Europol Joint Parliamentary Scrutiny Group - 5th meeting - 23/9/2019

Wojciech WIEWIOROWSKI

Speaking points[1]

I. INTRODUCTION

EDPS

- In the EU, **independent** data protection **supervision** is an essential part of the right to the protection of personal data under Article 8 CFR, as well as Article 16 TFEU.

- The **EDPS** is in charge of **supervising EU institutions** when dealing with data processing, including for the purpose of law enforcement.

- The EDPS took over responsibility for supervising the processing of personal data for operational activities of Europol on **1 May 2017** (= entry into application of the when the Europol Regulation - ER).

- Since then, the EDPS has been developing a sound and effective supervision scheme thanks to continuous **cooperation** with Europol and **close monitoring** of their operational activities.

EDPS, DPAs AND ECB

- While it is EDPS responsibility to supervise the processing of personal data by Europol, **national DPA** are responsible for overseeing the processing of personal data by their respective national law enforcement authorities (LEAs).

[1] This is a copy of the Assistant Supervisor's speaking notes, used for the purposes of the JPSG meeting. These notes are not a *verbatim* record of the Assistant Supervisor's presentation during the meeting.

- As **most data processed by Europol originate from Member States** (MS), Europol's supervision requires close cooperation with the relevant supervisory authorities in the MS.

- For this reason, establishment of a Cooperation Board (ECB) made of representatives from national DPAs and the EDPS. ECB is an **advisory body** on matters involving the processing of personal data by Europol, which originate in the MS.

- EDPS provides the **secretariat** for ECB, which meets at least twice a year.

II. EDPS ROLE AS SUPERVISOR OF EUROPOL

- **Challenges** of supervision of data processing activities **in the field of law enforcement** (LE):

    - Domain where **data subjects' rights are restricted**, justifying derogative regimes.

    - **Impact** of such data processing activities on individuals' rights and freedom is high:
        - Risks of being wrongly suspected, of being discriminated, of being denied asylum, etc.).
        - Many of data subjects concerned are vulnerable groups of people (minors, migrants, refugees, missing persons, but also suspects).

    - Data processing activities in LE are **opaque** to individuals. Difficult for data subjects to know who is processing their data and for what purposes.

    - Supervision of Europol's data processing activities is made more difficult by the fact that Europol **IT systems are complex** and process a **large volume of personal data**.

- **Specific role of the EDPS** in this context: ensuring that data subjects' rights are effectively protected, as individuals do not have the power to exercise this control to the same extent as in other areas.

III. EDPS SUPERVISORY ACTIVITIES - MAIN ACTIVITIES SINCE PREVIOUS JPSG MEETING

- Since taking on supervision in 2017, the EDPS has put in place a structured system of supervision designed to
  - encourage **cooperation** and ensure accountability and to
  - use our **supervisory tools** in the most appropriate way.

COOPERATION

- Close collaboration with Europol's Data Protection Function (DPF) team and operational staff, notably through **bi-monthly meetings**. Goal: anticipate consultations and other issues on data processing and define/plan for future activities, such as inspections or inquiries.

SUPERVISORY ACTIVITIES

Information: Europol has to inform the EDPS in certain cases. The information so collected creates the opportunity for EDPS to initiate activities aimed to improve the level of data protection and the efficiency of operational activities of Europol.

Examples:

- **Operational analysis projects**

  Europol can process PD to support criminal investigations and criminal intelligence operations carried out by LEAs in the MS, only so as part of *operational analysis projects* (OAP). Each OAP focuses on a specific crime area, such as child pornography, cybercrime, drug trafficking, organised criminal groups, property crimes or terrorism.

Europol has to inform the EDPS each time they open/modify/close an OAP.

- **PD breach**
  Obligation to inform EDPS without undue delay. Plus obligation to make an assessment of the level of the negative effect of the data breach to the rights and freedoms of the individuals and inform them in case this is high.

- **Transfer of data to 3rd countries with neither adequacy, nor operational agreement for the exchange of PD**
  Allowed in exceptional circumstances, for example to support investigations in the aftermath of a terrorist attack or to prevent an immediate and serious threat to public security. Europol must inform the EDPS when making use of these derogations

General consultations

Advice on all matters concerning the processing of personal data at Europol, in the form of Opinions.

Three examples from the past six months

- Consultation on **Europol's model working arrangement** with 3rd countries in order to clarify the provisions applying to the exchange of non-personal data and the ones applying to the exchange of personal data, in case Europol would have to use one of the derogations allowed by the Europol Regulation (under Art. 25).

- Since the end of March 2019, the EDPS has been in contact with Europol in order to **prepare for a "no-deal Brexit**", i.e. for the case where the UK would leave the EU without a withdrawal agreement that would cover personal data exchanges between Europol and UK LEAs.

- **FIU.net**

  FIUs (financial intelligence units) are in charge of establishing links between suspicious financial transactions and underlying criminal activities in order to prevent and to combat money laundering. FIUs exchange information through FIU.net.

  July 2018: EDPS Opinion on the **embedment of FIU.net into SIENA**.

  Compliance issue: under the Europol Regulation, **categories of data subjects** about whom data are exchanged through the network by FIUs, as these cannot include data about persons who are not "suspects". No definition in the Europol Regulation or at European level of when a person becomes a "suspect". The Europol Regulation refers to national law.

  The EDPS decided to **refer the matter to the Europol Cooperation Board** (ECB), as it is up to each national supervisory authority to make this interpretation.

  ECB Chair to explain in his intervention the position recently taken by the Board on the issue.

  The case of FIU.net is a clear **example of the need for close cooperation** between the EDPS and national DPAs.

Prior consultations

Whenever Europol plans a new data processing activity involving the processing of sensitive data or the possibility of significant risk to an individual, they must notify the EDPS providing a DPIA.

So far, EDPS issued six prior consultations.

Latest opinion (13/9/19) on modalities of access by Europol to **PNR** data in accordance with PNR Directive.

Inquiries

Own initiative inquiries on issues that come to our knowledge in the course of our other supervisory activities.

Four inquiries launched so far in 2019.

Complaints

Complaints from individuals relating to the processing of their personal data by Europol.

Since May 2017: only two admissible complaints.

Inspections

- Cornerstone of EDPS supervisory activities

- Audit in depth selected **legal and technical** aspects of data processing

- **Three general inspections** (once a year) since May 2017, last one in June

Scope of the June inspection includes:

- Focus on the processing of data in the areas of terrorist financing, fight against money laundering and illegal activities on the dark web.
- Use by Europol of derogations in order to transfer personal data to third countries.
- New practice by MS to send larger volume of data to Europol. This new trend results from the larger amount of personal data available to law enforcement authorities at national level in the context of criminal investigations and criminal intelligence operations.
- Europol's encryption methodologies
- check implementation of recommendations from previous inspection reports

We invite **experts from national DPAs** to participate in inspections:

- This helps tackle issues found at Europol level but with origin at national level. Ex: problems with data quality or insufficient justification for the processing of sensitive data or data on minors.

- Back home, experts can consider how to tackle these problems in their own supervisory activities.

Following on-site activities, recommendations for improvement outlined in an **inspection report** sent to ED of Europol and shared with ECB.

Close **follow up** of implementation.

- **Targeted inspection** on a specific aspect of the Terrorist Finance Tracking Programme (TFTP) Agreement in February 2019

- TFTP Agreement allows for the exchanges of financial information between the EU and the U.S. in order to generate financial intelligence in the fight against terrorism.
- Scope of EDPS inspection: **verification role** assumed by Europol under the TFTP Agreement (Art. 4), i.e. : check that the data requested by the U.S. to the Designated Provider of international financial payment messaging services (SWIFT) are necessary for the fight against terrorism and its financing. **Europol only verifies the requests** from the U.S. to SWIFT, it does not have access to the data that are actually transferred from SWIFT to the U.S.

- Results of the inspection: the EDPS made **8 recommendation**s to further improve Europol's verification role under Art. 4 TFTP, relating both to the verification process and to security measures.

- EDPS **report**
  - initially classified EU Secret (because refers to documents classified as such),
  - has just been declassified (i.e. is now public info) by the originator of the inspected documents (U.S.), with the exception of one recommendation, on the modalities of the encrypted communication between Europol and SWIFT
  - will be published on EDPS website in the coming days

- EDPS will closely follow up implementation of recommendations by Europol