EUROPOL

The Hague, 20 February 2019

Joint Parliamentary Scrutiny Group Secretariat

To the attention of the JPSG Co-Chairs

Europol reply to written questions from the delegation of the Netherlands to the Joint Parliamentary Scrutiny Group (JPSG)

Dear Ms Florea,

Dear Mr Moraes,

In accordance with Article 4.2 of the JPSG Rules of Procedure and Article 51 of the Europol Regulation, Europol would like to respond to the questions raised by the delegation of the Netherlands to the JPSG as follows:

1. **The draft multiannual programming document stresses the ambition to increase operational activities by Europol. For instance, its refers to "full scale delivery of operational service and impact". The delegation would like to request information about what practical consequences national police authorities might expect in this regard?**

The mission of Europol is to support the Member States in preventing and combating all forms of serious international and organised crime, cybercrime and terrorism. Europol realises its mission by providing a variety of operational products and services, with a view to achieving a positive impact for the security of the EU.

Europol aims at providing focused and tailor-made operational support adapted to the needs of Member States and the specific nature of the case. Europol determines the different levels of operational support through a prioritisation mechanism.

The ambition for delivering operational service is expressed in the new Europol Strategy 2020+, endorsed by the Europol MB in December 2018, in the strategic priority 2 – "Deliver agile operational support". A copy of the new Europol Strategy 2020+ is enclosed.

Europol re-assesses its type of services on a continuous basis, which include, as outlined in the Europol Programming Document 2019-2021 adopted by the Management Board on 30 January 2019 (copy enclosed), the following actions, for Europol to:

- Act as 24/7 contact point for urgent operational requests from Member States' Liaison Bureaux, Europol's National Units (ENUs), competent authorities and for on-the-spot deployment by Europol staff (cross-checking of data across all relevant data bases and applications available to Europol, mobile office support, mobile device extraction kits, digital and document forensic support, dismantling synthetic drug labs and cannabis cultivation and production sites, technical support to investigate counterfeit currency production, payment card fraud etc.);
- Actively support Member States in overcoming the technical challenges to their cyber and cyber-facilitated investigations, by identifying suitable tactics, devel-

oping dedicated tools, and sharing best practices to respond to the emerging operational needs (e.g. cryptocurrencies/Blockchain and big data analysis, etc.);

- Initiate the emergency procedures and crisis response steps in case of operational emergencies and terrorist incidents within the EU or impacting the security of the EU, including EU Internet Referral Unit (IRU) services which include social media investigative support and referral of terrorist propaganda online to Online Service Providers (OSPs) for subsequent removal;
- Support Member States in preventing and combating all forms of serious crime, focussing on the selection of High-Value-Targets (HVT), and including on crime related to the sexual exploitation of children, and to enhance victim identification efforts, including the development of the Image and Video Analysis Solution (IVAS);
- Coordination and financial support for operational meetings, as well as the Operational Action Plans (OAPs) corresponding to EU crime fighting priorities;

2. **Further information is also requested regarding Europols ambition to enhance its multi-disciplinary approach and the intention to increase Europol's ability to cooperate with the private sector. What activities does Europol envisage to deploy and what are the results aimed for? The Dutch delegation would appreciate detailed information about this matter.**

Under the Europol Regulation[1], Europol should maintain cooperative relations with private parties to the extent required for the accomplishment of its tasks. These cooperative relations may include the exchange of information, with the exception of personal data. Therefore, Europol is prohibited from exchanging personal data directly with private parties, with the exceptions defined in the Article 26(5), (6) of the Europol Regulation.

Similarly, private parties should generally not transfer personal data to Europol, with some exceptions, outlined in Europol legal basis. The Commission shall evaluate the practice of direct exchanges of personal data with private parties by 1 May 2019.

In a fast evolving criminal landscape and diversified emerging security threats, partnership with the private sector has increasingly gained importance for Europol work in a wide range of areas.

Below are some examples of cooperation with the private sector, including possible future developments, the:

- **EC3 (European Cybercrime Centre)** has established a network of more than 80 trusted private companies, divided into three advisory groups covering three major industries (Financial Services, Internet Security and Telecommunication Providers);
- **ECTC (European Counter Terrorism Centre)** is working towards the increase of cooperation with private parties within the ECTC Advisory Network. This Advisory Network is platform for knowledge transfer in the area of counter terrorism between researchers in academia and industry, on the one hand, and Europol, law enforcement and policy makers, on the other.

  Within ECTC, the **EU Internet Referral Unit (IRU)** since its set up in 2015 has been cooperating with the online industry, in the framework of the EU Internet Forum, with the objective of reducing accessibility to terrorist content online. This cooperation is built upon the voluntary approach and trust-based relationship with the industry. In the context of the envisaged legislative developments

[1] Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol)

at EU level in the area of fight against terrorist content online, EU IRU will upgrade its operational tools.

- **Europol-led SIRIUS project** aims to improve EU-US cooperation on cross border access to electronic evidence by producing and disseminating trainings and OSINT tools to EU Law enforcement Authorities and judicial authorities.
- Further to the launch of the **Europol Financial Intelligence Public Private Partnership (EFIPPP),** the first transnational public-private information sharing mechanism in the field of anti-money laundering and counter-terrorist financing. The EFIPP brings together the 15 international banks and representatives from 8 countries to build a common understanding of the threat, exchange strategic information (joint drafting of typologies) and facilitate the exchange of tactical information associated with on-going investigations, through domestic public-private partnerships. The EFIPPP is planning for a gradual expansion to new financial institutions and countries in 2019.

3. In the context of Rule of Law, questions can be raised about the extent to which it is desirable to negotiate and enter into third-country agreements, especially with countries that have a questionable reputation in the area of the protection of human rights. Which criteria does Europol use in identifying potential third countries? Which requirements and conditions apply?

In so far as necessary for the performance of its tasks, Europol may establish and maintain cooperative relations with external partners in accordance with Europol's new external relations regime outlined in Chapter V of the Europol Regulation. The Europol Regulation (2017) brought a new scheme of establishing its external relations.

Establishing operational cooperation (i.e. exchange of personal data) with new external partners is possible via an adequacy decision or an operational agreement which are concluded on behalf of the Union. The responsibility for the adequacy decision or the negotiation of a respective international agreement lies with the European Commission.

Data protection safeguards and fundamental rights are addressed by the European Commission in the corresponding negotiation mandate. Mandated by the Council and the European Parliament, the European Commission has chosen to enter into negotiations for international agreements with Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey.

Strategic cooperation (i.e. no-exchange of personal data, but sharing best practises, trainings, etc...) can be established via working arrangements negotiated and signed by Europol.

Further details were provided with the answers to the Written Question n. 1 by the Bundestag, sent to the JPSG Secretariat on 30 November 2018.

Please find the link to the list of operational agreements and strategic agreements.

In identifying potential third partners for operational cooperation, Europol takes political guidance from the European Commission and EEAS. Identification of partners for strategic cooperation is done by Europol on the basis of operational and strategic needs and considerations, in coordination with Member States and the European Commission. A list of priority countries is endorsed by Europol Management Board.

On a practical level, Europol's activities are subject to regular scrutiny by the European Data Protection Supervisor (EDPS).

4. How does Europol ensure the requirements as regards privacy and data protection, especially with regard to Europol's s ambition to further

gather intelligence, for example by further developing its travel intelligence capability?

Europol has a comprehensive, robust and tested regime in place that is widely recognised as safeguarding and ensuring the highest standards of data protection in the law enforcement world. It aims at ensuring the protection of privacy of the persons whose data are processed in Europol's systems. At the same time, it serves the needs of operational units in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States.

The full compliance with data protection principles[2] forms the basis for the trust of Member States. Namely Member States are the providers and owners of the intelligence processed at Europol and in this way one of the main beneficiaries of Europol's data protection regime. Additionally, citizens expect the organisation to tackle contemporary challenges to Europe's safety in a way that fully respects fundamental rights including the right of protection of personal data.

In this regard, a tailor-made set of rules has been created to effectively take into account both the operational needs of the agency and the individuals' right to effective data protection. The collection and processing of data is at the heart of Europol's activities. Any processing of personal data within Europol has to be explicitly allowed and made compliant with the data protection regime. The main objective of the Europol Regulation is to set a data processing environment that allows Europol to fully assist Member States in preventing and combating serious and organised crime and terrorism when simultaneously respecting fundamental rights such as the right to data protection.

In practical terms, the Europol Regulation redefines the agency's data processing architecture. The legislator no longer pre-defines databases or systems but instead adopts a 'data protection by design' approach and full transparency towards the Data Protection Officer (DPO) at Europol and the European Data Protection Supervisor (EDPS), the EDPS. High data protection and security standards are achieved by means of procedural safeguards that apply to any specific type of information. Thus, the Europol Regulation introduces a technology-neutral approach to data management and processing that provides for enhanced operational flexibility.

Under the Europol Regulation, there is no reference anymore to different information processing systems (for instance, Analysis Work Files (AWFs), Europol Information System (EIS), new systems). Instead, the emphasis of the text is on the exact purpose(s) for which data can be processed, namely: (i) cross-checking aimed at identifying connections or relevant links between information; (ii) analyses of a strategic or thematic nature; (iii) operational analysis; and, (iv) facilitating the exchange of information. In practice, data processing at Europol is performed with the aid of specifically designed software, refined techniques and sophisticated structures. The prioritisation and targeting of operational action is based on the specific purposes for which the data will be processed. In this way, the Europol Regulation provides for a close, functional relationship between the various forms of analysis. It is in particular by means of strategic analysis that the overall priorities can be distinguished and justified. It is by means of thematic analysis that within specific crime areas cases and approaches can be identified. It is within the framework of operational analysis that concrete investigations and operations will be supported. In this context, the Europol Regulation outlines not only the specific purposes of data processing activities, but also the sources of information as well as who may access the relevant data. The Europol Regulation highlights the holistic approach taken by Europol to protect personal data that foresees next to procedural safeguards the application of technical and organisational measures for the protection of information.

In this context, the main challenge is the application of the data protection framework to the day-to-day operations of the agency. The DPO plays a key role in this

[2] Article 28, Regulation (EU) 2016/794, Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol)

context as he is in the ideal position to ensure the lawfulness and compliance of data processing operations with the applicable legal framework. The DPO has a broad profile of tasks including:

- Assurance activities as described in Article 41 of the Europol Regulation as well as the DPO Implementing Rules;
- Consultation activities, including activities in relation to legal and technical-organisational data protection safeguards;
- Coordination activities, including the cooperation with the EDPS, national data protection authorities, participation in DPO networks such as the JHA DPO network;
- Awareness raising activities;
- Training activities, including regular newcomers' data protection sessions and other trainings upon special organisational need such as Guest Officers' training.

For travel Intelligence, the main aim is to implement the legal instruments that have been agreed to strengthen border management and internal security, such as the PNR Directive, the adjustments to the SIS, VIS and Eurodac legislation and the creation of EES and ETIAS, as well as the Interoperability Regulation. The legislative package includes provisions on data protection and human rights which will be duly implemented. The relevant internal and external entities including the DPO and the EDPS will continue to be involved throughout this process. In particular, the procedure of prior consultation of the EDPS as stipulated in Article 39 of the Europol Regulation (EDPS is pre-consulted each time any new type of processing operations by Europol entailing personal data processing so require)be applied as necessary.

5. **From Annex 1: Resource allocation per Activity 2019-2021" it can be concluded that resources allocated to counter terrorism are nearly as high as those allocated to combating serious and organised crime. How does this allocation correspond to the attention and resources that national authorities allocate to these matters?**

Europol does not have information about the allocation of resources in the national authorities; moreover, the allocation of resources at national level would not be comparable to Europol's allocation as the mandates and tasks of national authorities are broader and different to those of Europol.

Europol is funded by the EU Budget - its resource programming is detailed in the Multi-annual Financial Framework and the annual budget decided on by the EU Council and EU Parliament during the annual EU budgetary process. The programming document detailing the planned work of Europol and its draft estimate of revenue and expenditures is approved by the Management Board of the agency, which is comprised of representatives of all Member States and the European Commission. More generally, Europol strategic orientations are discussed and approved by the Management Board in light of the views consensually expressed by the national authorities themselves, as represented by the respective Management Board Members.

In the aftermath of the terrorist attacks in Paris (Nov. 2015), the Justice and Home Affairs Council re-affirmed its determination to intensify the efforts in the counter-terrorism domain. The Council supported the launching of the European Counter-Terrorism Centre at Europol as of 1 January 2016, including the EU Internet Referral Unit and urged the Commission to ensure that the necessary resources were made available to reinforce the ECTC.

6. **Further explanation is requested for goal 2 of the draft multiannual programming: "Europol will provide the most effective operational support and expertise to MS investigations [...]". The Dutch delegation would like to enquire what kind of operational support and expertise is**

meant in addition to providing information? What investigative authority do employees of Europol have while participating in national investigations? What is their mandate? How can the JPSG monitor these activities? Could Europol report on these activities to the JPSG?

Europol provides tailored high quality operational support to Member States investigations in three key priority areas, aligned with the European Agenda on Security, namely Serious and Organised Crime, Cybercrime and Counter-Terrorism.

Reply to question 1 outlines the kind of expertise and operational support Europol.

As regards the questions concerning Europol's mandate and questions concerning any investigative capacity or mandate, this is determined by Article 3 of the Europol Regulation, as equally found in Article 88 TFEU, which states that "*Europol shall support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy*". Additionally, according to Article 4 of the Europol Regulation, one of Europol's tasks reads:

"1. (...) (c) coordinate, organise and implement investigative and operational actions to support and strengthen actions by the competent authorities of the Member States, that are carried out: (i) jointly with the competent authorities of the Member States; or (ii) in the context of joint investigation teams (...).
(...) 5. Europol shall not apply coercive measures in carrying out its tasks."

Europol therefore may not and does not apply any coercive measures, but delivers support in connection with Member States' investigations, in line with its mandate and the above examples.

Finally, a specific area of support foreseen for Europol is its participation in Joint Investigation Teams, whereby Article 5(2) of the Europol Regulation (emphasis added) foresees that "*Europol staff may, **within the limits of the laws of the Member States** in which a joint investigation team is operating, assist in all activities and exchanges of information with all members of the joint investigation team."*

The applicable law governing any 'operational' activity by persons other than national police officers is therefore also the national law – to the extent it even allows such an involvement by Europol (or also possibly for other external parties, e.g. experts, consultants, etc.). Whether this expert's assistance in e.g. a house search or performing an IT-related analysis of seized computers, is considered an investigative or operational activity is also very different dependent on the respective national legislation.

Concerning the way JPSG can monitor these activities, it should be underlined that, in accordance to Art. 51 of the Europol regulation, Europol supports effective scrutiny by the JPSG through different means, taking into account the obligations of discretion and confidentiality.

One example of Europol's support to operations is characterised by Operation Dryer:

Analytical Project (AP) Sustrans (money-laundering) supported Operation Dryer jointly with AP Synergy (synthetic drugs trafficking and production). The investigation developed under the lead of Spain and involving Austria, The Netherlands and Germany, targeting an Organised Criminal Group (OCG) that offered synthetic drugs on the dark web and received cryptocurrency in return. Large amounts of money and cryptocurrency transfers between companies were detected. The OCG also created a network of companies to layer and manage clandestinely the assets derived from the sales of drugs, reaching links in offshore jurisdictions such as Sin-

gapore, Hong Kong or Gibraltar. Links were detected with other money laundering syndicates in charge of exchanging cryptocurrency for cash and transporting the illicit cash from the Netherlands to Spain. Through Europol's analysis, several investigations were brought together, triggering cooperation between the countries concerned. Searches took place at private and business premises, and large amounts of cash, cryptocurrency and evidence were seized. Europol provided expert support on-the-spot. Two laboratories with a large amount and variety of synthetic drugs were dismantled. In the first lab, more than 50 kg of pills and one million doses of LSD were found. In the second lab, an higher amount of drugs was found. Eight persons were arrested on suspicion of drug trafficking, money laundering and membership of a criminal organization.

Trusting these answers will prove satisfactory; Europol remains available for further clarifications.

Yours sincerely,

Oldřich Martinů
Deputy Executive Director Governance