EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
SUPERVISOR

Mr. Ranko OSTOJIC
Co-Chair of the JPSG
Head of the Croatian Parliament Delegation

Mr. Juan FERNANDO LOPEZ AGUILAR
Co-Chair of the JPSG
Chair of the Committee on Civil Liberties, Justice and Home Affairs
European Parliament

By email at:
jpsg.libesecretariat@europarl.europa.eu
jpsg@parleu2020.sabor.hr

Brussels, 29th May 2020

WW/LS/vm D(2020) 1330 **C 2020-0162**
Please use edps@edps.europa.eu for all correspondence

Subject: Invitation to exchange of information by electronic means in the framework of the JPSG

Dear Mr. Ostojic,
Dear Mr. López Aguilar,

The sixth meeting of the Joint Parliamentary Scrutiny Group ("JPSG") due to take place in Zagreb in the first half of 2020 unfortunately had to be cancelled due to the COVID19 pandemic and the earthquakes that hit Zagreb in March, and was replaced by an exchange of information by electronic means between the JPSG members and representatives of bodies originally invited to the meeting.

You have kindly asked me to share in writing the report and views of the EDPS on "Data Processing in Europol, with an emphasis on data flows pertaining to the Europol External Strategy and Operational Agreements with Third Countries", in order to initiate written exchanges with members of the JPSG who will be invited to send questions and contributions.

The Europol External Strategy for 2017-2020 sets up the objectives for Europol cooperation with third countries, in particular in the areas of the fight against serious and organised crime, cybercrime and terrorism. Europol's objective to optimise its network of operational and strategic partnerships is of specific interest to the EDPS as it involves an increase in the exchange of personal data. Europol's primary objective is to ensure proper exchange of information and strengthening its role as the EU criminal information hub, through strategic and operational partnerships with external partners in accordance with Articles 23 and 25 of the Europol Regulation ("ER").

In the course of 2019, the EDPS has carefully monitored the use by Europol of Articles 23 and 25 to transfer personal data to third countries, with which there was no cooperation agreement allowing for the exchange of personal data concluded before May 2017. In this context, the EDPS carried out the following activities:

- 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.

- 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.

- We explored with Europol, in reply to a consultation, the possibilities to use the derogation provided for by Article 25(6) ER.

On the basis of these supervisory activities, I would like to draw the members of the JPSG's attention to three matters for concern:

- It is paramount that all possibilities to transfer data abroad provided under Article 25(1) ER are fully exploited in order to avoid the risk of overusing the derogation contained in Article 25(6) ER, which should only be used in exceptional cases. There is indeed a risk that Europol would have to perform *ad hoc* adequacy assessments wherever there is no guidance from the Commission in that regard.

- It may be worth considering the possibility to include into operational agreements (even when they are not intended to authorised the exchange of personal data) basic data protection safeguards wherever there is sufficient basis to allow such transfers under the derogation provided by Article 25(5) ER. Our supervisory activities have shown that the lack of a secure communication channel with the third country in question may lead Europol to use alternative secure channels that do not always offer sufficient guarantees in terms of data protection (in particular, no guarantee that the information is only shared with the recipient and no information on the fact that the information has reached the recipient). This has led the EDPS to agree to have some basic data protection safeguards included in working arrangements, even if these are not intended to regulate the exchange of personal data, in order to also cover cases where the use of derogations is allowed.

- The difficulty to draw a clear line between the scope of application of Article 25(5) ER and Article 25(6) ER. While the cases under our scrutiny were quite clear, they have shown that this issue deserves further attention.

Furthermore, in accordance with Article 25(1) ER, the main legal channels for transfer of data to third countries are adequacy decisions under Article 36 of Directive (EU) 2016/680 ("Law Enforcement Directive") and international agreements pursuant to Article 218 TFEU. During the last year, there have been developments in both areas:

- In the context of the negotiations for a new partnership with the United Kingdom ("UK"), the Commission has proposed the first ever adequacy assessment under the Law Enforcement Directive, which will apparently affect also the cooperation of Europol with its British counterparts. The EDPS issued Opinion 2/2020[1], where we supported the approach and recommended that the adequacy assessment should in particular consider the impact on transfers by Union institutions, bodies, offices and agencies to the UK.

- On 31 January 2020, the EDPS adopted Opinion 1/2020 on the negotiating mandate to conclude an international agreement on the exchange of personal data between Europol and New Zealand law enforcement authorities[2]. The Opinion is principally based on the position already expressed by the EDPS in Opinion 2/2018 on negotiating mandates to conclude international agreements allowing the exchange of data between Europol and eight countries of the Middle East and North African regions[3]. At the same time, it takes also into account the specific situation of New Zealand and more specifically the existence of a well-developed national data protection system.

On 14 May 2020, the Commission issued an inception impact assessment[4] on the amendment of the ER. The review of the ER has been announced in the Commission Work Programme for 2020 with the aim to *"strengthen the Europol mandate in order to reinforce operational police cooperation"*[5]. The Commission has identified five objectives, each with several options, including streamlining and enhancing Europol's cooperation with third countries. The EDPS will follow closely the proposed changes to the ER and will issue an opinion in accordance with Article 42 of Regulation (EU) 2018/1725.

Finally, we have to recognise that external data flows are only half of the story. When discussing international data transfers, we must equally keep track of the expanding ways in which data enter Europol's systems. Over the past few years, Europol's access to EU large-scale IT systems has been significantly bolstered, *e.g.* through its extended access to the Schengen Information System ("SIS").

Europol's function of enabling information exchange between Member States, but also with the wider law enforcement community, is at the heart of its tasks and responsibilities. At the same time, EU large-scale IT systems were created with strong safeguards and limitations to reduce their potential negative effects on data subjects, as they include personal data on particularly

[1] https://edps.europa.eu/sites/edp/files/publication/20-02-24_opinion-eu-uk-partnership_en.pdf
[2] https://edps.europa.eu/sites/edp/files/publication/20-01-31_opinion_recommendation_europol_en.docx.pdf
[3] https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_international_agreements_europol_en.pdf
[4] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12387-Strengthening-of-Europol-s-mandate
[5] https://eur-lex.europa.eu/resource.html?uri=cellar%3A7ae642ea-4340-11ea-b81b-01aa75ed71a1.0002.02/DOC_1&format=PDF

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. Therefore, 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.

You have requested my views on the external component of personal data flows, which certainly also merits careful scrutiny. However, 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.

I am looking forward to receiving your written contributions and possible questions linked to this report.

Kind regards,

[signed]

Wojciech Rafał WIEWIÓROWSKI