04 February 2026

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

"Joint Parliamentary Scrutiny Group on Europol (JPSG) - 18th meeting"

Wojciech Wiewiórowski
European Data Protection Supervisor

Chair, Co-Chairs, Honourable Members of National Parliaments and of the European Parliament, Ladies and Gentlemen,

It is a pleasure to address the Joint Parliamentary Scrutiny Group once again, and I thank the Cypriot Presidency for hosting us here in Nicosia.

The JPSG is central to democratic accountability over Europol's activities, and the EDPS greatly values this opportunity for open and substantive exchange.

Today, I will focus on four points:

- our perspective on the Commission's Evaluation Report of December 2025
- the added value of DPIAs and prior consultations,
- the handling of complaints of individuals in the context of access requests
- the EDPS annual audits of Europol

Point 1 - Commission Evaluation Report

Let me start with the **Commission's Evaluation Report of December 2025, as it is an important milestone considering the upcoming review of the Europol Regulation**.

We carefully read the report. However, we regret that the EDPS was **not among the sources consulted**. The Commission missed the opportunity to use our in-depth knowledge as independent supervisor of Europol's operational data processing.

In today's intervention, I present **EDPS' evidence-based insights** to complement and reframe certain aspects of the Commission's evaluation report.

But first, I want to underscore one key message from this report: **data protection builds trust, and trust enables information sharing.**

Let me quote the report:

"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, although there is still scope for improvement. Only one Member State expressed a negative view."

This shows that not only the effectiveness of Europol's action, but also the very possibility to expand the agency's remit, intrinsically depend on compliance with key data protection guarantees. Respect for those guarantees is not optional. It is essential for police cooperation in the Area of Freedom, Security and Justice.

More work is needed to fully unlock Europol's data-processing powers; however, such progress must remain strictly in line with the applicable rules. And it is precisely in this context where independent supervision plays an essential role.

In this regard, let me now address some of the concerns raised by the Evaluation Report.

POINT 2 - PRIOR CONSULTATIONS AND DPIAS

The Report refers to the **costs and time of DPIAs and prior consultations**.

On this point, a clarification is necessary.

Prior consultations are **not carried out by default**. They are required only for processing operations that **Europol itself identifies as high-risk for data subjects**. National law enforcement authorities are subject to similar obligations under the Law Enforcement Directive.

The EDPS is bound by legal deadlines to provide his Opinions in response to Europol's prior consultation requests: the EDPS should issue its opinion within a maximum of ten weeks. **In no case the EDPS exceeded these deadlines**. Let me also remind you that where urgency is proven, special arrangements can apply to meet operational needs. Europol may exceptionally initiate processing even before the expiry of the legal deadline given to the EDPS to deliver his Opinion.

Far from slowing Europol down, EDPS Opinions provide **legal certainty, reduce litigation risk, and reinforce legitimacy**. For this reason, it is crucial that **adequate resources** are guaranteed for independent supervision and for Europol's implementation of safeguards.

A robust data protection framework is **not a hindrance** — it is an **enabler** of Europol's effectiveness in compliance with EU law.

Since the last JPSG meeting in November 2025, the EDPS has received **three additional prior consultation requests from Europol**. This number of prior consultations is steady since the entry into force of the 2022 review of Europol's mandate. It stems from the need by Europol to put in place the expanded mandate given by this latest review, such as the possibility for Europol to propose to Member States the creation information alerts on third-country nationals in the Schengen Information System.

This ongoing work reflects important realities:

- the continuous need for clear data protection guidance in a rapidly evolving operational environment;
- the relevance of the EDPS' expertise in supervising Europol's data processing;
- and the importance of constructive cooperation between Europol and the EDPS to ensure compliance in practice, not only on paper.

Let me share a real-world example of *ex ante* controls that builds trust through data protection: our Supervisory Opinion in response to Europol's prior consultation on the **Internet Facing Operational Environment - Quick Reaction Area**. This is a new cloud-based environment to retrieve and pre-process information, including personal data, obtained from online sources. It is designed to facilitate the large-scale triage of online data, allowing for the identification of information required for operational processing purposes.

Our Opinion identifies the measures required to prevent critical compliance issues:

- The first is ensuring that the IT solution in question does not become a full-fledged data processing environment, parallel to Europol's regular operational environment.
- The second consists of Europol remaining fully accountable and maintaining effective control over the data processing.

Point 3 - Data subjects' access requests and cooperation between supervisory authorities

The Evaluation Report also mentions concerns about **data subjects' access requests**, for which Europol can now be directly addressed, even when the data owner is a Member State.

On this point, we agree that roles and responsibilities between Europol and Member States could be clarified to better reflect operational reality.

In parallel, the EDPS has established **new ways of cooperating with national supervisory authorities** to ensure consistent handling of requests. This is another area where supervision evolves together with operational practice.

Point 4 - Annual inspections

Let me finally turn to our annual inspections of Europol.

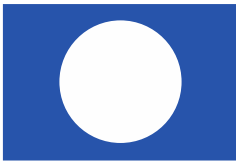
The **EDPS 2025 inspection report is about to be finalised**. It will include important findings on Europol's implementation of key provisions introduced by the **2022 Europol Regulation recast,** such as the enhanced **cooperation possibilities with private parties** and the reinforced regime for **transfers to third countries**. Both topics were key drivers of the latest reform.

The 2022 amendments expanded Europol's operational and data-processing possibilities, and considerable work is ongoing at Europol to enact them. In line with the inspection carried out in 2023, our latest inspection looked at how new Europol's processing powers are implemented in practice, what safeguards exist, and where gaps remain between legal potentials and operational reality.

In short, we verified whether Europol's actions to implement important innovations brought about the 2022 recast are carried out in a way that is **lawful, proportionate, accountable, and respectful of fundamental rights**. The findings of the inspection carried out in 2023 and 2025 will support Europol in ensuring that the 2022 recast Regulation delivers its intended added value while maintaining high standards of data protection.

Allow me a few words also regarding our earlier inspections carried out in 2017, 2018 and 2019.

In December last year, and after lengthy exchanges that lasted almost ten years, I decided **to close the respective cases**, based on the high rate of recommendations implemented by Europol - 90% in total. Still 15 out of 150 recommendations are outstanding. The 15 outstanding items concern issues of particular importance, such as appropriate security measures for the Computer Forensics Network, and their full and effective implementation now rests with Europol under its accountability obligations.



These examples show that meaningful results come from shared commitment and mutual understanding.

Our supervision is not abstract. It enables data-protection-compliant operational innovation to the benefit of law enforcement.

Conclusion

Let me conclude.

The EDPS does not seek to restrain Europol. We seek to ensure that its growing powers are exercised in a way that is **lawful, trusted and sustainable**.

Security and data protection are not opposites. They are mutually reinforcing. Without compliance, there is no trust. Without trust, there is no effective cooperation.

Thank you for the opportunity to share the EDPS perspective with the JPSG. We stand ready to continue our close cooperation with this Group, with Europol, and with national authorities.

Thank you for your attention.