

Requests for clarifications received from Members of the EP Delegation to the JPSG

Exchange of information by electronic means

6th meeting of the Joint Parliamentary Scrutiny Group on Europol

Reporting on Europol Activities September 2019-June 2020

Requests for clarification by MEP Caterina CHINNICI

European Serious and Organised Crime Centre

In the Reporting on Europol Activities September 2019-June 2020 there is a mention of the reorganization of the European Serious and Organized Crime Center, which will include, alongside the current European Migrant Smuggling Center (EMSC), a Unit specializing in drug trafficking and a Unit for the fight against organized crime in order to respond to the needs of the Member States to receive more specialized support in investigating high-risk multi-criminals and organized crime groups.

1. Could Europol provide more information about this reorganization and the reasons behind this decision?
2. In particular, with regard to the Unit for the fight against organized crime, does Europol believe that its work would be significantly facilitated if the European Union were to bring all the measures adopted so far in the fight against organized crime to a uniform and systematically coherent regulatory framework, for example through the adoption of a *European framework directive against organized crime*?

Child abuse material online

In the Reporting on Europol Activities September 2019-June 2020, the important OPERATION GARGAMEL operation is illustrated, according to which, on March 31st, the Belgian police with the support of Europol dismantled a global network of child abuse with links in over 40 countries, starting with a search during which over 9 million photos and videos of the abuse of thousands of children from all over the world were found. Thanks to the identification task force Europol has managed to identify 70 children and 30 suspects. The Belgian federal judicial police managed to identify 60 suspects (including 24 in Belgium) and 40 victims, bringing the total to 90 suspects and 110 victims.

3. With regard to this investigation, which once again proves that such a horrendous crime has, unfortunately, no hints to diminish, can Europol say whether, to date, investigations continue to identify the other victims involved, given the huge number of child pornographic material acquired?

The global nature of this type of crime requires global intra-EU collaboration and especially with third countries. Also taking into account that many of the minors involved in these criminal networks often belong to vulnerable categories and, therefore, their identification is more difficult (unaccompanied minors, minors from families in extreme poverty).

4. For this reason, does Europol collaborate with the competent law enforcement authorities of Third Countries and / or the various organizations aimed at monitoring this phenomenon such as, for example, the National Center for Missing & Exploited Children - NCMEC? If so, is the degree of collaboration with them considered sufficient?

Europol Innovation Lab

Request for clarification by MEP Caterina CHINNICI

In 2020 Europol set up the Innovation Lab, which aims to act as a monitoring hub for new technological developments and promote innovation, also through the development of common technological solutions for Member States in the field of internal security.

One of the first projects undertaken within the Innovation Lab program concerns a mechanism that allows greater speed for the recognition and reporting of child pornography online. This is a very important project given the constantly increasing volume of child pornography published online.

1. Could Europol give us clarifications on the collaboration with private online platforms on this project?

We know, in fact, how important a close public-private cooperation on this issue is and, therefore, I would like more details on the possible participation and involvement of private stakeholders.

2. Again, with regard to the new Innovation Lab, I would like to ask if there is also a revision of the technological tools for the exchange of information.

We know that law enforcement authorities and judicial authorities of the Member States face difficulties in the exchange of big amount of data through safe channels.

3. Is it possible to develop programs which overcome these difficulties and which allow a fruitful and secure collaboration between Europol and the Member States?

Request for clarification by MEP Patrick BREYER

1. The document stresses that "currently the Europol Innovation Lab is supporting EU Member States to implement three recently awarded H2020 funding projects". However, the document only provides two examples. Could you please provide a complete list of all the projects and more detailed information on each of them?

Reporting on Europol External Relations September 2019-June 2020

Request for clarification by MEP Clare DALY

Paragraph:

'Europol continued its cooperation with Israel established by a Working Arrangement signed in 2018. Israel has its Liaison Bureau in Europol Headquarters since September 2018 and cooperation has been assessed very positively by both Europol operational units and the Liaison Officers' community. Israel is connected to SIENA. There has been active engagement in a number of operations, for example focusing on CEO fraud, crypto trading, investment scams and numerous contacts of a more strategic nature'

Questions:

1. Could you please provide a full list of third-countries and authorities connected to SIENA, particularly those with which Europol does not have 'operational agreements' but only 'working arrangements'? (Europol website only mentions Australia, Canada, Norway, Liechtenstein, Moldova, Switzerland and the United States)
2. Could you please provide us with more information and some examples on the type of 'active engagement' of Israel National Police in those operations? Could you please clarify whether personal data has been transferred to Israel (or to other third-countries with which there is no operational agreement in place)? If that is the case, on which legal basis?
3. On which legal basis was the connection to SIENA granted? Is the Memorandum of Understanding mentioned in Article 20 of the Working Arrangement with Israel publicly available?
4. Could you please provide detailed information on the functioning of SIENA? In particular, could you describe how it can prevent that personal data is exchange in the absence of an adequate legal basis?

Management Board activities from September 2019 to June 2020

Request for clarification by MEP Caterina CHINNICI

In the September 2019-June 2020 Report on the Activities of the Europol Management Board, the achievement of an employment agreement with OLAF in the fields of combating fraud, corruption and money laundering is announced. From the data provided by the Europol Agency¹ itself, we know that criminal organizations will try to exploit the economic crisis due to the CoVid-19 pandemic. One of the biggest risks has been identified in the laundering of money from illegal activities.

1. For this reason, I would like to ask if the working agreement between Europol and OLAF provides for particular attention towards the crime of money laundering.

¹ From the most recent Europol Report "Beyond the pandemic- How Covid19 will shape the serious and organized crime landscape in EU"

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

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

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?

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?

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?