Working Arrangement
on cooperative relations
between the European Anti-Fraud Office (OLAF) and the European Union Agency for Law Enforcement Cooperation (Europol)

The European Anti-Fraud Office
(hereafter referred to as "OLAF")

and

the European Union Agency for Law Enforcement Cooperation
(hereafter referred to as "Europol")

– together referred to as "The Parties" –

Aware of the urgent problems arising from international organised crime, especially terrorism, and other forms of serious crime and their possible link to illegal activities affecting the Union's financial interest,

Aware of the need to work together to fight fraud as well as the potential for enhanced cooperation,

Recalling the duty of mutual sincere cooperation as laid down in Article 13(2) of the Treaty on European Union,

Considering OLAF mandate to carry out administrative investigations intended to combat fraud, corruption and any other illegal activity adversely affecting the Union's financial interests as well as Article 13 of Regulation (EU, Euratom) 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF), as amended, as a basis for the cooperation with Europol and the possibility to exchange operational, tactical, strategic or technical information, including personal data and classified information, in the framework of such cooperation,

Considering Articles 4(j), 21, 23 and 24 of the Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation, as amended, (hereafter referred to as "Europol Regulation") as well as that the Europol Management Board has on 22 April 2020 approved the present Working Arrangement,

Considering the application of Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies to the processing of administrative personal data held by Europol, in accordance with Article 46 of the Europol Regulation,

Considering that the Parties have concluded a Memorandum of Understanding on the secure communication line between the European Anti-Fraud Office and the European Union Agency for Law Enforcement Cooperation of 31 January 2018,

Considering that the existing Administrative Arrangement between the European Police Office (Europol) and the European Anti-Fraud Office (OLAF) of 8 April 2004 should be replaced by the present Arrangement,

Have agreed as follows:

Chapter I – Purpose and Scope

1. Purpose

1.1. The purpose of this Working Arrangement (hereafter referred to as "Arrangement") is to establish cooperative relations between OLAF and Europol within the existing limits of the respective legal frameworks and mandates of the Parties, in particular through the exchange of information between the Parties including personal data.

1.2. This Arrangement does not cover the exchange of information and cooperation in relation to OLAF investigations carried out concerning Europol staff in accordance with Article 4 of Regulation (EU, Euratom) No 883/2013 and with the decision of the Management Board of Europol of 3 October 2018[1].

2. Definitions

For the purpose of this Arrangement:

a. "personal data" means any information relating to an identified or identifiable natural person, an identifiable person being a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier or to one or more

[1] Decision of the Management Board of Europol on the accession of Europol to the Interinstitutional Agreement of 25 May 1999 between the European Parliament, the Council, and the European Commission concerning internal investigations by the European Anti-Fraud Office.

factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

b. "information" means personal and non-personal data.

3. Scope of cooperation

The cooperation as established in this Arrangement relates to the relevant areas within the respective mandates of the Parties, including, but not limited to, fraud, corruption, money laundering, intellectual property crime or any illegal activity affecting the financial interests of the EU.

4. Forms of cooperation

The cooperation may, additional to the exchange of operational, tactical, strategic or technical information in particular include:

- exchange of information including case-related information,
- cooperating or participating in joint operations, such as Joint Customs Operations, Joint Action Days and Joint Investigation Teams, or in the framework of EMPACT Operational Actions,
- exchange of specialist knowledge, reports and results of analyses,
- information on criminal investigation procedures and on crime prevention methods,
- training activities and staff exchange for training purposes,
- support concerning the use of technical tools/equipment.

Chapter II – Mode of cooperation

5. Point of Contact

5.1. Each Party will designate a single point of contact within its organisation in order to maintain institutionally coordinated cooperation and implementation of the Arrangement, while affording experts the freedom to exchange information in accordance with the terms of this Arrangement.

5.2. The Parties will designate their points of contact by means of exchange of letters at the time of signature of this Arrangement. Any change in a designated point of contact will be promptly notified in writing.

6. Consultations and closer cooperation

6.1. The Parties agree that regular exchanges, as appropriate, are essential to further the cooperation and enhance, as well as monitor the development of the provisions of this Arrangement. Specifically:

- High level meetings between OLAF and Europol will take place regularly, to discuss issues relating to this Arrangement and cooperation in general;
- OLAF and Europol will meet regularly on matters of common interest for the purpose of realising their objectives and coordinating their respective activities;
- Where relevant, a representative of OLAF may be invited to attend the meetings of the Heads of Europol National Units, at their discretion.

6.2. The Parties should consult each other before communicating with media on operations, in which they were both involved, such as Joint Customs Operations, Joint Action Days and Joint Investigations Teams. The Parties should agree the text of a joint or individual press release on results thereof. Each Party should react to the request for such consultation as soon as possible, and preferably within 48 hours.

7. Liaison officers

The Parties may agree to the secondment of liaison officer(s). The liaison officers' tasks, rights and obligations, their number, and the costs involved shall be governed by a separate instrument agreed between the Parties.

Chapter III – Information exchange

8. General provisions

8.1. Exchange of information between the Parties will only take place in accordance with their respective legal framework and the provisions of this Arrangement.

8.2. Parties will only supply information to each other which was collected, stored and transmitted in accordance with their respective legal framework and has not been clearly obtained in obvious violation of human rights.

8.3. If during information-processing activities in respect of an individual investigation or specific project Europol or a Member State identifies information relevant to the application of OLAF's mandate, Europol should on its own initiative or upon request of OLAF provide OLAF with that information, in accordance with Article 19(2) of the Europol Regulation. For this, Europol should seek the Member State's consent for sharing the information with OLAF, unless the Member State has not indicated any restrictions.

8.4. In accordance with Article 36 of the Europol Regulation and Article 17 of Regulation 2018/1725, individuals shall have the right to access their personal data transmitted on the basis of the present Arrangement, and to have such personal data corrected or erased. In cases where these rights are exercised, the transmitting Party shall be consulted before a final decision on the request is taken, including concerning possible applicable restrictions to the rights of the data subject. The final decision shall be subsequently notified to the transmitting party.

8.5. Applications for public access to documents under Regulation (EC) No 1049/2001 transmitted on the basis of the present Arrangement will be submitted to the transmitting Party for their advice as soon as possible. The advice should be provided within a timeframe which allows compliance with the legal deadlines.

9. Exchange of personal data

9.1. Any exchange of personal data shall be in accordance with and based upon the Parties' respective legal frameworks, in particular Articles 19(2), 21(6) and (7), 23(6) of the Europol Regulation.

9.2. The Parties shall determine at the moment of transmission of the personal data or before, the purpose for which the data are transmitted. Europol may indicate any restriction at the moment of transmission of personal data on its use and erasure, including possible access restrictions in general or specific terms. Where the need for such restrictions becomes apparent after the supply, Europol shall inform of such restrictions at a later stage.

9.3. The Parties shall retain personal data only as long as it is necessary and proportionate for the purpose for which it was transmitted. Europol shall review the need

for continued storage no later than three years after the transmission. During the review, Europol may decide on the continued storage of data until the following review which shall take place after another period of three years if that is still necessary for the performance of its tasks. If no decision is taken on the continued storage of data, those data shall be erased automatically.

9.4. Personal data transmitted by Europol which have been included in an OLAF case file within the OLAF Case Management System shall be retained in accordance with Commission Decision (EU) 2018/1962 of 11 December 2018 laying down internal rules concerning the processing of personal data by the European Anti-Fraud Office (OLAF).

9.5. Where a Party has reason to believe that personal data previously transmitted by it is incorrect, inaccurate, no longer up to date or should not have been transmitted, it shall inform the other Party which shall correct or erase the personal data and provide notification thereof.

9.6. Where a Party has reason to believe that personal data previously received by it is incorrect, inaccurate, no longer up to date or should not have been transmitted, it shall inform the other Party which shall provide its position on the matter.

9.7. Personal data, by automated or other means, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, or data concerning a person's health or sex life shall not be transmitted between the Parties unless such transmission is strictly necessary and proportionate.

10. Indirect access by OLAF to information stored by Europol

10.1. In accordance with Article 21(1) of the Europol Regulation, Europol shall take all appropriate measures to enable OLAF, within its mandate, to have indirect access on the basis of a hit/no hit system to information provided to Europol for the purposes of points (a), (b) and (c) of Article 18(2) of the Europol Regulation.

10.2. Searches of information in accordance with paragraph 1 shall be carried out only for the purpose of identifying whether information available at OLAF matches with information processed at Europol.

10.3. Any restriction on access to the information or on the use to be made thereof, including as regards its transmission, erasure or destruction, shall be respected by OLAF and any further recipients.

10.4. In the case of a hit, Europol shall initiate, in an expedient manner, the procedure by which the information that generated the hit may be shared, in accordance with the decision of the provider of the information to Europol, and only to the extent that the information data generating the hit is are necessary for the performance of OLAF's tasks.

10.5. OLAF should provide Europol with information on which of their staff members have been authorised to perform searches of information in accordance with paragraph 1; Europol shall allow such searches only after this information has been received.

10.6. The Parties shall inform each other if, as a result of a hit, there are indications that information may be incorrect or may conflict with other information.

10.7. The Parties may consider concluding an arrangement implementing access by OLAF to information stored by Europol on the basis of Article 21 of the Europol Regulation.

11. Use of the information

11.1. In accordance with Articles 19 and 21(6) of the Europol Regulation and Article 4 of Regulation 2018/1725 information if transmitted with a purpose, notwithstanding the obligation to do so referred to in point 9(2), may be used only for the purpose for which it was transmitted and any restriction on its use, erasure or destruction, including possible access restrictions in general or specific terms, shall be respected by the Parties.

11.2. Information may not be further processed or used in a manner that is incompatible with the initial purpose, unless authorised by the transmitting Party.

12. Onward transmission of the personal data received

In accordance with Article 23(7) of the Europol Regulation any onward transmission of personal data, including to Union bodies, Member States, third countries and international organisations will receive the prior explicit authorisation by the transmitting Party, in specific or in general terms. Such consent may only be given when allowed under the applicable legal framework of the transmitting Party. Parties will endeavour to address any request for such an onward transfer expeditiously.

13. Assessment of the source and of the information

13.1. Europol shall assess the reliability of the source of information as well as the accuracy of the information in accordance with Article 29 of the Europol Regulation.

13.2. OLAF will endeavour to carry out an assessment according to the same standards when supplying information to Europol.

14. Security of processing of personal data

14.1. In line with their respective legal frameworks, the Parties will ensure that the personal data exchanged or received is protected through appropriate technical and organisational measures. Such measures will only be necessary where the effort they involve is proportionate to the objective they are designed to achieve in terms of protection, and will be designed to:

a. deny unauthorised persons' access to data processing equipment used for processing personal data (equipment access control),

b. prevent the unauthorised reading, copying, modification or removal of personal data media (data media control),

c. prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data (storage control),

d. prevent the use of automated data-processing systems by unauthorised persons using data-communication equipment (user control),

e. ensure that persons authorised to use an automated data-processing system have access only to the personal data covered by their access authorisation (data access control),

f. ensure that it is possible to verify and establish to which bodies personal data may be or have been transmitted using data communication equipment (communication control),

g. ensure that it is possible to verify and establish what personal data have been accessed by which member of personnel and at what time (access log),

h. ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the personal data were input (input control),

i. prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control),

j. ensure that installed systems may, in the event of interruption, be restored immediately (recovery),

k. ensure that the functions of the system perform without fault, that the appearance of faults in the functions is immediately reported (reliability) and that stored personal data cannot be corrupted by system malfunctions (integrity).

14.2. The Parties shall handle security incidents, including personal data breaches, in accordance with their applicable legal frameworks and internal procedures. The Parties shall immediately notify each other in the event of any personal data breach and of any measures taken to address the personal data breach and to mitigate the risk to the rights and freedoms of natural persons.

Chapter IV – Security of information

15. Protection of information

Each Party shall:

a. protect information subject to this Arrangement, regardless of its form, until it has reached its end of life and is securely destroyed. This obligation shall not apply to information which is expressly marked or clearly recognisable as public information,

b. ensure that it has a security organisation, policies and measures in place to comply with the requirements set out in this Arrangement,

c. manage information security risks for all systems processing information exchanged under this Arrangement and assess these risks on a regular basis and whenever there is a significant change to any of the risk components,

d. ensure that all persons handling information exchanged under this Arrangement are subject to a security screening in accordance with the legal framework of the receiving Party,

e. ensure that access to information is limited to authorised persons who need to have access to it in order to perform their official duties,

f. ensure that all persons handling information exchanged under this Arrangement are appropriately trained and familiar with the relevant security rules, policies and procedures,

g. ensure that all staff handling information exchanged under this Arrangement are made aware of their obligation to protect the information and acknowledge the obligation in writing,

h. ensure that the premises where information exchanged under this Arrangement is stored or handled have an appropriate level of physical security in accordance with the legal framework of the receiving Party,

i. ensure that it has a framework in place for reporting, managing and resolving security incidents and breaches.

16. Arrangement on the exchange and protection of classified information

16.1. The security procedures for exchanging and protecting classified information exchanged between the Parties shall be set out in an arrangement on the exchange and protection of classified information agreed between the Parties.

16.2. Exchange of classified information is conditional upon the conclusion of the arrangement on the exchange and protection of classified information.

Chapter V – Liability and Disputes

17. Liability

Each Party shall be liable, in accordance with its respective legal framework and other applicable Union rules, for any damage caused to an individual as a result of legal or factual errors in information exchanged.

18. Settlement of disputes

18.1. All disputes which may emerge in connection with the interpretation or application of the present Arrangement shall be settled by means of consultations and negotiations between representatives of the Parties.

18.2. In the event of serious failings of either Party to comply with the provisions of this Arrangement, or is a Party of the view that such a failing may occur in the near future, either Party may suspend the application of this Arrangement temporarily, pending the application of paragraph 1. Obligations inherent upon the Parties under the Arrangement will nonetheless remain in force.

Chapter VI – Final provisions

19. Secure communication line

19.1. The establishment, implementation and operation of a secure communication line for the purpose of exchange of information between OLAF and Europol is agreed upon between the Parties in the Memorandum of Understanding of 31 January 2018.

19.2. In case a Party considers it has suffered damage or detriment caused by the other Party as a result of wrongful actions relating to the establishment, implementation, operation, replacement or dismantling of the secure communication line, the Parties will seek an equitable solution in accordance with the procedure referred to in point 18.

19.3. Any dispute between the Parties concerning the interpretation or application of provisions relating to the establishment, implementation or operation of the secure communication line will be settled in accordance with point 18.

20. Expenses

The Parties will bear their own expenses which arise in the course of implementation of the present Arrangement, unless otherwise stipulated in this Arrangement.

21. Amendments

This Arrangement may be amended in writing, at any time by mutual consent between the Parties, and approved in accordance with the Parties' respective applicable procedures.

22. Application of the Arrangement

22.1. This Arrangement is applicable as from the day following the day of its signature.

22.2. This Arrangement does not exceed the respectively applicable legal frameworks of the Parties, nor create obligations incompatible with them, and does not cover mutual legal assistance.

22.3. The Administrative Arrangement between the European Police Office (Europol) and the European Anti-Fraud Office (OLAF) signed on 8 April 2004 is replaced by this Working Arrangement. The legal effects of the Administrative Arrangement remain in force.

Done in duplicate in the English language.

For **OLAF**

Ville Itälä
Director General

Done at Brussels
on 8 / 10 / 2020

For **Europol**

Catherine De Bolle
Executive Director

Done at The Hague
on 23 / 09 / 2020