EDPS

24 February 2025

EUROPEAN
DATA
PROTECTION
SUPERVISOR

The EU's independent data protection authority

Joint Parliamentary Scrutiny Group (JPSG) on the European Union Agency for Law Enforcement Cooperation (Europol), Warsaw, Poland

Keynote speech by;

Wojciech Wiewiórowski
European Data Protection Supervisor

It is a great pleasure to be here today to provide you with an update on the by the European Data Protection Supervisor's work in its supervision of personal data processing by Europol.

I am especially honoured to be here in Warsaw in the Room where almost 15 years ago I was confirmed by the Senate of the Republic of Poland for the position of the Polish Data Protection Authority.

I remember this room very well for the lively parliamentary debates on Poland joining the Schengen Zone (including introduction of the SIS or rather SISOne4All) in 2008 when I was representing the Government and the Ministry of Interior and in 2011 when I acted as the Data Protection Authority during the discussion on the statute of September 16th, 2011 on the exchange of information with law enforcement authorities of the Member States of the European Union, non-EU/EEA countries, agencies of the European Union and international organisations.

These particularly relate to consultations on new forms of joint operational analysis between Europol and EU Member States, and continuous developments in the use of artificial intelligence for law enforcement purposes.

I also want to take this opportunity to underline some significant initiatives taken by Europol that, in my opinion, will demand the EDPS' attention in the next year.

I. Joint Operational Analysis between EU Member States and Europol

To start, I would like to recall that during the last group meeting I referred to the emergence of new joint operational processing environments. Today, I would like to bring to your attention the questions that these developments raise from a data protection's perspective.

Joint controllership in joint operational analysis: As you know, the possibility for Europol and EU Member States' authorities to carry out joint operational analysis is a key innovation introduced by the latest amendments to the Europol Regulation, and in particular Article 20(2a). This latter provision allows EU Member States to grant each other direct access to information they provide to Europol for the purpose of joint operational analysis, which in turn requires the development of new joint operational environments between national police and Europol.

As European Data Protection Supervisor, we previously stressed that the implementation of joint operational analysis, as envisioned by the current Europol Regulation, means that Europol and participating EU Member States have joint controllership over personal data processing. They are joint controllers because they jointly define the purpose and means of the joint operational analysis, and exert influence over the processing. Being joint controllers also means that they share the obligation to ensure compliance with the applicable data protection guarantees. Therefore, before starting joint operational analysis in the context of a criminal investigation, Europol and the EU Member States concerned need to clearly define, and agree on, their respective data protection responsibilities.

In October last year, I received a request for prior consultation by Europol on a new tool designed to give EU Member States direct access to datasets included in Europol's Analysis Projects, and these will be processed in so-called Joint Operational Analysis Cases (JOACs).

In my written Opinion on the request, I stressed again that Europol's proposed processing operations to implement the concept of joint operational analysis will qualify as a form of joint controllership. I understand that the implementation of this concept will be gradual, with the technical solution initially serving primarily as a tool for visualising data. However, this is already a significant step towards a truly collaborative processing environment.

In my Opinion, I also explicitly recommend that Europol and the competent authorities of the EU Member States participating in any future joint operational analysis case conclude an arrangement (in line with Article 86 Regulation 2018/1725). Such agreement is necessary to lay out the responsibilities of the joint controllers in terms of:

- information security;

- providing information to data subjects; and

- cooperating in replying to individuals' access requests, or to any other requests by data subjects to exercise their rights.

The move towards joint controllership in joint operational analysis also implies the need for enhanced coordination and cooperation between supervisory authorities. Here, I must highlight the crucial importance of coordination in the scrutiny of Europol, a principle that is also at the heart of your work as members of the joint parliamentary scrutiny group. Just as this group brings together national and European members of parliament to ensure effective political oversight and democratic accountability of Europol, the Coordinated Supervision Committee facilitates close cooperation among supervisory authorities to guarantee robust oversight of Europol's data processing operations. Since last year, the EDPS has the privilege of chairing this group. By working together, we can ensure the timely identification of potential risks or vulnerabilities and develop a new, more coordinated approach to Europol's supervision, ultimately strengthening the protection of fundamental rights in the context of law enforcement cooperation.

II. Artificial Intelligence, including machine learning

Moving on to the topic of machine learning and artificial intelligence (AI), I continue to receive consultations from Europol on AI matters, and I value our close collaboration on this matter. AI in law enforcement is not only addressed in the new AI Act, but it also includes a significant personal data processing component, that the EDPS scrutinises in its traditional role as a Data Protection Authority.

From this perspective, I would like to bring up a topic that I did not have the opportunity to discuss with you at the last group meeting, namely Europol's processing of biometric data, and in particular the use of facial recognition technology, which is a technology mostly based on AI technology. Facial recognition was one of the critical focus areas in my supervisory role over the last mandate. If not properly regulated and governed, such applications are prone to unduly interfere with fundamental rights – also beyond the right to protection of personal data. In fact, regulating facial recognition technology is a key priority for many data protection authorities, including the Information Commissioner of the United Kingdom, who has recently outlined a strategic approach to regulating AI.

For Europol, Article 30 of the Europol Regulation, governs the processing of special categories of personal data, which also includes all forms of biometric data when processed for uniquely identifying a natural person. It is important to recognise that each subcategory of biometric data—such as fingerprints, facial recognition—comes with its own set of risks and considerations.

The processing of biometric data is permissible only under **strict conditions of necessity** and **proportionality**. I have dedicated significant effort over the last mandate to providing guidance on this notion of "strict necessity and proportionality" in the context of Article 30, for instance in response to prior consultations submitted by Europol on facial recognition technology. In the EDPS' Supervisory Opinions, I applied the criteria developed by the Court of Justice in its recent case law, which clarifies that the notion of "strict necessity" should be understood as requiring: first, that the need to processing this personal data is an 'absolute' one, which must be assessed with particular rigour; and second, to verify if this data can be further minimised as it is being processed. This specifically includes ensuring that personal data is: a) adequate, b) relevant, and c) limited to what is necessary for the purposes for which it is processed.

In light of the above, I have carefully avoided granting any blanket greenlight to the law enforcement use of 'biometrics' as a whole. Even when focusing on a particular type of biometric data, such as facial recognition, we must examine the specific context and sphere of application. Therefore, assessments should be conducted on a case-by-case basis, ensuring that the use of biometric data is justified, necessary, and proportionate in each concrete scenario where it is proposed. This approach allows for a more precise application of data protection principles and better protection of individuals' rights.

One area that I have closely examined is the use of facial recognition technology in cases connecting different sources of child sexual abuse material. In these instances, I believe there is a use case that would pass the necessity test. I therefore focused on verifying that the technology is reliable and fair and does not exhibit biases that could lead to misidentification or unequal treatment.

This also links back to the topic of AI use in law enforcement, more broadly. Facial recognition, like any other AI tool, can only give you the most statistically likely result, that is, the model's best-educated guess. As a statistical tool, AI can be relevant to generate leads (for instance by trying to ascertain how much nude skin is in a certain image), but as a probabilistic tool that is prone to errors, we must be careful to deploy it in situations where we can assure that it is fundamentally fair, and that we keep clear those data that are generated as a 'machine' hint, from those for which we know they are accurate.

III. Looking ahead: Strategic Priorities

Now looking ahead, the EDPS has identified a number of strategic priorities that will inform its supervisory work regarding Europol in the short and medium term.

1st Priority - Research and innovation: the EDPS will continue to play an important role in empowering Europol's data scientists to push the boundaries of innovation while ensuring that their work is built on a solid foundation of data protection. By providing guidance and closely monitoring the implementation of Article 33a of the Europol Regulation, the EDPS can support Europol in its efforts to incorporate safeguards required to guarantee the responsible processing of personal data for research and innovation projects, including those that make use of AI.

2nd Priority - International cooperation: Investigation of cross-border crime, terrorism, and cyber-related offences often relies on information sharing with authorities of non-EU/EEA countries. There are a number of legal instruments that Europol may use for such purposes. According to Article 25 of the Europol Regulation, these include adequacy decisions, international agreements and other legally binding instruments, as well as a set of additional 'transfer tools', including appropriate safeguards and the use of so-called derogations from the general data transfer regime. As we see again that more use is made of these derogations, Europol’s international transfers of data will be a key area of focus of our supervisory activities, with specific focus on the additional ‘transfer tools’ available under Article 25.

3rd Priority - Cooperation with private parties: I will closely supervise personal data flows between Europol and private parties. I am fully aware that criminal investigations increasingly rely on law enforcement authorities’ cooperation with private parties and that the latest amendments of the Europol Regulation enable various forms of public-private cooperation. The agency can now directly receive personal data from private entities, but also proactively share information with them. Yet, recognising the sensitive nature of these activities, the legislator subjected the possibility for Europol to exchange data with private parties to clear limitations, and stringent necessity and proportionality requirements.

As Europol prepares its new strategy to streamline cooperation in the context of public-private partnerships, it is high time for the EDPS to verify the correct application of the relevant legal framework. Last month, the EDPS had an operational meeting with the agency to discuss ongoing developments in this area. The discussions have been constructive and very informative, giving us the opportunity to identify matters of concern that we believe deserve further scrutiny. In particular, I will focus on the implementation of the provisions under Europol Regulation that enable direct exchanges of personal data with the private sector (Articles 26, 26a, and 26b ER). The interplay between the provisions of the Europol Regulation enabling private-public data exchanges, and other tools at the agency's disposal, to receive or collect personal data from the internet also requires close examination.

IV. Conclusion and Thanks

To conclude, I would like to emphasise that the office of the EDPS is committed to ensuring that Europol's processing of personal data is carried out in a manner that respects the fundamental rights of individuals, while also supporting the agency's efforts to combat serious and organised crime. My supervisory work is focused on providing guidance and oversight to ensure that Europol's use of new technologies, such as artificial intelligence and biometric data, remains in line with the data protection framework.

I would like to thank you, members of the Joint Parliamentary Scrutiny Group on Europol, for your attention to these important issues. Your scrutiny and oversight are essential in ensuring that Europol's activities are transparent, accountable, and respectful of fundamental rights. I appreciate the opportunity to have discussed these matters with you today and look forward to continuing our cooperation in the future. Thank you.