EDPS

04 November 2025

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Joint Parliamentary Scrutiny Group on Europol (JPSG) - 17th meeting

Wojciech Wiewiórowski
European Data Protection Supervisor

Honourable Members of the Joint Parliamentary Scrutiny Group on Europol, esteemed national parliamentarians and Members of the European Parliament, chairman Zarzalejos, chairman Ujazdowski, chairman Frysztak, I am very grateful for this opportunity to intervene before the JPSG.

I will use my time today to share some key lessons learned from overseeing Europol during my time as the European Data Protection Supervisor. I will highlight the increasing relevance of the EDPS' work by sharing insights derived from direct supervisory practice.

The job of the EDPS is to make sure Europol's work respects EU data protection rules. To fulfil this sensitive mandate the EDPS has been entrusted with a specific set of supervisory powers.

I would like to present to you, through real examples and insights from supervisory practice, why our oversight work is more important than ever.

The technical knowledge and practical experience that my office and I have acquired in the supervision of Europol can help shape the future of data-driven policing in the EU, and ensure we have strong data protection for years to come.

Moving on to the key lessons learned mentioned earlier, I would like to emphasize how data protection supervision is crucial for implementing the new tasks entrusted to Europol, in full compliance with the applicable safeguards.

In recent years, you, the lawmakers, have given Europol significant new tasks. As EDPS, I closely monitored Europol's efforts in putting these powers to the test. I'm talking about their new ability to:

- Process large and complex sets of data.
- Proactively collect publicly available information, including from social media.
- Develop and use Artificial Intelligence tools for operational purposes.
- Cooperate directly with national police through joint analysis in criminal investigations.
- Exchange information in new ways with private companies.

These powers are designed to enhance Europol's operational capabilities and optimise means and resources. However, their implementation also has a significant impact on individuals' fundamental rights and freedoms, and raises serious questions about accountability.

My experience shows that Europol is well aware of these implications, and related compliance risks. It is clear that ensuring the correct application of data protection rules is also in the best interests of law enforcement itself.

Right now, Europol is working to put into practice some of the most innovative provisions included in the amended regulation. These ongoing efforts show the complex nature of the agency's current responsibilities. They also highlight the need to carefully oversee and assess the impact of Europol's data processing, and have adequate measures and mechanisms in place to respect people's rights to personal data protection.

Our supervisory practices also show that, to date, important data protection safeguards and related provisions in the amended Europol Regulation have yet to be implemented. I refer, most notably, to the need for Europol to make full use of the new rules and the conditions for processing data that Europol did not categorize and allocate to specific categories of data subjects within its databases (so-called non-DSC data) in support of criminal investigations.

Other relevant provisions now included in the Europol Regulation have not been used to the extent expected. A significant example is the processing of personal data for research and innovation purposes. In that regard, the EDPS was notified of only one research and innovation project involving the processing of personal data so far.

There is still work to be done to achieve the full implementation of the Europol legal framework, in line with the applicable data protection safeguards. This is where my office, the EDPS, plays a vital role.

One specific way in which the EDPS contributes to timely identifying, assessing, and addressing data protection risks is through prior consultations.

As we know, data protection by design is a proactive principle. As such, it requires an early assessment of the potential impact that Europol's new processing activities may have on data subjects' rights and freedoms.

Based on EDPS guidance, Europol developed a robust methodology and streamlined procedures, leading to significantly improved data protection impact assessments (DPIAs). The agency now relies on a consistent approach to verify whether a new processing operation is 'risky' from a privacy and data protection standpoint.

The rising number of "prior consultations" received from Europol shows that this approach is working, and confirms the need for thorough data protection scrutiny before sensitive processing operations begin. In the last 11 months, Europol has prior consulted the EDPS 8 times — double the number from the previous year. The supervisory opinions issued in response to such prior consultations and always within the legal deadline provided by the law allowed key data protection-related questions to be addressed, for instance, on how Europol:

- Collects and analyses cryptocurrency data to track cybercrime, money laundering and terrorist funding.
- Develops new AI tools to be deployed for investigative purposes.
- Collects open source information from private companies, and the internet in general.
- Queries specific EU databases (VIS, EES) with the use of biometric data.

Our work relies on specialised expertise, sound methodologies, and a pragmatic approach to supervision. This also means that the EDPS advice to Europol is not just delivered through a formal, written opinion. It is part of an ongoing dialogue, which involves regular staff-level exchanges with Europol representatives and the agency's Data Protection Function. This way of

working facilitates mutual understanding through the timely detection and discussion of relevant data protection questions.

A thorough data protection assessment of Europol's operations often also requires an understanding of how the agency's processing activities interplay with the ones carried out by national law enforcement authorities. In this respect, EDPS coordination and cooperation with national DPAs is also of utmost importance.

Audits are also another key tool through which the EDPS concretely fosters Europol's data protection compliance.

Virtually every year so far, my office has cooperated with experts from national DPAs to inspect specific areas of Europol's work that deserve special attention.

This past July, a team composed of EDPS staff and two national experts jointly audited Europol activities on several topics, including:

Their use of a facial recognition tool.
Their access to the Schengen Information System.
How they transfer data to third countries.
And the exchange of information with private companies.

The choice to focus on these topics reflects our effort to ensure complementarity between the EDPS advisory work, and verification of compliance. For example, my office had advised Europol on the new facial recognition tool before they started using it. The audit was a chance to go back and check if they actually followed that advice. In the case of international transfers and cooperation with private parties, the audit focused on the decisions, procedures and actions adopted by Europol to set in motion the operational novelties introduced by the 2022 reform. This practical approach helps my office to timely identify and address possible compliance issues, and prevent risks of infringements.

In addition to what has been mentioned so far, and turning to the second key lesson I would like to discuss, it is worth emphasizing that the EDPS' investigative and corrective powers are crucial for effective data protection enforcement.

The EDPS job is not just to give advice. When necessary, I must use my power to redress and correct wrongdoings. I can exercise these powers when compliance issues are found in relation to a specific processing operation, or through the investigation of complaints.

In this context, processing complaints lodged against Europol is a core part of the EDPS duties.

Individuals concerned by Europol's data processing have the right to seek redress from the EDPS. Data protection rights are subject to significant restrictions in the law enforcement domain. Our

role is to verify that such restrictions are lawful, and limited to what is necessary and proportionate.

Our case work shows that the investigation of complaints requires an in-depth scrutiny of how personal data are transmitted to Europol, as well as of the reasons for the processing with respect of specific individuals (the complainants). It also entails an examination of the roles and responsibilities of the different authorities involved in, or concerned by, the processing.

Often, Europol's decisions related to data subjects' rights, and the handling of individuals' requests thereof, are taken in consultation with the Member States, in particular those that transmitted the data. In such cases, the EDPS decisions on complaints require the involvement of DPAs responsible to supervise the concerned national authorities.

And for this reason, cooperation with national DPAs is increasingly crucial.

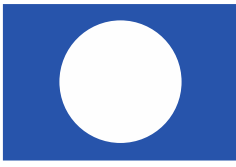
The EDPS has streamlined its procedures to ensure more rigorous investigations, including systematic onsite checks and close cooperation with national Data Protection Authorities (DPAs). A new working method was created jointly by EDPS and national supervisory authorities within the Coordinated Supervision Committee (CSC). This new method is designed to ensure the same high level of scrutiny, at both the European and national level, in the handling of complaints concerning data provided to Europol by Member States' police. Such cooperation is crucial for an adequate assessment of the lawfulness of data processing, as well as for the effective verification of necessity and proportionality of restrictions of data subject rights.

Looking ahead, the expansion of Europol's powers will make the work of EDPS ever more relevant.

The EU security strategy envisions a future where Europol will not only acquire an enhanced operational role (e.g. Operational Task Forces), but possibly also become a fully-fledged operational agency.

The experience from other growing EU agencies operating in the Area of Freedom, Security and Justice teaches us a clear lesson: strong oversight is essential to provide legal certainty, ensure compliance, and prevent accountability gaps.

As Europol's powers expand, the work of the EDPS, will become even more relevant. To keep up, my office needs the right tools and resources to do its job effectively. Ex-ante control of high-risk processing operations should remain the rule in the law enforcement context, as law enforcement activities constitute a quintessential expression of state authority and are characterised by a particular degree of opacity. Practice has shown that ex-ante control provides clear added value for individuals, as several high risks could otherwise go undetected without the EDPS's involvement at an early stage. By contrast, relying solely on ex-post control could prove more disruptive for law enforcement authorities, since unlawful processing operations would then need to be banned or substantially redesigned to achieve compliance with the data protection framework.



We also need to build a robust system of coordinated supervision. The EDPS ongoing work within the CSC underlines our commitment in establishing a consistent approach to cooperation with, and among, competent SAs.

In parallel, we are devoting significant efforts preparing for the AI Act as the Market Surveillance Authority (MSA) for AI systems developed or deployed by the Union institutions, agencies and bodies. Our preparations comprise three core pillars: governance, risk management, and supervision. In this context, we are building the foundation for effective supervision and cooperation based on mutual trust.

Thank you for your attention.