19 February 2024

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

"14th meeting of the Joint Parliamentary Scrutiny Group on Europol"

Wojciech Wiewiórowski
European Data Protection Supervisor

During the last 5 months, my supervisory activities regarding Europol were focused:

- on the processing of biometric data, including facial recognition;
- on new working methods including on the way EU/EEA Member States' law enforcement authorities can access Europol's systems and carry out operational analysis jointly and reciprocally with Europol; and
- on inspection activities.

I would like to focus my address today on these hree main topics.

Firstly, on the processing of biometric data. We have observed these last six months the preparations for a **new expansion** of the processing of **biometric data**, by paving the way for an increased use of facial recognition tools. In this regard, we have advised Europol on the update of the portfolio of Analysis Projects that streamline the processing of biometric data and on the use of its updated Face Recognition Solution. As part of our role as the advisor of the EU legislator, we have also issued a legislative opinion on the recent Proposal for a Regulation on enhancing police cooperation in relation to the prevention, detection and investigation of migrant smuggling and trafficking in human beings, which I invite you all to read.

This trend is also observed in other legislative initiatives and affects not only the work of Europol but the work of national law enforcement authorities as well. For instance, the Prüm II Proposal, which lays down the conditions and procedures for the automated searching of DNA profiles and facial images in the national databases of the Member States and of Europol raise several fundamental rights and data protection concerns.

In light of this anticipated increase in the processing of biometric data, in my legislative Opinions I underlined the main legal requirements to which the co-legislators and Europol should adhere to when providing for / or processing biometric data.

First of all, EU law (regulation on data protection for EU institutions, agencies and bodies) considers processing biometric data for the purpose of uniquely identifying a natural person as a special category of personal data. Additionally, there are specific conditions laid down in Article 30(2) of Europol Regulation. In particular, processing of biometric data is allowed 'only **where strictly necessary and proportionate** for the purposes of research and innovation projects [...] and for operational purposes, within Europol's objectives, and only for preventing or combating crime that falls within Europol's objectives'. In my legislative 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) a **particularly strict checking** as to whether the **principle of data minimisation is observed**.
Another important issue that has to be tackled when processing biometric data, is what control measures would be applied as regards the quality of these data. While the EDPS understands that data from crime scenes or similar settings cannot always be of high quality, there needs to be a minimum quality standard, especially when artificial intelligence tools are being used.

In light of the above, when assessing Europol's Face Recognition Solution I have requested that the Agency:

- specifies the categories of individuals for whom facial recognition will be used for operational analysis;
- implements a 'pilot' approach in handling facial images, which will allow for an evidence-driven decision-making,
- provides further evidence on the accuracy of the algorithm **on minors under 12**, before subjecting these minors to the facial recognition system.

Secondly, I would like to focus on today concerns the new working methods between Europol and national authorities. Here, I would like to inform you of another general trend identified in recent years where Europol and national law enforcement authorities conduct jointly operational analysis by allowing access to each other's systems and tools.

Examples of this approach are:

- Europol's access to national IT environments for specific investigations;
- The Joint Operational Analysis Concept, which enables Member States to allow other Member States to directly access the information they provide to Europol for the purpose of conducting joint operational analysis;
- Most recently, the setting up of operational task forces and Europol deployment for operational support in relation to investigation of migrant smuggling and trafficking in human beings.

All these new working methods might have possible implications in terms of allocating the data protection responsibilities between Europol and national law enforcement authorities, and can pose new challenges for their supervision that we will try to tackle by cooperating more closely with our fellow national DPAs. This new trend, in my view, requires as well the close cooperation of other bodies exercising scrutiny, like national Parliaments (hence our meeting today) so that an

effective supervision can be ensured. I am analysing the possible effects of such working methods in the pending investigation regarding Europol's access to national and international information systems, which I launched pursuant to the findings of one of the previous Europol inspections.

Thirdly, on 2 and 3 October 2023 my office carried out Europol's annual inspection in the Hague, focusing on

- Europol's processing of Passenger Name Record ('PNR') data;
- Europol's access to Visa Information System;
- Data Subject Categorisation, and
- The implementation of the technical controls and safeguards under Europol's Action Plan in response to the EDPS admonishment over the processing of large datasets.

We are currently at the stage of drafting our inspection report and we will inform you on our findings and recommendations at the next instance of the JPSG.

Lastly, I would like to refer to our continuous cooperation with Europol, both at staff and management level, by holding biannual meetings with the Deputy Executive Director of Governance, where we aim at discussing all pending issues, and which is indispensable for ensuring that appropriate data protection at Europol.