



12 November 2024

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Europol Joint Parliamentary Scrutiny Group - 15th meeting

Speech by;

Wojciech Wiewiórowski European Data Protection Supervisor

I. Introduction

Honourable Members of the Joint Parliamentary Scrutiny Group on Europol, esteemed national parliamentarians, and Members of the European Parliament, it is a privilege to address you today. Your role in overseeing Europol is crucial to ensuring that the Agency operates within the legal frameworks established by the European Union while respecting the fundamental rights of our citizens.

The purpose of this address is to highlight how the European Data Protection Supervisor (EDPS) – fulfilling its supervisory tasks – complements and supports the work of the Joint Parliamentary Scrutiny Group (JPSG).

As you know very well – the EDPS is the independent supervisory authority tasked with the responsibility to oversee personal data processing at EU institutions bodies and agencies – including Europol - and to control its compliance with EU data protection law. We discharge this supervisory function through the set of powers and means that Union legislator entrusted to us. One of our duties is to report to the JPSG on issues relating to the protection of fundamental rights and freedoms of natural persons, and in particular the protection of personal data, with regard to Europol's activities. The knowledge that the EDPS derives from the oversight of Europol's personal data processing is a key resource at your disposal to better enforce democratic scrutiny and ensure accountability of the agency. Our experience in cooperating with national data protection authorities, for instance in the context of the Coordinated Supervision Committee (CSC), also adds value to Europol's oversight framework.

The EDPS full supervision of Europol started on 1 May 2017. In our role, we progressively consolidated close working relations with the agency, which we supervise with impartiality, integrity, transparency, and pragmatism: the values that guide the EDPS in the exercise of all its supervisory functions. Along the years, we supported Europol in the enforcement of the legal safeguards that apply to their core business, which is the processing of operational personal data to support the Member States in preventing and combating organised and serious crime, as well as terrorism.

The EDPS' first hand understanding of Europol working methods and data processing environments enables the embedding of data protection guarantees in law enforcement practices. Indeed, Europol regularly seeks our expert advice on all matters concerning the processing of personal data. The relevance of EDPS supervisory activities vis-a-vis Europol is well reflected by the findings of our most recent inspection report, which focuses on the processing of PNR data, on the access to VIS data as well as on the data protection challenges raised by the processing of large data sets.

Changes in the regulatory framework governing Europol's operations, and the expansion of the agency's tasks and responsibilities call for ever-closer scrutiny and cooperation with the EDPS. We stand ready to assess how the new data processing powers entrusted to Europol can affect data subjects' rights, and to provide recommendations that Europol, in its role of controller, will have to implement to ensure compliance with data protection rules. This role was supplemented by the European legislator this year with the set of supervisory tasks derived for the

Artificial Intelligence Act which are however of slightly different nature and place us rather in the role of market surveillance authority not affecting the classic data protection authority role.

I am here also to discuss with you some of the focus areas of the EDPS supervision of Europol in the last year that I expect to remain in the EDPS focus in the upcoming years. These areas include:

- handling of large datasets,
- use of joint operational environments between national police and Europol, and
- use of biometrics and AI tools.

I want to go more deeply into these topics with you to showcase why they deserve special attention in the EDPS' work, and how we strategically approach our supervision in their regard. Let's start with few topics connected with handling of large datasets and the separation of bulk data from specific data

II. Framework of Data Handling in the Europol Regulation

The basic idea of the Europol Regulation was that Europol should be processing data on specific individuals who were clearly identified and categorized. This included:

- suspects,
- victims,
- witnesses, and
- other defined roles within criminal investigations.

The basic premise is that persons should be known and labelled according to their role, to be able to apply corresponding the legal restrictions that the law provides. Through categorisation, the aim was to allow for targeted data processing, and avoid unnecessary intrusion into individuals' privacy. Effectively, this is an implementation of the principles of data minimisation and purpose limitation for law enforcement. It is a way to balance privacy and security, to empower police to exchange information with Europol, while putting limits on what acceptable use is.

This resulted, as you know, in Annex 2 of the Europol Regulation, which explicitly details the categories of persons on whom information can be processed. It specifies not only who could be included but also the types of data permissible for each category. Data collection on suspects for instance is more permissible than data on witnesses. The system was designed to maintain a strong grasp on what data was being processed, to impose a degree of data management, and served as safeguards against over collection of data.

I want to give another practical example of how this original idea of close data management is supposed to play out. Under the Europol Regulation, Europol is obliged to report to the EDPS on the processing of personal data, especially concerning sensitive categories. This includes data revealing political opinions, religious beliefs, sexual orientation, and other protected characteristics. For Europol to report meaningfully on such sensitive data, it must have in some way a more detailed knowledge of its datasets. This entails not just storing data but understanding its content, or the origin, and the context in which it was collected.

As we have argued before in our order of 3 January 2022, without knowing the exact contents of its large datasets, Europol may process data beyond its legal mandate or fail to report on sensitive data as required, posing compliance risks.

In today's digital age, it is only natural that Europol increasingly encounters large and complex datasets. These bulk data collections often come from diverse sources and may include vast amounts of personal information, some of which may be sensitive. Analysing and categorizing every piece of data within these large datasets is a monumental task. Sensitive information like political opinions may be deeply embedded, making it challenging to identify without extensive processing. Combing through these datasets can take years. During this time, fulfilling reporting obligations as they are required by the Europol regulation becomes practically difficult if not impossible, leading to potential over retention of data, but also to weaker oversight as no one is fully aware of what is embedded in the datasets.

Recognising these challenges, the EU legislator wisely established an exceptional regime within the Europol Regulation—specifically Articles 18a and 18(6a). This regime allows Europol to process large datasets that cannot comply with the standard data processing requirements due to their volume and complexity. The exceptional regime includes specific conditions and safeguards to prevent misuse, such as stricter oversight, limited retention periods, and clear purposes for data processing. In substance, it provides a legal framework for handling bulk data while ensuring protection of fundamental rights. It is therefore crucial that Europol make full use of these provisions when dealing with large datasets.

It is essential that Europol does not mix large, undefined datasets with the regular processing framework designed for categorised data. When the composition of datasets is unknown, applying the regular framework becomes problematic as it could lead to non-compliance with data protection standards. This is where Europol must switch to Article 18(6a) and Article 18a. As EDPS, I have focused a lot of my attention to ensuring that Europol distinguishes between data processed under the normal regime and that under the exceptional regime. This distinction is also vital for effective supervision and protection of individuals' rights. By maintaining separate frameworks, and ensure the correct categorisation of data subjects and data types, we uphold the integrity of Europol's operations and reinforce public trust in our collective commitment to data protection.

III. Joint Operational Environments

As another critical focus area in our supervisory role, I would like to address the emerging concept of joint operational environments in law enforcement on which I have already issued guidance to Europol. Traditionally, law enforcement agencies have operated within separate systems, communicating and sharing information through effectively the equivalent of exchanging emails to transfer case information from one system to another. I can understand the growing desire among law enforcement agencies to move beyond this paradigm and to collaborate more effectively by jointly processing personal data in shared operational environments.

Recognising the need for enhanced collaboration, the EU co-legislators have taken steps to enable joint operational environments through the new Article 20(2a) of the Europol Regulation. This provision allows Europol and national law enforcement authorities to jointly process personal data, facilitating closer cooperation in operational activities.

Before embarking on joint processing, we need to define the respective data protection responsibilities of all parties involved. In the joint operational environments of the future, Europol and national authorities will most probably process personal data as joint controllers, since they would be jointly agreeing on the exact data to be processed in the joint environment, the purpose of such processing and its duration.

This joint controllership scheme would mean that a clear allocation of the respective responsibilities of the involved parties for compliance with data protection rules, including the Law Enforcement Directive and the Europol Regulation, should take place. A respective agreement would include provisions, in between others, regarding the responsible party for applying data security measures, handling of data subject rights, and defining procedures for data breaches.

All these elements are important to maintain the trust of the citizens in the data governance of these environments. Defining them in a clear way is necessary to ensure accountability, transparency, and compliance with the Europol Regulation and national laws implementing the law enforcement directive.

Aside from cooperation between the law enforcement authorities, we also need to step up our coordination between national data protection authorities and the EDPS as we move towards the implementation of these new joint operational environments. Coordinated supervision between the EDPS and national Data Protection Authorities will be essential, including via the Coordinated Supervision Committee to ensure consistent views and supervisory actions between data protection authorities on matters related to Europol.

IV. Biometrics

Another critical focus area in our supervisory role over the last mandate has been Europol processing of biometric data, and in particular the use of facial recognition technology, which entails large scale processing of biometric data to authenticate or to identify a person. Law enforcement have a clear interest in the collection and processing of biometric data, including through the deployment of facial recognition technologies. However, if not properly regulated and governed, such applications are also prone to interfere with fundamental rights – also beyond the right to protection of personal data – and are able to affect our social and democratic political stability.

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 recognize that each subcategory of biometric data—such as fingerprints, facial recognition—comes with its own set of risks and considerations.

The processing of such 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 my supervisory opinions, I highlighted the recent case law of the Court of Justice, which stresses that the requirement of 'strict necessity' should be interpreted as

- (1) establishing strengthened conditions for lawful processing of sensitive data,
- (2) requiring a particularly rigorous assessment of its necessity, and
- (3) requiring a particularly strict checking as to whether the principle of data minimisation is observed.

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, our assessments are 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 we have closely examined is the use of facial recognition technology in cases involving connecting different series of child sexual abuse material. In these instances, we believe there is a use case that would pass the necessity test. We 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 to the topic of AI more broadly in law enforcement, as facial recognition, like any other AI tool, can only give you the most statistically likely result, that is, the model's besteducated 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, thus 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.

V. Way forward

I urge you to support measures that uphold robust data protection standards, even as we adapt to new technological realities. I believe this includes:

- endorsing the continuous separation of big data sets from data where the Data Subject Categorisation is concluded,
- to ensure that where police are cooperating ever-more closely, there are strong oversight measures in place so that all actors are kept accountable for their actions in joint environments, and
- to keep clearly separate AI-supported guesses on closest matches and use those only as leads.

At the EDPS, we are more than willing to discuss practical solutions that allow Europol to fulfil its mission without compromising the principles of data protection and privacy that are foundational to the European Union. Ongoing dialogue between the EDPS, Europol, and the European and national Parliaments is essential. Through this venue, we have the opportunity to align our viewpoints and to move forward with renewed clarity on the issues that will be in the focus the next few years.

Finally, I must mention that the increasing complexity and scale of data processing operations at Europol, for instance the advent of joint operational environments, do not only place resource requirements on Europol, but also on the EDPS. With the increases in data processing across the justice and home affairs area, notably also in interoperability, the EDPS must maintain its capacity to perform thorough assessments, audits, and provide timely guidance. Adequate resources will enable us to keep pace with technological advancements, understand new methodologies employed by law enforcement, and address emerging data protection challenges effectively.

I call upon you, esteemed members of the Joint Parliamentary Scrutiny Group, to support adequate budgetary allocations for the EDPS, and for your national data protection authorities, in your respective capacities. Investing in data protection supervision and enforcement is an investment in the integrity and credibility of the EU's data protection framework. The rules are there, and they have to be enforced. Thank you for your attention and for your unwavering dedication to protecting the privacy and data rights of our citizens. Together, we can ensure that we use law enforcement data in a way, which is clear, responsible, and in full respect of the values, we all share.

			684
		500	
ECH.			
C/V			