6th meeting of the Joint Parliamentary Scrutiny Group on Europol
Exchange of Information by Electronic Means

Requests for clarifications

Data Processing in Europol, with an emphasis on data flows pertaining to the Europol External Strategy and Operational Agreements with Third Countries

EUROPEAN PARLIAMENT DELEGATION TO THE JPSG

Requests for clarification by MEP Clare DALY

Paragraph:
'We closed our inquiry into the model working arrangement used by Europol to establish cooperative relations with the authorities of third countries, under Article 23(4) ER. We were concerned that the definition of "information" as comprising both personal and non personal data would create misunderstandings and lead to unlawful transfers of personal data to these countries. After a series of meetings with Europol staff, we agreed on a wording that would ensure that such working arrangements are not used to transfer personal data outside of the cases defined under Article 25 ER.'

Questions:

1. Could you please clarify whether such a broad definition of 'information' used in the existing working arrangements has actually led to unlawful transfer of personal data to third countries?

   The model working arrangement under scrutiny was only used with Israel, Japan and New Zealand. Transfers to these countries fall under the provisions of Chapter V of the Europol Regulation (ER), irrespective of the content of the working arrangement. In 2019, the EDPS inspected the cases where Europol used the derogations under Article 25(5) ER. This inspection has shown that, even if the procedure in place could be improved in some aspects, Europol is very well aware of the applicable regime. As the inquiry was still ongoing, we decided to focus the inspection on transfers notified to the EDPS.

2. Could you please provide us with the new wording agreed between the EDPS and Europol staff? In that regard, could you please clarify the legal value of the new wording and to which instruments it applies? Shall it be included in future working arrangements, or does it aim to amend existing arrangements, too?

   The EDPS decided to open an inquiry because on the one hand the Working Arrangement contained a definition of information covering both personal and non-personal data and on the other hand it provided that in some cases exchange of personal data might be allowed under the conditions of Article 25(5) and (6) ER.

The new version of the model Working Arrangement still contain these two provisions but adds a specific Chapter that regulates the exchange of information. This Chapter specifies the safeguards that apply whenever the parties exchange information and the additional minimum safeguards when they exchange personal data, provided it is duly authorised under the applicable legal frameworks. These provisions are meant to enable Europol to use secure communication channels in use to transfer personal data if necessary under the exceptional cases regulated by Article 25(5) and (6) ER and to define ex-ante the minimum data protection safeguards that should surround these transfers.

This should not be read as a blanket authorisation for transferring personal data to these countries and the wording of the Working Arrangement is clear on this aspect. Europol must assess on a case-by-case basis, when the authorisation to transfer personal data is granted, whether the data protection safeguards contained in the working arrangement are sufficient or whether they should be supplemented by additional safeguards.

The new wording will be used only in future working arrangements. We were not informed of any intention of Europol to reopen the negotiations with Israel, Japan or New Zealand to modify the content of the Working Arrangements.

For the precise wording of the new model working arrangement, we invite you to formulate your request to Europol according to the rules established by the Working Arrangement of the European Parliament and Europol established under Article 52 of the Europol Regulation. The EDPS is not allowed to share this document on behalf of Europol as the document is classified.

3. Can you provide more information on the number of exceptional transfers of personal data pursuant to Article 25, Paragraphs 5 and 6, ER?

Since the entry into force of the Europol Regulation on 1st May 2017, the EDPS was informed that Europol made use twice of the derogations contained in Article 25(5) ER to transfer data to third countries (both in the course of 2019). So far we have not been informed of any use of Article 25(6) ER to base such transfers.

Paragraph:
'We inspected specific transfers authorised on a case-by-case basis by Europol's Executive Director to ensure that the process in place and the safeguards devised complied with the Article 25(5) ER.'

Question:

4. Could you please outline briefly the specific steps involved in such an inspection and the main findings?

The 2019 Europol inspection report details the steps, findings and recommendations of the inspection. This document is EU-restricted, meaning that the EDPS is not allowed to publicly discuss its content. We will however share with Mrs. Clare Daly the relevant parts of the report, in accordance with the applicable security rules.

Paragraph:
'*EU large-scale IT systems...include personal data on particularly vulnerable persons, such as witnesses, missing or at-risk persons in the SIS. Data subjects and their family members may face prejudice or danger in their country of origin or another third country based on information kept in these systems… Utmost caution should remain regarding any communication of data from EU large-scale IT systems to third countries, including where it is further processed and exchanged as intelligence.'*

Questions:

5. Does the EDPS have particular and specific concerns about the use of data from large-scale IT systems by Europol last year that have given rise to this comment? Or is the EDPS simply flagging it as an area requiring caution going forward? Is the current framework governing the communication of data from large-scale IT systems by Europol to third countries sufficiently robust, in the view of the EDPS, to ensure that vulnerable persons will not be put at risk by the transfer of their data (including unnecessary or extraneous information about them) to third countries?

The topic was indeed flagged to mark the overall sensitivity of the use of personal data from large-scale IT databases. Europol has a unique position and status in relation to these systems, which remains one of the focal points of the EDPS.

While the EDPS has expressed its concerns in the past around the myriad of legal instruments applicable in this field, which renders it opaque to data subjects, the individual instruments do share strict limits on any communication of their data to third countries. Together with the Europol Regulation, the framework appears adequate to mitigate related risks for vulnerable persons. However, this is to be reassessed continuously in light of their use in practice.

Paragraph:
Without a holistic view including of the intake of personal data from within the EU, the full scope of risks for data subjects might be overlooked. The interplay between internal access to EU large-scale IT systems and external exchanges with third countries should always be kept in mind, not in the least for any future project in the framework of interoperability,'

Questions:

6. Does the EDPS have specific recommendations in this regard, in addition to the previously published opinions? Is the EDPS satisfied that their recommendations in this regard are being kept in mind and followed in this context?

This point was flagged as well by the EDPS in response to the recent adoption of legal instruments creating new large scale information systems, revising existing ones or establishing their interconnection, which impact Europol's personal data processing activities. Considering that these instruments are quite recent and were to some extent negotiated in parallel, close scrutiny also as regards their future implementation will be needed to ensure that there are no gaps, including on potential transfers of the data accessed by Europol to third countries.