the applicable rules established under the ER,
- Unclear retention periods for data processed under Article 26(2) ER, and inconsistencies in the application of the erasure obligation set out thereof,
- Insufficient documentation on mandate checks regarding CSAM data received from private parties, and inconsistencies in the verifications that apply to such data in the context of Europol's intake processes,
- Lack of exhaustive reporting to the Management Board on the personal data exchanged with private parties pursuant to Articles 26, 26a and 26b ER.

Recommendations and follow-up of the audit

As a result of the inspection activities and his findings, the EDPS has issued a set of 29 recommendations addressed to Europol. The main findings and recommendations are included at the end of each section of the report (with a full compiled list of recommendations inserted in Section 5). The recommendations contained in the report are issued in order to ensure compliance with the Europol Regulation and relevant provisions of Regulation 2018/1725.