Council of the European Union

Brussels, 19 January 2021
(OR. en)

5388/21

Interinstitutional File:
2020/0349(COD)

SIRIS 9
ENFOPOL 18
COPEN 20
SCHENGEN 6
IXIM 21
CODEC 58
IA 9

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	13908/20 + COR 1
No. Cion doc.:	COM(2020) 796 final
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

Delegations will find in the Annex the text of the Commission proposal for a Regulation amending Regulation (EU) 2016/794 (Europol Regulation).

During the informal videoconference of the members of the Law Enforcement Working Party on 25 January 2021, delegations will examine provisions pertaining to thematic blocs 1 and 3, as set out in 5397/21, that is ***enabling Europol to cooperate effectively with private parties*** and ***strengthening Europol's role on research and innovation***.

Delegations are kindly invited to refer to 5397/21 in order to identify the exact provisions to be discussed.

For working purposes, delegations may also refer to WK 757 2021 containing a document consolidating the proposed amendment to the Europol Regulation with the text of the Europol Regulation, as currently in force[1].

---

[1] However, WK 757 2021 is of a purely working character, and while changes agreed in the LEWP will also be introduced in its successive revisions, delegations should always refer to the present document (5388/21) or its future revised versions regarding the evolution of the Council's position.

ANNEX

2020/0349 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 88 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The European Union Agency for Law Enforcement Cooperation (Europol) was established by Regulation (EU) 2016/794 of the European Parliament and of the Council[2] to 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.

[2] 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 (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

(2) Europe faces a security landscape in flux, with evolving and increasingly complex security threats. Criminals and terrorists exploit the advantages that the digital transformation and new technologies bring about, including the inter-connectivity and blurring of the boundaries between the physical and digital world. The COVID-19 crisis has added to this, as criminals have quickly seized opportunities to exploit the crisis by adapting their modes of operation or developing new criminal activities. Terrorism remains a significant threat to the freedom and way of life of the Union and its citizens.

(3) These threats spread across borders, cutting across a variety of crimes that they facilitate, and manifest themselves in poly-criminal organised crime groups that engage in a wide range of criminal activities. As action at national level alone does not suffice to address these transnational security challenges, Member States' law enforcement authorities have increasingly made use of the support and expertise that Europol offers to counter serious crime and terrorism. Since Regulation (EU) 2016/794 became applicable, the operational importance of Europol's tasks has changed substantially. The new threat environment also changes the support Member States need and expect from Europol to keep citizens safe.

(4) As Europe faces increasing threats from organised crime groups and terrorist attacks, an effective law enforcement response must include the availability of well-trained interoperable special intervention units specialised in the control of crisis situations. In the Union, the law enforcement units of the Member State cooperate on the basis of Council Decision 2008/617.[3] Europol should be able to provide support to these special intervention units, including by providing operational, technical and financial support.

[3] Council Decision 2008/617/JHA of 23 June 2008 on the improvement of cooperation between the special intervention units of the Member States of the European Union in crisis situations (OJ L 210, 6.8.2008).

(5) In recent years large scale cyber attacks targeted public and private entities alike across many jurisdictions in the Union and beyond, affecting various sectors including transport, health and financial services. Cybercrime and cybersecurity cannot be separated in an interconnected environment. The prevention, investigation and prosecution of such activities is supported by coordination and cooperation between relevant actors, including the European Union Agency for Cybersecurity ('ENISA'), competent authorities for the security of network and information systems ('NIS authorities') as defined by Directive (EU) 2016/1148[4], law enforcement authorities and private parties. In order to ensure the effective cooperation between all relevant actors at Union and national level on cyber attacks and security threats, Europol should cooperate with the ENISA through the exchange of information and by providing analytical support.

(6) High-risk criminals play a leading role in criminal networks and pose a high risk of serious crime to the Union's internal security. To combat high-risk organised crime groups and their leading members, Europol should be able to support Member States in focusing their investigative response on identifying these persons, their criminal activities and the members of their criminal networks.

(7) The threats posed by serious crime require a coordinated, coherent, multi-disciplinary and multi-agency response. Europol should be able to facilitate and support such intelligence-led security initiatives driven by Member States to identify, prioritize and address serious crime threats, such as the European Multidisciplinary Platform Against Criminal Threats. Europol should be able to provide administrative, logistical, financial and operational support to such activities, supporting the identification of cross-cutting priorities and the implementation of horizontal strategic goals in countering serious crime.

---

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1–30).

(8) The Schengen Information System (SIS), established in the field of police cooperation and judicial cooperation in criminal matters by Regulation (EU) 2018/1862 of the European Parliament and of the Council[56], is an essential tool for maintaining a high level of security within the area of freedom, security and justice. Europol, as a hub for information exchange in the Union, receives and holds valuable information from third countries and international organisations on persons suspected to be involved in crimes falling within the scope of Europol's mandate. Following consultation with the Member States, Europol should be able to enter data on these persons in the SIS in order to make it available directly and in real-time to SIS end-users.

(9) Europol has an important role to play in support of the evaluation and monitoring mechanism to verify the application of the Schengen *acquis* as established by Council Regulation (EU) No 1053/2013. Given the need to reinforce the Union's internal security, Europol should contribute with its expertise, analysis, reports and other relevant information to the entire evaluation and monitoring process, from programming to on-site visits and the follow-up. Europol should also assist in developing and updating the evaluation and monitoring tools.

(10) Risk assessments are an essential element of foresight to anticipate new trends and to address new threats in serious crime and terrorism. To support the Commission and the Member States in carrying out effective risk assessments, Europol should provide threats assessment analysis based on the information it holds on criminal phenomena and trends, without prejudice to the EU law provisions on customs risk management.

---

5 Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56–106).

6 Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56–106).

(11) In order to help EU funding for security research to develop its full potential and address the needs of law enforcement, Europol should assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation that are relevant to Europol's objectives. When Europol assists the Commission in identifying key research themes, drawing up and implementing a Union framework programme, it should not receive funding from that programme in accordance with the conflict of interest principle.

(12) It is possible for the Union and the Members States to adopt restrictive measures relating to foreign direct investment on the grounds of security or public order. To that end, Regulation (EU) 2019/452 of the European Parliament and of the Council[7] establishes a framework for the screening of foreign direct investments into the Union that provides Member States and the Commission with the means to address risks to security or public order in a comprehensive manner. As part of the assessment of expected implications for security or public order, Europol should support the screening of specific cases of foreign direct investments into the Union that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes.

(13) Europol provides specialised expertise for countering serious crime and terrorism. Upon request by a Member State, Europol staff should be able to provide operational support to that Member State's law enforcement authorities on the ground in operations and investigations, in particular by facilitating cross-border information exchange and providing forensic and technical support in operations and investigations, including in the context of joint investigation teams. Upon request by a Member State, Europol staff should be entitled to be present when investigative measures are taken in that Member State and assist in the taking of these investigative measures. Europol staff should not have the power to execute investigative measures.

---

[7] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (OJ L 79I , 21.3.2019, p. 1–14).

(14) One of Europol's objectives is to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combatting forms of crime which affect a common interest covered by a Union policy. To strengthen that support, Europol should be able to request the competent authorities of a Member State to initiate, conduct or coordinate a criminal investigation of a crime, which affects a common interest covered by a Union policy, even where the crime concerned is not of a cross-border nature. Europol should inform Eurojust of such requests.

(15) Publishing the identity and certain personal data of suspects or convicted individuals, who are wanted based on a Member State's judicial decision, increases the chances of locating and arresting such individuals. To support Member States in this task, Europol should be able to publish on its website information on Europe's most wanted fugitives for criminal offences in respect of which Europol is competent, and facilitate the provision of information by the public on these individuals.

(16) To ensure that processing of personal data by Europol is limited to the categories of data subjects whose data may be processed under this Regulation, Europol should be able to verify if personal data received in the context of preventing and countering crimes falling within the scope of Europol's objectives corresponds to one of those categories of data subjects. To that end, Europol should be able to carry out a pre-analysis of personal data received with the sole purpose of determining whether such data falls into those categories of data subjects. To this end, Europol should be able to filter the data by checking it against data already held by Europol. Such pre-analysis should take place prior to Europol's data processing for cross-checking, strategic analysis, operational analysis or exchange of information. If the pre-analysis indicates that personal data does not fall into the categories of data subjects whose data may be processed under this Regulation, Europol should delete that data.

(17) Data collected in criminal investigations have been increasing in size and have become more complex. Member States submit large and complex datasets to Europol, requesting Europol's operational analysis to detect links to other crimes and criminals in other Member States and outside the Union. Member States cannot detect such cross-border links through their own analysis of the data. Europol should be able to support Member States' criminal investigations by processing large and complex datasets to detect such cross-border links where the strict requirements set out in this Regulation are fulfilled. Where necessary to support effectively a specific criminal investigation in a Member State, Europol should be able to process those data sets that national authorities have acquired in the context of that criminal investigation in accordance with procedural requirements and safeguards applicable under their national criminal law and subsequently submitted to Europol. Where a Member State provides Europol with an investigative case file requesting Europol's support for a specific criminal investigation, Europol should be able to process all data contained in that file for as long as it supports that specific criminal investigation. Europol should also be able to process personal data that is necessary for its support to a specific criminal investigation in a Member State if that data originates from a third country, provided that the third country is subject to a Commission decision finding that the country ensures an adequate level of data protection ('adequacy decision'), or, in the absence of an adequacy decision, an international agreement concluded by the Union pursuant to Article 218 TFEU, or a cooperation agreement allowing for the exchange of personal data concluded between Europol and the third country prior to the entry into force of Regulation (EU) 2016/794, and provided that the third county acquired the data in the context of a criminal investigation in accordance with procedural requirements and safeguards applicable under its national criminal law.

(18) To ensure that any data processing is necessary and proportionate, Member States should ensure compliance with national and Union law when they submit an investigative case file to Europol. Europol should verify whether, in order to support a specific criminal investigation, it is necessary and proportionate to process personal data that may not fall into the categories of data subjects whose data may generally be processed under Annex II of Regulation (EU) 2016/794. Europol should document that assessment. Europol should store such data with functional separation from other data and should only process it where necessary for its support to the specific criminal investigation, such as in case of a new lead.

(19) To ensure that a Member State can use Europol's analytical reports as part of judicial proceedings following a criminal investigation, Europol should be able to store the related investigative case file upon request of that Member State for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process. Europol should store such data separately and only for as long as the judicial proceedings related to that criminal investigation are on-going in the Member State. There is a need to ensure access of competent judicial authorities as well as the rights of defence, in particular the right of suspects or accused persons or their lawyers of access to the materials of the case.

(20) Cross-border cases of serious crime or terrorism require close collaboration between the law enforcement authorities of the Member States concerned. Europol provides tools to support such cooperation in investigations, notably through the exchange of information. To further enhance such cooperation in specific investigations by way of joint operational analysis, Member States should be able to allow other Member States to access directly the information they provided to Europol, without prejudice to any restrictions they put on access to that information. Any processing of personal data by Member States in joint operational analysis should take place in accordance with the rules and safeguards set out in this Regulation.

(21) Europol provides operational support to the criminal investigations of the competent authorities of the Member States, especially by providing operational and forensic analysis. Member States should be able to make the results of these activities available to their relevant other authorities, including prosecutors and criminal courts, throughout the whole lifecycle of criminal proceedings]. To that end, Europol staff should be enabled to give evidence, which came to their knowledge in the performance of their duties or the exercise of their activities, in criminal proceedings, without prejudice to the applicable use restrictions and national criminal procedural law.

(22) Europol and the European Public Prosecutor's Office ('EPPO') established by Council Regulation (EU) 2017/1939[8], should put necessary arrangements in place to optimise their operational cooperation, taking due account of their respective tasks and mandates. Europol should work closely with the EPPO and actively support the investigations and prosecutions of the EPPO upon its request, including by providing analytical support and exchanging relevant information, as well as cooperate with it, from the moment a suspected offence is reported to the EPPO until the moment it determines whether to prosecute or otherwise dispose of the case. Europol should, without undue delay, report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence. To enhance operational cooperation between Europol and the EPPO, Europol should enable the EPPO to have access, on the basis of a hit/no hit system, to data available at Europol, in accordance with the safeguards and data protection guarantees provided for in this Regulation. The rules on the transmission to Union bodies set out in this Regulation should apply to Europol's cooperation with the EPPO. Europol should also be able to support criminal investigations by the EPPO by way of analysis of large and complex datasets.

---

8 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (OJ L 283, 31.10.2017, p. 1–71).

(23) Europol should cooperate closely with the European Anti-Fraud Office (OLAF) to detect fraud, corruption and any other illegal activity affecting the financial interests of the Union. To that end, Europol should transmit to OLAF without delay any information in respect of which OLAF could exercise its competence. The rules on the transmission to Union bodies set out in this Regulation should apply to Europol's cooperation with OLAF.

(24) Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects. To reinforce cooperation with third countries in preventing and countering crimes falling within the scope of Europol's objectives, the Executive Director of Europol should be allowed to authorise categories of transfers of personal data to third countries in specific situations and on a case-by-case basis, where such a group of transfers related to a specific situation are necessary and meet all the requirements of this Regulation.

(25) To support Member States in cooperating with private parties providing cross-border services where those private parties hold information relevant for preventing and combatting crime, Europol should be able to receive, and in specific circumstances, exchange personal data with private parties.

(26) Criminals increasingly use cross-border services of private parties to communicate and carry out illegal activities. Sex offenders abuse children and share pictures and videos world-wide using online platforms on the internet. Terrorists abuse cross-border services by online service providers to recruit volunteers, plan and coordinate attacks, and disseminate propaganda. Cyber criminals profit from the digitalisation of our societies using phishing and social engineering to commit other types of cybercrime such as online scams, ransomware attacks or payment fraud. As a result from the increased use of online services by criminals, private parties hold increasing amounts of personal data that may be relevant for criminal investigations.

(27) Given the borderless nature of the internet, these services can often be provided from anywhere in the world. As a result, victims, perpetrators, and the digital infrastructure in which the personal data is stored and the service provider providing the service may all be subject to different national jurisdictions, within the Union and beyond. Private parties may therefore hold data sets relevant for law enforcement which contain personal data with links to multiple jurisdictions as well as personal data which cannot easily be attributed to any specific jurisdiction. National authorities find it difficult to effectively analyse such multi-jurisdictional or non-attributable data sets through national solutions. When private parties decide to lawfully and voluntarily share the data with law enforcement authorities, they do currently not have a single point of contact with which they can share such data sets at Union-level. Moreover, private parties face difficulties when receiving multiple requests from law enforcement authorities of different countries.

(28) To ensure that private parties have a point of contact at Union level to lawfully share multi-jurisdictional data sets or data sets that could not be easily attributed so far to one or several specific jurisdictions, Europol should be able to receive personal data directly from private parties.

(29) To ensure that Member States receive quickly the relevant information necessary to initiate investigations to prevent and combat serious crime and terrorism, Europol should be able to process and analyse such data sets in order to identify the relevant Member States and forward to the national law enforcement authorities concerned the information and analysis necessary to investigate these crimes under their respective jurisdictions.

(30) To ensure that it can identify all relevant national law enforcement authorities concerned, Europol should be able to inform private parties when the information received from them is insufficient to enable Europol to identify the law enforcement authorities concerned. This would enable private parties which have shared information with Europol to decide whether it is in their interest to share additional information with Europol and whether they can lawfully do so. To this end, Europol can inform private parties of missing information, as far as this is strictly necessary for the identification of the relevant law enforcement authorities. Special safeguards should apply to such transfers in particular when the private party concerned is not established within the Union or in a third country with which Europol has a cooperation agreement allowing for the exchange of personal data, or with which the Union has concluded an international agreement pursuant to Article 218 TFEU providing for appropriate safeguards, or which is the subject of an adequacy decision by the Commission, finding that the third country in question ensures an adequate level of data protection.

(31) Member States, third countries, international organisation, including the International Criminal Police Organisation (Interpol), or private parties may share multi-jurisdictional data sets or data sets that cannot be attributed to one or several specific jurisdictions with Europol, where those data sets contain links to personal data held by private parties. Where it is necessary to obtain additional information from such private parties to identify all relevant Member States concerned, Europol should be able to ask Member States, via their national units, to request private parties which are established or have a legal representative in their territory to share personal data with Europol in accordance with those Member States' applicable laws. In many cases, these Member States may not be able to establish a link to their jurisdiction other than the fact that the private party holding the relevant data is established under their jurisdiction. Irrespective of their jurisdiction with regard the specific criminal activity subject to the request, Member States should therefore ensure that their competent national authorities can obtain personal data from private parties for the purpose of supplying Europol with the information necessary for it to fulfil its objectives, in full compliance with procedural guarantees under their national laws.

(32) To ensure that Europol does not keep the data longer than necessary to identify the Member States concerned, time limits for the storage of personal data by Europol should apply. Once Europol has exhausted all means at its disposal to identify all Member States concerned, and cannot reasonably expect to identify further Member States concerned, the storage of this personal data is no longer necessary and proportionate for identifying the Member States concerned. Europol should erase the personal data within four months after the last transmission has taken place, unless a national unit, contact point or authority concerned resubmits the personal data as their data to Europol within this period. If the resubmitted personal data has been part of a larger set of personal data, Europol should only keep the personal data if and in so far as it has been resubmitted by a national unit, contact point or authority concerned.

(33) Any cooperation of Europol with private parties should neither duplicate nor interfere with the activities of the Financial Intelligence Units ('FIUs'), and should only concern information that is not already to be provided to FIUs in accordance with Directive 2015/849 of the European Parliament and of the Council[9]. Europol should continue to cooperate with FIUs in particular via the national units.

(34) Europol should be able to provide the necessary support for national law enforcement authorities to interact with private parties, in particular by providing the necessary infrastructure for such interaction, for example, when national authorities refer terrorist content online to online service providers or exchange information with private parties in the context of cyber attacks. Where Member States use the Europol infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol should not have access to that data.

---

[9] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).

(35) Terrorist attacks trigger the large scale dissemination of terrorist content via online platforms depicting harm to life or physical integrity, or calling for imminent harm to life or physical integrity. To ensure that Member States can effectively prevent the dissemination of such content in the context of such crisis situations stemming from ongoing or recent real-world events, Europol should be able to exchange personal data with private parties, including hashes, IP addresses or URLs related to such content, necessary in order to support Member States in preventing the dissemination of such content, in particular where this content aims at or has the effect of seriously intimidating a population, and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers.

(36) Regulation (EU) 2018/1725 of the European Parliament and of the Council[10][11]sets out rules on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies but it did not apply to Europol. To ensure uniform and consistent protection of natural persons with regard to the processing of personal data, Regulation (EU) 2018/1725 should be made applicable le to Europol in accordance with Article 2(2) of that Regulation, and should be complemented by specific provisions for the specific processing operations that Europol should perform to accomplish its tasks.

---

10 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

11 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

(37) Given the challenges that the use of new technologies by criminals pose to the Union's security, law enforcement authorities are required to strengthen their technological capacities. To that end, Europol should support Member States in the use of emerging technologies in preventing and countering crimes falling within the scope of Europol's objectives. To explore new approaches and develop common technological solutions for Member States to prevent and counter crimes falling within the scope of Europol's objectives, Europol should be able to conduct research and innovation activities regarding matters covered by this Regulation, including with the processing of personal data where necessary and whilst ensuring full respect for fundamental rights. The provisions on the development of new tools by Europol should not constitute a legal basis for their deployment at Union or national level.

(38) Europol should play a key role in assisting Member States to develop new technological solutions based on artificial intelligence, which would benefit national law enforcement authorities throughout the Union. Europol should play a key role in promoting ethical, trustworthy and human centric artificial intelligence subject to robust safeguards in terms of security, safety and fundamental rights.

(39) Europol should inform the European Data Protection Supervisor prior to the launch of its research and innovation projects that involve the processing of personal data. For each project, Europol should carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data and all other fundamental rights, including of any bias in the outcome. This should include an assessment of the appropriateness of the personal data to be processed for the specific purpose of the project. Such an assessment would facilitate the supervisory role of the European Data Protection Supervisor, including the exercise of its corrective powers under this Regulation which might also lead to a ban on processing. The development of new tools by Europol should be without prejudice to the legal basis, including grounds for processing the personal data concerned, that would subsequently be required for their deployment at Union or national level.

(40) Providing Europol with additional tools and capabilities requires reinforcing the democratic oversight and accountability of Europol. Joint parliamentary scrutiny constitutes an important element of political monitoring of Europol's activities. To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny Group with annual information on the use of these tools and capabilities and the result thereof.

(41) Europol's services provide added value to Member States and third countries. This includes Member States that do not take part in measures pursuant to Title V of Part Three of the Treaty on the Functioning of the European Union. Member States and third countries may contribute to Europol's budget based on separate agreements. Europol should therefore be able to receive contributions from Member States and third countries on the basis of financial agreements within the scope of its objectives and tasks.

(42) Since the objective of this Regulation, namely to support and strengthen action by the Member States' law enforcement services 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, cannot be sufficiently achieved by the Member States but can rather, due to the cross-border nature of serious crime and terrorism and the need for a coordinated response to related security threats, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(43) [In accordance with Article 3 of the Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and the Treaty on the Functioning of the European Union, Ireland has notified its wish to take part in the adoption and application of this Regulation.] OR [In accordance with Articles 1 and 2 of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.]

(44) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(45) The European Data Protection Supervisor was consulted, in accordance with Article 41(2) of Regulation (EU) 2018/1725 of the European Parliament and the Council, and has delivered an opinion on [...].

(46) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, in particular the right to the protection of personal data and the right to privacy as protected by Articles 8 and 7 of the Charter, as well as by Article 16 TFEU. Given the importance of the processing of personal data for the work of law enforcement in general, and for the support provided by Europol in particular, this Regulation includes effective safeguards to ensure full compliance with fundamental rights as enshrined in the Charter of Fundamental Rights. Any processing of personal data under this Regulation is limited to what is strictly necessary and proportionate, and subject to clear conditions, strict requirements and effective supervision by the EDPS.

(47) Regulation (EU) 2016/794 should therefore be amended accordingly,

HAVE ADOPTED THIS REGULATION:

Article 1

Regulation (EU) 2016/794 is amended as follows:

(1) Article 2 is amended as follows:

(a) points (h) to (k) and points (m), (n) and (o) are deleted;

(b) point (p) is replaced by the following:

"(p) 'administrative personal data' means all personal data processed by Europol apart from operational data;";

(c) the following point (q) is added:

"(q) 'investigative case file' means a dataset or multiple datasets that a Member State, the EPPO or a third country acquired in the context of an on-going criminal investigation, in accordance with procedural requirements and safeguards under the applicable national criminal law, and submitted to Europol in support of that criminal investigation."

(2) Article 4 is amended as follows:

(a) paragraph 1 is amended as follows:

(i) point (h) is replaced by the following:

"(h) support Member States' cross-border information exchange activities, operations and investigations, as well as joint investigation teams, and special intervention units, including by providing operational, technical and financial support;";

(ii) point (j) is replaced by the following:

“(j) cooperate with the Union bodies established on the basis of Title V of the TFEU and with OLAF and ENISA, in particular through exchanges of information and by providing them with analytical support in the areas that fall within their competence;”;

(iii) point (m) is replaced by the following:

“(m) support Member States’ actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States, the coordination of law enforcement authorities’ response to cyberattacks, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;”;

(iv) the following points (q) to (r) are added:

“(q) support Member States in identifying persons whose involvement in crimes falling within the scope of Europol’s mandate, as listed in Annex I, constitute a high risk for security, and facilitate joint, coordinated and prioritised investigations;

(r) enter data into the Schengen Information System, in accordance with Regulation (EU) 2018/1862 of the European Parliament and of the Council*, following consultation with the Member States in accordance with Article 7 of this Regulation, and under authorisation by the Europol Executive Director, on the suspected involvement of a third country national in an offence in respect of which Europol is competent and of which it is aware on the basis of information received from third countries or international organisations within the meaning of Article 17(1)(b);

(s) support the implementation of the evaluation and monitoring mechanism under Regulation (EU) No 1053/2013 within the scope of Europol’s objectives as set out in Article 3;

(t) proactively monitor and contribute to research and innovation activities relevant to achieve the objectives set out in Article 3, support related activities of Member States, and implement its research and innovation activities regarding matters covered by this Regulation, including the development, training, testing and validation of algorithms for the development of tools.

(u) support Member States' actions in preventing the dissemination of online content related to terrorism or violent extremism in crisis situations, which stems from an ongoing or recent real- world event, depicts harm to life or physical integrity or calls for imminent harm to life or physical integrity, and aims at or has the effect of seriously intimidating a population, and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers.

_____

* Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).";

(b) in paragraph 2, the second sentence is replaced by the following:

"Europol shall also assist in the operational implementation of those priorities, notably in the European Multidisciplinary Platform Against Criminal Threats, including by facilitating and providing administrative, logistical, financial and operational support to Member States-led operational and strategic activities.";

(c) in paragraph 3, the following sentence is added:

"Europol shall also provide threats assessment analysis supporting the Commission and the Member States in carrying out risk assessments.";

(d) the following paragraphs 4a and 4b are inserted:

"4a. Europol shall assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation activities that are relevant to achieve the objectives set out in Article 3. When Europol assists the Commission in

identifying key research themes, drawing up and implementing a Union framework programme, the Agency shall not receive funding from that programme.

4b. Europol shall support the screening of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council* that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Article 3 on the expected implications for security.

_____

* Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (OJ L 79I , 21.3.2019, p. 1).”

(e) in paragraph 5, the following sentence is added:

“Europol staff may assist the competent authorities of the Member States, at their request and in accordance with their national law, in the taking of investigative measures.”

(3) in Article 6, paragraph 1 is replaced by the following:

“1. In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the Member State or Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation.”

(4) In Article 7, paragraph 8 is replaced by the following:

“8. Member States shall ensure that their financial intelligence units established pursuant to Directive (EU) 2015/849 of the European Parliament and of the Council* are allowed to cooperate with Europol in accordance with Article 12 of Directive (EU) 2019/1153 of the European Parliament and the Council**, in particular via their national unit regarding financial information and analyses, within the limits of their mandate and competence.

_____

* Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).

** Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (OJ L 186, 11.7.2019, p. 122).”

(5) Article 18 is amended as follows:

(a) paragraph 2 is amended as follows:

(i) point (d) is replaced by the following wording:

“(d) facilitating the exchange of information between Member States, Europol, other Union bodies, third countries, international organisations and private parties;”

(ii), the following points (e) and (f) are added:

“(e) research and innovation regarding matters covered by this Regulation for the development, training, testing and validation of algorithms for the development of tools;

(f) supporting Member States in informing the public about suspects or convicted individuals who are wanted based on a national judicial decision relating to a criminal offence in respect of

which Europol is competent, and facilitate the provision of information by the public on these individuals."

(b) the following paragraph 3a is inserted:

"3a. Processing of personal data for the purpose of research and innovation as referred to in point (e) of paragraph 2 shall be performed by means of Europol's research and innovation projects with clearly defined objectives, duration and scope of the personal data processing involved, in respect of which the additional specific safeguards set out in Article 33a shall apply."

(c) paragraph 5 is replaced by the following:

"5. Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in paragraph 2 are listed in Annex II."

(d) the following paragraph 5a is inserted:

"5a. Prior to the processing of data under paragraph 2 of this Article, Europol may temporarily process personal data received pursuant to Article 17(1) and (2) for the purpose of determining whether such data comply with the requirements of paragraph 5 of this Article, including by checking the data against all data that Europol already processes in accordance with paragraph 5.

The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data.

Europol may only process personal data pursuant to this paragraph for a maximum period of one year, or in justified cases for a longer period with the prior authorisation of the EDPS, where necessary for the purpose of this Article. Where the result of the processing indicates that personal data do not comply with the requirements of paragraph 5 of this Article, Europol shall delete that data and inform the provider of the data accordingly."

(6) The following Article 18a is inserted:

"Article 18a

Information processing in support of a criminal investigation

1. Where necessary for the support of a specific criminal investigation, Europol may process personal data outside the categories of data subjects listed in Annex II where:

(a) a Member State or the EPPO provides an investigative case file to Europol pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol pursuant to point (c) of Article 18(2); and

(b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case file without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded.

2. Europol may process personal data contained in an investigative case for as long as it supports the on-going specific criminal investigation for which the investigative case file was provided by a Member State or the EPPO in accordance with paragraph 1, and only for the purpose of supporting that investigation.

The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data.

Without prejudice to the processing of personal data under Article 18(5a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be accessed where necessary for the support of the specific criminal investigation for which they were provided.

3. Upon request of the Member State or the EPPO that provided an investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to that criminal investigation are on-going in that Member State.

That Member State may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as judicial proceedings following a related criminal investigation are on-going in another Member State.

The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Such personal data shall be functionally separated from other data and may only be accessed where necessary for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process.

4. Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports. Where a third country provides an investigative case file to Europol, the EDPS shall be informed. Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights. Where Europol, or the EDPS, reaches the conclusion that there are preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not process it. Data processed pursuant to this paragraph may only be accessed by Europol where necessary for the support of the specific criminal investigation in a Member State or in Member States. It shall be shared only within the Union.”;

(7) Article 20 is amended as follows:

(a) the following paragraph 2a is inserted:

“2a. In the framework of conducting dedicated operational analysis projects as referred to in Article 18(3), Member States may determine information to be made directly accessible by Europol to selected other Member States for the purpose of enhanced collaboration in specific investigations, without prejudice to any restrictions of Article 19(2).”;

(b) in paragraph 3, the introductory phrase is replaced by the following:

“3. In accordance with national law, the information referred to in paragraphs 1, 2 and 2a shall be accessed and further processed by Member States only for the purpose of preventing and combating, and for judicial proceedings related to:”;

(c) the following paragraph 5 is added:

“5. When national law allows for Europol staff to provide evidence which came to their knowledge in the performance of their duties or the exercise of their activities, only Europol staff authorised by the Executive Director to do so shall be able to give such evidence in judicial proceedings in the Member States.”;

(8) The following Article 20a is inserted:

“Article 20a

Relations with the European Public Prosecutor’s Office

1. Europol shall establish and maintain a close relationship with the European Public Prosecutor’s Office (EPPO). In the framework of that relationship, Europol and the EPPO shall act within their respective mandate and competences. To that end, they shall conclude a working arrangement setting out the modalities of their cooperation.

2. Europol shall actively support the investigations and prosecutions of the EPPO and cooperate with it, in particular through exchanges of information and by providing analytical support.

3. Europol shall take all appropriate measures to enable the EPPO to have indirect access to information provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system. Article 21 shall apply mutatis mutandis with the exception of its paragraph 2.

4. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence."

(9) In Article 21, the following paragraph 8 is added:

"8. If during information-processing activities in respect of an individual investigation or specific project Europol identifies information relevant to possible illegal activity affecting the financial interest of the Union, Europol shall on its own initiative without undue delay provide OLAF with that information."

(10) Article 24 is replaced by the following:

"Article 24

Transmission of operational personal data to Union institutions, bodies, offices and agencies

1. Subject to any further restrictions pursuant to this Regulation, in particular pursuant to Article 19(2) and (3) and without prejudice to Article 67, Europol shall only transmit operational personal data to another Union institution, body, office or agency if the data are necessary for the legitimate performance of tasks of the other Union institution, body, office or agency.

2. Where the operational personal data are transmitted following a request from another Union institution, body, office or agency, both the controller and the recipient shall bear the responsibility for the lawfulness of that transmission.

Europol shall verify the competence of the other Union institution, body, office or agency . If doubts arise as to this necessity of the transmission of the personal data, Europol shall seek further information from the recipient.

The recipient Union institution, body, office or agency shall ensure that the necessity of the transmission of the operational personal data can be subsequently verified.

3. The recipient Union institution, body, office or agency shall process the operational personal data only for the purposes for which they were transmitted."

(11) Article 25 is amended as follows:

(a) In paragraph 5, the introductory phrase is replaced by the following:

"By way of derogation from paragraph 1, the Executive Director may authorise the transfer or categories of transfers of personal data to third countries or international organisations on a case-by-case basis if the transfer is, or the related transfers are:";

(b) In paragraph 8, the following sentence is deleted:

"Where a transfer is based on paragraph 5, such a transfer shall be documented and the documentation shall be made available to the EDPS on request. The documentation shall include a record of the date and time of the transfer, and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred."

(12) Article 26 is amended as follows:

(a) paragraph 2 is replaced by the following:

“2. Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 in order to identify all national units concerned, as referred to in point (a) of paragraph 1. Europol shall forward the personal data and any relevant results from the processing of that data necessary for the purpose of establishing jurisdiction immediately to the national units concerned. Europol may forward the personal data and relevant results from the processing of that data necessary for the purpose of establishing jurisdiction in accordance with Article 25 to contact points and authorities concerned as referred to in points (b) and (c) of paragraph 1. Once Europol has identified and forwarded the relevant personal data to all the respective national units concerned, or it is not possible to identify further national units concerned, it shall erase the data, unless a national unit, contact point or authority concerned resubmits the personal data to Europol in accordance with Article 19(1) within four months after the transfer takes place.”

(b) paragraph 4 is replaced by the following:

“4. If Europol receives personal data from a private party in a third country, Europol may forward those data only to a Member State, or to a third country concerned with which an agreement on the basis of Article 23 of Decision 2009/371/JHA or on the basis of Article 218 TFEU has been concluded or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation. Where the conditions set out under paragraphs 5 and 6 of Article 25 are fulfilled, Europol may transfer the result of its analysis and verification of such data with the third country concerned.”

(c) paragraphs 5 and 6 are replaced by the following:

"5. Europol may transmit or transfer personal data to private parties on a case-by-case basis, where it is strictly necessary, and subject to any possible restrictions stipulated pursuant to Article 19(2) or (3) and without prejudice to Article 67, in the following cases:

(a) the transmission or transfer is undoubtedly in the interests of the data subject, and either the data subject has given his or her consent; or

(b) the transmission or transfer is absolutely necessary in the interests of preventing the imminent perpetration of a crime, including terrorism, for which Europol is competent; or

(c) the transmission or transfer of personal data which are publicly available is strictly necessary for the performance of the task set out in point (m) of Article 4(1) and the following conditions are met:

(i) the transmission or transfer concerns an individual and specific case;

(ii) no fundamental rights and freedoms of the data subjects concerned override the public interest necessitating the transmission or transfer in the case at hand; or

(d) the transmission or transfer of personal data is strictly necessary for Europol to inform that private party that the information received is insufficient to enable Europol to identify the national units concerned, and the following conditions are met:

(i) the transmission or transfer follows a receipt of personal data directly from a private party in accordance with paragraph 2 of this Article;

(ii) the missing information, which Europol may refer to in these notifications, has a clear link with the information previously shared by that private party;

(iii) the missing information, which Europol may refer to in these notifications, is strictly limited to what is necessary for Europol to identify the national units concerned.

6. With regard to points (a), (b) and (d) of paragraph 5 of this Article, if the private party concerned is not established within the Union or in a country with which Europol has a cooperation agreement allowing for the exchange of personal data, with which the Union has concluded an international agreement pursuant to Article 218 TFEU or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, the transfer shall only be authorised by the Executive Director if the transfer is:

(a) necessary in order to protect the vital interests of the data subject or another person; or

(b) necessary in order to safeguard legitimate interests of the data subject; or

(c) essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or

(d) necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences for which Europol is competent; or

(e) necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence for which Europol is competent.

Personal data shall not be transferred if the Executive Director determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer referred to in points (d) and (e).

Transfers shall not be systematic, massive or structural."

(d) the following paragraphs 6a and 6b are inserted:

"6a. Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned.

Irrespective of their jurisdiction over the specific crime in relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives.

6b. Europol's infrastructure may be used for exchanges between the competent authorities of Member States and private parties in accordance with the respective Member States' national laws. In cases where Member States use this infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol shall not have access to that data."

(e) paragraphs 9 and 10 are deleted;

(13) the following Article 26a is inserted:

"Article 26a

Exchanges of personal data with private parties in crisis situations

1. Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 to prevent the dissemination of online content related to terrorism or violent extremism in crisis situations as set out in point (u) of Article 4(1).

2. If Europol receives personal data from a private party in a third country, Europol may forward those data only to a Member State, or to a third country concerned with which an agreement on the basis of Article 23 of Decision 2009/371/JHA or on the basis of Article 218 TFEU has been concluded or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation. Where the conditions set out under paragraphs 5 and 6 of Article 25 are fulfilled, Europol may transfer the result of its analysis and verification of such data with the third country concerned.

3. Europol may transmit or transfer personal data to private parties, on a case-by-case basis, subject to any possible restrictions stipulated pursuant to Article 19(2) or (3) and without prejudice to Article 67, where the transmission or transfer of such data is strictly necessary for preventing the dissemination of online content related to terrorism or violent extremism as set out in point (u) of Article 4(1), and no fundamental rights and freedoms of the data subjects concerned override the public interest necessitating the transmission or transfer in the case at hand.

4. If the private party concerned is not established within the Union or in a country with which Europol has a cooperation agreement allowing for the exchange of personal data, with which the Union has concluded an international agreement pursuant to Article 218 TFEU or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, the transfer shall be authorised by the Executive Director.

5. Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol for preventing the dissemination of online content related to terrorism or violent extremism as set out in point (u) of Article 4(1). Irrespective of their jurisdiction with regard to the dissemination of the content in relation to which Europol requests the personal data, Member States shall ensure that the competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives.

6. Europol shall ensure that detailed records of all transfers of personal data and the grounds for such transfers are recorded in accordance with this Regulation and communicated upon request to the EDPS pursuant to Article 40.

7. If the personal data received or to be transferred affect the interests of a Member State, Europol shall immediately inform the national unit of the Member State concerned."

(14) the following Article 27a is inserted:

"Article 27a

Processing of personal data by Europol

1. This Regulation, Article 3 and Chapter IX of Regulation (EU) 2018/1725 of the European Parliament and of the Council* shall apply to the processing of operational personal data by Europol.

Regulation (EU) 2018/1725, with the exception of its Chapter IX, shall apply to the processing of administrative personal data by Europol.

2. References to 'applicable data protection rules' in this Regulation shall be understood as references to the provisions on data protection set out in this Regulation and in Regulation (EU) 2018/1725.

3. References to 'personal data' in this Regulation shall be understood as references to 'operational personal data', unless indicated otherwise.

4. Europol shall determine the time limits for the storage of administrative personal data in its rules of procedure.

_____

* Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).”

(15) Article 28 is deleted;

(16) Article 30 is amended as follows:

(a) in paragraph 2, the first sentence is replaced by the following:

“2. Processing of personal data, by automated or other means, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data and biometric data for the purpose of uniquely identifying a natural person or data concerning a person’s health or sex life or sexual orientation shall be allowed only where strictly necessary and proportionate for preventing or combating crime that falls within Europol’s objectives and if those data supplement other personal data processed by Europol.”;

(b) in paragraph 3, the first sentence is replaced by the following:

“Only Europol shall have direct access to personal data as referred to in paragraphs 1 and 2, except for the cases outlined in Article 20 (2a).”

(c) paragraph 4 is deleted;

(d) paragraph 5 is replaced by the following:

"5. Personal data as referred to in paragraphs 1 and 2 shall not be transmitted to Member States, Union bodies, or transferred to third countries and international organisations unless such transmission or transfer is strictly necessary and proportionate in individual cases concerning crimes that falls within Europol's objectives and in accordance with Chapter V.";

(17) Article 32 is replaced by the following:

"Article 32

Security of processing

Europol and Member States shall establish mechanisms to ensure that security measures referred to in Article 91 of Regulation (EU) 2018/1725 are addressed across information system boundaries.";

(18) Article 33 is deleted;

(19) the following Article 33a is inserted:

"Article 33a

Processing of personal data for research and innovation

1. For the processing of personal data performed by means of Europol's research and innovation projects as referred to in point (e) of Article 18(2), the following additional safeguards shall apply:

(a) any project shall be subject to prior authorisation by the Executive Director, based on a description of the envisaged processing activity setting out the necessity to process personal data, such as for exploring and testing innovative solutions and ensuring accuracy of the project results, a description of the personal data to be processed, a description of the retention period and conditions for access to the personal data, a data protection impact assessment of the risks to all rights and freedoms of data subjects, including of any bias in the outcome, and the measures envisaged to address those risks;

(b) (b) the Management Board and the EDPS shall be informed prior to the launch of the project; (c) any personal data to be processed in the context of the project shall be temporarily copied to a separate, isolated and protected data processing environment within Europol for the sole purpose of carrying out that project and only authorised staff of Europol shall have access to that data;

(c) (d) any personal data processed in the context of the project shall not be transmitted, transferred or otherwise accessed by other parties;

(d) (e) any processing of personal data in the context of the project shall not lead to measures or decisions affecting the data subjects;

(e) (f) any personal data processed in the context of the project shall be deleted once the project is concluded or the personal data has reached the end of its retention period in accordance with Article 31;

(f) (g) the logs of the processing of personal data in the context of the project shall be kept for the duration of the project and 1 year after the project is concluded, solely for the purpose of and only as long as necessary for verifying the accuracy of the outcome of the data processing.

3. Europol shall keep a complete and detailed description of the process and rationale behind the training, testing and validation of algorithms to ensure transparency and for verification of the accuracy of the results.";

(20) Article 34 is amended as follows:

(a) paragraph 1 is replaced by the following:

"1. In the event of a personal data breach, Europol shall without undue delay notify the competent authorities of the Member States concerned, of that breach, in accordance with the conditions laid down in Article 7(5), as well as the provider of the data concerned unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.";

(b) paragraph 3 is deleted;

(21) Article 35 is amended as follows:

(a) paragraphs 1 and 2 are deleted;

(b) in paragraph 3, the first sentence is replaced by the following:

“Without prejudice to Article 93 of Regulation 2018/1725, if Europol does not have the contact details of the data subject concerned, it shall request the provider of the data to communicate the personal data breach to the data subject concerned and to inform Europol about the decision taken.“;

(b) paragraphs 4 and 5 are deleted.”;

(22) Article 36 is amended as follows:

(a) paragraphs 1 and 2 are deleted;

(b) paragraph 3 is replaced by the following:

“3. Any data subject wishing to exercise the right of access referred to in Article 80 of Regulation (EU) 2018/1725 to personal data that relate to the data subject may make a request to that effect, without incurring excessive costs, to the authority appointed for that purpose in the Member State of his or her choice, or to Europol. Where the request is made to the Member State authority, that authority shall refer the request to Europol without delay, and in any case within one month of receipt.”;

(c) paragraphs 6 and 7 are deleted(1)

(23) Article 37 is amended as follows:

(a) paragraph 1 is replaced by the following:

“1. Any data subject wishing to exercise the right to rectification or erasure of personal data or of restriction of processing referred to in Article 82 of Regulation (EU) 2018/1725 of personal data that relate to him or her may make a request to that effect, through the authority appointed for that purpose in the Member State of his or her choice, or to Europol. Where the request is made to the Member State authority, that authority shall refer the request to Europol without delay and in any case within one month of receipt.”;

(b) paragraph 2 is deleted;

(c) in paragraph 3, the first sentence is replaced by the following:

“Without prejudice to Article 82(3) of Regulation 2018/1725, Europol shall restrict rather than erase personal data as referred to in paragraph 2 if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject.”;

(d) paragraphs 8 and 9 are deleted.”;

(24) the following Article 37a is inserted:

“*Article 37a*

Right to restriction of processing

Where the processing of personal data has been restricted under Article 82(3) of Regulation (EU) 2018/1725, such personal data shall only be processed for the protection of the rights of the data subject or another natural or legal person or for the purposes laid down in Article 82(3) of that Regulation.”;

(25) Article 38 is amended as follows:

(a) paragraph 4 is replaced by the following:

“4. Responsibility for compliance with Regulation (EU) 2018/1725 in relation to administrative personal data and for compliance with this Regulation and with Article 3 and Chapter IX of Regulation (EU) 2018/1725 in relation to operational personal data shall lie with Europol.”;

(b) in paragraph 7 the third sentence is replaced by the following:

“The security of such exchanges shall be ensured in accordance with Article 91 of Regulation (EU) 2018/1725”;

(26) Article 39 is amended as follows:

(a) paragraph 1 is replaced by the following:

“1. Without prejudice to Article 90 of Regulation (EU) 2018/1725, any new type of processing operations to be carried out shall be subject to prior consultation of the EDPS where special categories of data as referred to in Article 30(2) of this Regulation are to be processed.”;

(b) paragraphs 2 and 3 are deleted;

(27) The following Article 39a in inserted:

"*Article 39a*

Records of categories of processing activities

1. Europol shall maintain a record of all categories of processing activities under its responsibility. That record shall contain the following information:

(a) Europol's contact details and the name and the contact details of its Data Protection Officer;

(b) the purposes of the processing;

(c) the description of the categories of data subjects and of the categories of operational personal data;

(d) the categories of recipients to whom the operational personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of operational personal data to a third country, an international organisation, or private party including the identification of that third country, international organisation or private party;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 91 of Regulation (EU) 2018/1725.

2. The records referred to in paragraph 1 shall be in writing, including in electronic form.

3. Europol shall make the records referred to in paragraph 1 available to the EDPS on request.";

(28) Article 40 is amended as follows:

(a) the title is replaced by the following:

“Logging”

(b) paragraph 1 is replaced by the following:

“1. In line with Article 88 of Regulation (EU) 2018/1725, Europol shall keep logs of its processing operations. There shall be no possibility of modifying the logs.”;

(c) in paragraph 2, the first sentence is replaced by the following:

“Without prejudice to Article 88 of Regulation (EU) 2018/1725, the logs prepared pursuant to paragraph 1, if required for a specific investigation related to compliance with data protection rules, shall be communicated to the national unit concerned.”;

(29) Article 41 is replaced by the following:

“Article 41

Designation of the Data Protection Officer

1. The Management Board shall appoint a Data Protection Officer, who shall be a member of the staff specifically appointed for this purpose. In the performance of his or her duties, he or she shall act independently and may not receive any instructions.

2. The Data Protection Officer shall be selected on the basis of his or her personal and professional qualities and, in particular, the expert knowledge of data protection and practices and the ability to fulfil his or her tasks under this Regulation.

3. The selection of the Data Protection Officer shall not be liable to result in a conflict of interests between his or her duty as Data Protection Officer and any other official duties he or she may have, in particular in relation to the application of this Regulation.

4. The Data Protection Officer shall be designated for a term of four years and shall be eligible for reappointment. The Data Protection Officer may be dismissed from his or her post by the Executive Board only with the agreement of the EDPS, if he or she no longer fulfils the conditions required for the performance of his or her duties

5. After his or her designation, the Data Protection Officer shall be registered with the European Data Protection Supervisor by the Management Board

6. Europol shall publish the contact details of the Data Protection Officer and communicate them to the EDPS.";

(30) the following Articles 41a and 41b are inserted:

"Article 41a

Position of the Data Protection Officer

1. Europol shall ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. Europol shall support the Data Protection Officer in performing the tasks referred to in Article 41c by providing the resources and staff necessary to carry out those tasks and by providing access to personal data and processing operations, and to maintain his or her expert knowledge. The related staff may be supplemented by an assistant DPO in the area of operational and administrative processing of personal data.

3. Europol shall ensure that the Data Protection Officer does not receive any instructions regarding the exercise of those tasks. The Data Protection Officer shall report directly to the Management Board. The Data Protection Officer shall not be dismissed or penalised by the Management Board for performing his or her tasks.

4. Data subjects may contact the Data Protection Officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation and under Regulation (EU) 2018/1725. No one shall suffer prejudice on account of a matter brought to the attention of the Data Protection Officer alleging that a breach of this Regulation or Regulation (EU) 2018/1725 has taken place.

5. The Management Board shall adopt further implementing rules concerning the Data Protection Officer. Those implementing rules shall in particular concern the selection procedure for the position of the Data Protection Officer, his or her dismissal, tasks, duties and powers, and safeguards for the independence of the Data Protection Officer.

6. The Data Protection Officer and his or her staff shall be bound by the obligation of confidentiality in accordance with Article 67(1).

Article 41b

Tasks of the Data Protection Officer

1. The Data Protection Officer shall, in particular, have the following tasks with regard to processing of personal data:

(a) ensuring in an independent manner the compliance of Europol with the data protection provisions of this Regulation and Regulation (EU) 2018/1725 and with the relevant data protection provisions in Europol's rules of procedure; this includes monitoring compliance with this Regulation, with Regulation (EU) 2018/1725, with other Union or national data protection provisions and with the policies of Europol in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits.;

b) informing and advising Europol and staff who process personal data of their obligations pursuant to this Regulation, to Regulation (EU) 2018/1725 and to other Union or national data protection provisions;

c) providing advice where requested as regards the data protection impact assessment and monitoring its performance pursuant to Article 89 of Regulation (EU) 2018/1725;

d) keeping a register of personal data breaches and providing advice where requested as regards the necessity of a notification or communication of a personal data breach pursuant to Articles 92 and 93 of Regulation (EU) 2018/1725;

(e) ensuring that a record of the transfer and receipt of personal data is kept in accordance with this Regulation;

(f) ensuring that data subjects are informed of their rights under this Regulation and Regulation (EU) 2018/1725 at their request;

(g) cooperating with Europol staff responsible for procedures, training and advice on data processing;

(h) cooperating with the EDPS;

(i) cooperating with the national competent authorities, in particular with the appointed Data Protection Officers of the competent authorities of the Members States and national supervisory authorities regarding data protection matters in the law enforcement area;

(j) acting as the contact point for the European Data Protection Supervisor on issues relating to processing, including the prior consultation under Articles 39 and 90 of Regulation (EU) 2018/1725, and consulting, where appropriate, with regard to any other matter;

(k) preparing an annual report and communicating that report to the Management Board and to the EDPS;

2. The Data Protection Officer shall carry out the functions provided for by Regulation (EU) 2018/1725 with regard to administrative personal data.

3. In the performance of his or her tasks, the Data Protection Officer and the staff members of Europol assisting the Data Protection Officer in the performance of his or her duties shall have access to all the data processed by Europol and to all Europol premises.

4. If the Data Protection Officer considers that the provisions of this Regulation, of Regulation (EU) 2018/1725 related to the processing of administrative personal data or the provisions of this Regulation or of Article 3 and of Chapter IX of Regulation (EU) 2018/1725 concerning the processing of operational personal data have not been complied with, he or she shall inform the Executive Director and shall require him or her to resolve the non-compliance within a specified time.

If the Executive Director does not resolve the non-compliance of the processing within the time specified, the Data Protection Officer shall inform the Management Board. The Management Board shall reply within a specified time limit agreed with the Data Protection Officer. If the Management Board does not resolve the non-compliance within the time specified, the Data Protection Officer shall refer the matter to the EDPS.";

(31) In Article 42, paragraphs 1 and 2 are replaced by the following:

"1. For the purpose of exercising their supervisory function the national supervisory authority shall have access, at the national unit or at the liaison officers' premises, to data submitted by its Member State to Europol in accordance with the relevant national procedures and to logs as referred to in Article 40.

2. National supervisory authorities shall have access to the offices and documents of their respective liaison officers at Europol.";".

(32) Article 43 is amended as follows:

(a) in paragraph 1, the first sentence is replaced by the following:

“The EDPS shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and Regulation (EU) 2018/1725 relating to the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data by Europol, and for advising Europol and data subjects on all matters concerning the processing of personal data.”;

(b) paragraph 5 is replaced by the following:

“5. The EDPS shall draw up an annual report on his or her supervisory activities in relation to Europol. That report shall be part of the annual report of the EDPS referred to in Article 60 of Regulation (EU) 2018/1725. The national supervisory authorities shall be invited to make observations on this report before it becomes part of the annual report. The EDPS shall take utmost account of the observations made by national supervisory authorities and, in any case, shall refer to them in the annual report.

The report shall include statistical information regarding complaints, inquiries, and investigations, as well as regarding transfers of personal data to third countries and international organisations, cases of prior consultation, and the use of the powers laid down in paragraph 3.”;

(33) in Article 44, paragraph 2 is replaced by the following:

“2. In the cases referred to in paragraph 1, coordinated supervision shall be ensured in accordance with Article 62 of Regulation (EU) 2018/1725. The EDPS shall use the expertise and experience of the national supervisory authorities in carrying out his or her duties as set out in Article 43(2). In carrying out joint inspections together with the EDPS, members and staff of national supervisory authorities shall, taking due account of the principles of subsidiarity and proportionality, have powers equivalent to those laid down in Article 43(4) and be bound by an obligation equivalent to that laid down in Article 43(6).”;

(34) Articles 45 and 46 are deleted;

(35) Article 47 is amended as follows:

(a) paragraph 1 is replaced by the following:

" 1. Any data subject shall have the right to lodge a complaint with the EDPS if he or she considers that the processing by Europol of personal data relating to him or her does not comply with this Regulation or Regulation (EU) 2018/ 1725.";[*we have to replace the whole paragraph]*["1. or Regulation (EU) 2018/ 1725."

(b) in paragraph 2, the first sentence is replaced by the following:

"Where a complaint relates to a decision as referred to in Article 36, 37 or 37a of this Regulation or Article 80, 81 or 82 of Regulation (EU) 2018/1725, the EDPS shall consult the national supervisory authorities of the Member State that provided the data or of the Member State directly concerned.";";

(c) the following paragraph 5 is added:

"5. The EDPS shall inform the data subject of the progress and outcome of the complaint, as well as the possibility of a judicial remedy pursuant to Article 48.";

(36) Article 50 is amended as follows:

(a) the title is replaced by:

"Right to compensation";

(b) paragraph 1 is deleted;

(c) paragraph 2 is replaced by the following:

“2. Any dispute between Europol and Member States over the ultimate responsibility for compensation awarded to a person who has suffered material or non-material damage in accordance with Article 65 of Regulation (EU) 2018/1725 and national laws transposing Article 56 of Directive (EU) 2016/680 shall be referred to the Management Board, which shall decide by a majority of two-thirds of its members, without prejudice to the right to challenge that decision in accordance with Article 263 TFEU.”;.”

(37) Article 51 is amended as follows:

(a) in paragraph 3, the following points (f) to (i) are are added:

“(f) annual information about the number of cases in which Europol issued follow-up requests to private parties or own-initiative requests to Member States of establishment for the transmission of personal data in accordance with Article 26, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks;

(g) annual information about the number of cases where it was necessary for Europol to process personal data outside the categories of data subjects listed in Annex II in order to support Member States in a specific criminal investigation in accordance with Article 18a, including examples of such cases demonstrating why this data processing was necessary;

(h) annual information about the number of cases in which Europol issued alerts in the Schengen Information System in accordance with Article 4(1)(r), and the number of ‘hits’ these alerts generated, including specific examples of cases demonstrating why these alerts were necessary for Europol to fulfil its objectives and tasks;

(i) annual information about the number of pilot projects in which Europol processed personal data to train, test and validate algorithms for the development of tools, including AI-based tools, for law enforcement in accordance with Article 33a, including information on the purposes of these projects and the law enforcement needs they seek to address.”;

(38) in Article 57, paragraph 4 is replaced by the following:

“4. Europol may benefit from Union funding in the form of contribution agreements or grant agreements in accordance with its financial rules referred to in Article 61 and with the provisions of the relevant instruments supporting the policies of the Union. Contributions may be received from countries with whom Europol or the Union has an agreement providing for financial contributions to Europol within the scope of Europol’s objectives and tasks. The amount of the contribution shall be determined in the respective agreement.”;

(39) Article 61 is amended as follows:

(a) Paragraph 1 is replaced by the following:

“1. The financial rules applicable to Europol shall be adopted by the Management Board after consultation with the Commission. They shall not depart from Commission Delegated Regulation (EU) No 2019/715 unless such a departure is specifically required for the operation of Europol and the Commission has given its prior consent.”

(b) paragraphs 2 and 3 are replaced by the following:

“2. Europol may award grants related to the fulfilment of its objectives and tasks as referred to in Articles 3 and 4.”;

3. Europol may award grants without a call for proposals to Member States for performance of activities falling within Europol’s objectives and tasks.”;

(c) the following paragraph 3a is inserted:

“3a. Where duly justified for operational purposes, financial support may cover the full investment costs of equipment, infrastructure or other assets.”;

(40) Article 67 is replaced as follows:

"*Article 67*

Security rules on the protection of classified information and sensitive non-classified information

1. The Europol shall adopt its own security rules that shall be based on the principles and rules laid down in the Commission's security rules for protecting European Union classified information (EUCI) and sensitive non-classified information including, inter alia, provisions for the exchange of such information with third countries, and processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/443 (44) and (EU, Euratom) 2015/444 (45). Any administrative arrangement on the exchange of classified information with the relevant authorities of a third country or, in the absence of such arrangement, any exceptional ad hoc release of EUCI to those authorities, shall be subject to the Commission's prior approval.

2. The Management Board shall adopt the Europol's security rules following approval by the Commission. When assessing the proposed security rules, the Commission shall ensure that they are compatible with Decisions (EU, Euratom) 2015/443 and (EU, Euratom) 2015/444."

(41) in Article 68, the following paragraph 3 is added:

"3. The Commission shall, by [three years after entry into force of this Regulation], submit a report to the European Parliament and to the Council, assessing the operational benefits of the implementation of the competences provided for in Article 18(2)(e) and (5a), Article 18a, Article 26 and Article 26a with regard to Europol's objectives. The report shall cover the impact of those competences on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights.".

Article 2

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*