Conseil de
l'Union européenne

Bruxelles, le 9 février 2022
(OR. en, fr)

5920/22

LIMITE

ENFOPOL 65
SIRIS 20
COPEN 44
SCHENGEN 12
IXIM 27
CODEC 135
IA 11

Dossier interinstitutionnel: 2020/0349(COD)

NOTE POINT "I"

Origine:	Secrétariat général du Conseil
Destinataire:	Comité des représentants permanents
N° doc. Cion:	13908/20 + COR 1
Objet:	Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation – Confirmation du texte de compromis final en vue d'un accord

1. La Commission a présenté le projet de révision du mandat d'Europol susvisé le 9 décembre 2020.

2. Le mandat de négociation du Conseil de l'Union européenne a été adopté lors de la réunion du Coreper du 30 juin 2021.

3. Au Parlement européen, la commission compétente est celle des libertés civiles, de la justice et des affaires intérieures (LIBE). M. Javier ZARZALEJOS (PPE / Espagne) a été désigné rapporteur pour ce dossier. Le 11 octobre 2021, la Commission LIBE du Parlement européen a adopté son propre mandat de négociation.

4. Les négociations interinstitutionnelles ont commencé le 27 octobre 2021.

5. Les délégations ont été tenues régulièrement informées du déroulement des négociations dans des réunions des conseillers JAI ou du groupe "Application de la loi".

6. Le 26 janvier 2022, le Coreper a examiné le compromis global en vue du trilogue politique du 1er février 2022 où les colégislateurs ont trouvé un accord politique sur toutes les questions encore ouvertes à ce stade.

7. Compte tenu de ce qui précède, le Coreper est invité:

– à approuver le texte figurant en annexe de la présente note et

– à marquer son accord pour que le président du Coreper envoie une lettre au président de la Commission LIBE du Parlement européen afin de l'informer que si le Parlement européen adopte sa position en première lecture, conformément à l'article 294, paragraphe 3, du traité sur le fonctionnement de l'Union européenne, dans les termes qui figurent à l'annexe de ladite lettre, après la mise au point par les juristes-linguistes, le Conseil approuvera la position du Parlement conformément à l'article 294, paragraphe 4, du traité sur le fonctionnement de l'Union européenne et adoptera l'acte législatif.

ANNEXE

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[1] 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.

[1] 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***capabilities*** 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 ***and the possibility to conceal their crimes or identities through the use of increasingly sophisticated techniques. Criminals have proven their ability to adapt*** their modes of operation or developing***develop*** new criminal activities ***in times of crisis, including by leveraging technology-enabled tools for multiplying and expanding the range and scale of the criminal activities they engage in***. 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***and cross-border cooperation do*** 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 ***prevent and*** counter serious crime and terrorism. Since Regulation (EU) 2016/794 became applicable, the operational importance of Europol's tasks has changed***increased*** substantially. The new threat environment also changes the ***scope and type of*** support Member States need and expect from Europol to keep citizens safe.

(3a) The additional tasks conferred upon Europol by this Regulation should allow Europol to better support national law enforcement authorities while fully preserving the responsibilities of the Member States in the area of national security laid down in Article 4(2) of the Treaty on the European Union. The reinforced mandate of Europol should be balanced with strengthened safeguards with regard to fundamental rights and increased accountability, liability and oversight, including parliamentary oversight and through the Management Board. To allow Europol to fulfil its mandate, its additional competences and tasks should be matched with adequate human and financial resources.

(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 ***man-made*** crisis situations. In the Union, the***those*** law enforcement units of the Member State cooperate on the basis of Council Decision 2008/617.[2] Europol should be able to provide support to these special intervention units, including by providing operational, technical and financial support***, complementing the efforts undertaken by Member States***.

(5) In recent years***, large-scale cyber-attacks, including*** large scale cyber attacks ***originating in third countries,*** 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, ***detection,*** 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[3], 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***cyber-attacks and cybersecurity*** threats, Europol should cooperate with the ENISA ***within their respective mandates*** through the exchange of information and by providing analytical support.

---

[2] 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).

[3] 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) ***1)***.

(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 ***financial assets, 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***prioritise*** 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 ***identified*** priorities and the implementation of horizontal strategic goals in countering serious crime.

(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[4] [5], 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***In the framework of its mandate and its task of supporting*** the Member States ***in preventing and combating serious crime and terrorism***, Europol should be able to enter data on these persons***support the Member States in processing third-country data and data from international organisations by proposing the possible entry by Member States of a new category of information alerts*** in the ***interest of the Union into the SIS,***SIS in order to make it available directly and in real-time to SIS end-users***to the end-users of the SIS. To that end, a periodic reporting mechanism should be put in place in order to ensure that Member States and Europol are informed on the data inserted in the SIS. The modalities for Member States' cooperation for the processing of data and the insertion of alerts into the SIS, notably as concerns the fight against terrorism, should be subject to continuous coordination amongst the Member States. Criteria on the basis of which Europol would issue proposals for the entry of alerts into the Schengen Information System should be further specified by the Management Board***.

[4] 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).

[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).

(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***Europol should therefore, upon request,*** contribute with its expertise, analysis***analyses***, reports and other relevant information to the entire***Schengen*** 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***mechanism***.

(10) Risk assessments are an essential element of foresight***contribute*** 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***Union*** law provisions on customs risk management.

(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. ***Where relevant, Europol should be able to disseminate the results of its activities as part of its contribution to creating synergies between the research and innovation activities of relevant Union bodies and agencies. Where appropriate, Europol should be able to consult the Joint Research Centre when defining and conceptualising research and innovation activities regarding matters covered by this Regulation. Europol should take all necessary measures to avoid conflicts of interest.*** 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***. Europol should therefore receive adequate and reliable funding for its research and innovation efforts so that it can assist the Member States and the Commission in that area*** 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[6] establishes a framework for the screening of foreign direct investments into the Union***. Foreign direct investments in emerging technologies deserve particular attention as they can have far-reaching implications for*** that provides Member States and the Commission with the means to address risks to security or ***and*** public order***, in particular when such technologies are deployed by law enforcement authorities. Given its role in monitoring emerging technologies and its active involvement in developing new ways of using those technologies for law enforcement purposes, notably through its Innovation Lab and Innovation Hub*** in a comprehensive manner. As part of the assessment of expected implications for security or public order, Europol ***has extensive knowledge regarding the opportunities offered by such technologies as well as the risks associated to their use. Europol*** should ***therefore have the possibility to*** support the screening of specific cases ***Member States in the screening*** of foreign direct investments into the Union that concern undertakings providing technologies***, including software used*** used or being developed by Europol or by Member States for the prevention and investigation of crimes ***covered by Europol's objectives or critical technologies that could be used to facilitate terrorism. In this context, Europol's expertise should support the screening of the foreign direct investments and the related risks to security. Particular account should be taken of whether the foreign investor has already been involved in activities affecting security in a Member State, whether there is a serious risk that the foreign investor engages in illegal or criminal activities, or whether the foreign investor is controlled directly or indirectly by the government of a third country, including through subsidies***.

[6] 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).

(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.

(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***the Executive Director*** should be able to ***propose to*** the competent authorities of a Member State to initiate, conduct or coordinate a criminal investigation of a crime, which ***concerns only one Member State and*** 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***. Europol should inform Eurojust and, where relevant, the European Public Prosecutor's Office ('the EPPO'),*** of such requests ***proposal***.

(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 ***to the Member States and Europol*** on these individuals.

(15a) After having received personal data, and after having ascertained that this data falls under its tasks, Europol may be faced with four situations. First, Europol may receive personal data that falls into the categories of data subjects set out in Annex II of this Regulation. Second, Europol may receive investigative data that national authorities are authorised to process in a criminal investigation in accordance with procedural requirements and safeguards applicable under their national law, for which they request Europol's support for a specific criminal investigation, and that does not fall into the categories of data subjects set out in Annex II of this Regulation. In that case, Europol should be able to process that investigative data for as long as it supports the specific criminal investigation. Third, Europol may receive personal data, without the request for support for a specific criminal investigation, that might not fall into the categories of data subjects set out in Annex II of this Regulation. In that case, Europol should be able to verify if that personal data corresponds to one of those categories of data subjects. Fourth, Europol may receive personal data that is submitted for research and innovation projects, and that does not fall into the categories of data subjects set out in Annex II of this Regulation. In all four situations, Europol may process the personal data to support Member States in countering serious crime and terrorism.

(15b) In accordance with Article 73 of Regulation (EU) 2018/1725, Europol should, where applicable and as far as possible, make a clear distinction between the operational personal data of these different categories of data subjects.

(15c) In cases where Member States use Europol's 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 and should be considered to be a 'processor' within the meaning of Article 87 of Regulation (EU) 2018/1725. In these cases, the requirements linked to the categories of data subjects set out in Annex II of this Regulation should not apply. In cases where Member States use Europol's infrastructure for exchanges of personal data on crimes within the scope of the objectives of Europol and where they grant access to Europol to that data, the requirements linked to the categories of data subjects set out in Annex II of this Regulation should apply to any other processing of that data by Europol.

(16) To ensure that processing of personal data by Europol is limited to the categories ***While respecting the principle*** of data subjects whose data may be processed under this Regulation, ***minimisation*** 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***the*** categories of data subjects ***set out in Annex II of this Regulation***. 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 ***by checking the data against data it already holds, without further analysing the data for additional leads at this stage***. Such pre-analysis should take place prior to***, and separate from,*** Europol's data processing for cross-checking, strategic analysis, operational analysis or exchange of information ***and after Europol has established that the data are relevant and necessary for the performance of its tasks. Once confirmed that personal data falls into the categories of data subjects set out in Annex II, Europol should be able to process that personal data for cross-checking, strategic analysis, operational analysis or exchange of information. If Europol concludes***. 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 ***set out in Annex II***, Europol should delete that data.

(16a) As a result of new available information in the context of investigations, for example regarding additional suspects, the categorisation of personal data in a given dataset may change over time. For this reason, Europol should be allowed to process personal data when it is strictly necessary and proportionate for the purpose of determining the categories of data subjects for a maximum period eighteen months. Europol should be able to extend the maximum processing period up to 3 years in duly justified cases and provided that such an extension is necessary and proportionate. The European Data Protection Supervisor (EDPS) should be informed of the extension. Where the processing of personal data for the purpose of determining the categories of data subjects is no longer necessary and justified, and in any case after the end of the maximum processing period, Europol should delete the relevant data.

(16b) For personal data outside the categories of data subjects set out in Annex II of this Regulation that Europol received prior to the entry into force of Amending Regulation XX, Europol should be able to process that data in accordance with the provisions set out in this Regulation, provided that the requirements for such processing are fulfilled. First, Europol should be able to process such personal data in support of a criminal investigation or to ensure the veracity, reliability and traceability of the criminal intelligence process, provided that the transitional arrangements concerning the processing of personal data received in support of a criminal investigation are fulfilled. Second, Europol should be able to verify if such personal data corresponds to one of the categories of data subjects set out in Annex II of this Regulation by carrying out a pre-analysis of that personal data for a maximum period of 18 months counting from the day of initial receipt of the data by Europol, or in justified cases, for a longer period with the prior authorisation of the EDPS. The total period of processing for such pre-analysis should not exceed a period of three years counting from the day of initial receipt of the data by Europol.

(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***can*** detect such cross-border links ***less effectively*** through their own analysis of the data. Europol should ***therefore*** be able to support Member States' criminal investigations by processing large and complex datasets to detect such cross-border links where the strict requirements ***and safeguards*** 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 ***such investigative data*** that national authorities have acquired in the context of***are authorised to process in*** 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***This*** should also be able to process***include*** personal data that is necessary for its support to a specific criminal investigation in***where*** 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 ***has not been able to ascertain whether that data falls into the categories*** 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***subjects set out in Annex II of this Regulation. Where a Member State, the EPPO or Eurojust provide Europol with investigative data requesting Europol's support for a specific criminal investigation,*** 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***should be able to process that data for as long as it supports that specific*** criminal investigation***,*** in accordance with procedural requirements and safeguards ***under*** applicable under its ***Union or*** 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 data to Europol. When submitting*** investigative case file to***data to Europol to request*** Europol***'s support for a specific criminal investigation, Member States should consider the scale and complexity of the processing and the type and importance of the investigation. Member States should inform Europol when their authorisation to process data in the specific criminal investigation in accordance with procedural requirements and safeguards under the applicable national law has ceased to exist***. 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.

(18a) Europol should also be able to process personal data that is necessary for its support to a specific criminal investigation in one or more Member States if that data originates from a third country, provided that the third country is the subject of an adequacy decision, an international agreement concluded by the Union pursuant to Article 218 TFEU that includes the transfer of personal data for law enforcement purposes, 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, or in the case of which appropriate safeguards with regard to the protection of personal data exist or are provided for in a legally binding instrument 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. Where investigative data are provided to Europol by a third country, Europol should 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, as far as possible, that there are no objective indications that investigative data has been collected in the third country in obvious violation of fundamental rights. Where Europol reaches the conclusion that those conditions are not met, it should not process the data and delete it. Where a third country provides investigative data to Europol, the Data Protection Officer (DPO) should be able to notify the EDPS where relevant.

(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 ***data*** upon request of that Member State***, the EPPO or Eurojust*** 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. ***To this end, Europol should log all evidence and the methods by which it has been produced or acquired by Europol to allow for effective scrutiny of evidence by the defence.***

(20) Cross-border cases of serious crime or terrorism require close collaboration***cooperation*** 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 ***access*** the information they provided to Europol, without prejudice to any ***general or specific*** 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 ***and in Directive (EU) 2016/680 of the European Parliament and of the Council***[7].

[7] ***Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89)***

(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')***EPPO*** established by Council Regulation (EU) 2017/1939[8], should put necessary ***conclude working*** arrangements in place to optimise***setting out the process for*** 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 ***to data held by Europol***, on the basis of a hit/no hit system, to data available at ***which only notifies*** Europol ***in the case of a hit***, in accordance with the safeguards and data protection guarantees provided for in this Regulation***, including any restrictions indicated by the entity which provided the information to Europol. If the information is covered by a restriction issued by a Member State, Europol should inform that Member State for it to comply with its obligations under the EPPO Regulation. The concerned Member State should subsequently inform the EPPO in accordance with its national procedure***. 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 ***in accordance with the safeguards and data protection guarantees provided for in this Regulation***.

---

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***In circumstances where it is essential to the investigation of*** crimes falling within the scope of Europol's objectives, the Executive Director of Europol should be allowed to authorise categories***a category*** of transfers of personal data to third countries in specific situations and on a case-by-case basis, where such a group ***a category*** of transfers related to a***relates to the same*** specific situation***, consists of the same categories of personal data and the same categories of data subjects, is*** are necessary and meet***proportionate for the investigation of the specific crime and meets*** all the requirements of this Regulation. ***Individual transfers covered by a category of transfers may include only some of these categories of personal data and categories of data subjects. A category of transfers of personal data to third countries should be possible in specific situations where the transfer of personal data is necessary either in order to protect the vital interests of the data subject or of another person, or essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country, or to safeguard legitimate interests of the data subject, or in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions, or 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 or the execution of a specific criminal sanction.***

(24a) Transfers not based on the abovementioned authorisation by the Executive Director, an adequacy decision, an international agreement or a cooperation agreement should be allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where Europol has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist. Europol should be able to take into account bilateral agreements concluded between Member States and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. Europol should be able to also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, Europol should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, Europol should be able to require additional safeguards.

(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 ***serious*** crime ***and terrorism***, Europol should be able to receive, and***,*** in specific circumstances***cases where this is necessary and proportionate***, exchange personal data with private parties.

(26) Criminals increasingly use cross-border***the*** services of***offered by*** private parties to communicate and carry out illegal activities. Sex offenders abuse***exploit*** children and share pictures and videos ***constituting child sexual abuse material*** world-wide using***on*** online platforms on the internet***or with peers via number-independent interpersonal communications services***. Terrorists abuse cross-border***utilise the*** services ***offered*** by online service providers to recruit volunteers, plan and coordinate attacks, and disseminate propaganda. Cyber criminals profit from the digitalisation of our societies ***and from the lack of digital literacy and skills of the general population*** using phishing and social engineering to commit other types of cybercrime such as online scams, ransomware attacks or payment fraud. As a result from***of*** the increased use of online services by criminals, private parties hold increasing amounts of personal data***, including subscriber, traffic and content 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, ***the online service provider*** 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***datasets*** 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***datasets*** through national solutions. ***Europol should have measures in place to facilitate the cooperation with private parties, including with respect to the sharing of information.***
When private parties decide to lawfully and voluntarily share the data with law enforcement authorities, they do ***not*** currently not have a single point of contact with which they can share such data sets***datasets*** 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***and voluntarily provide multi-jurisdictional datasets or datasets that cannot*** be easily attributed so far to one or several specific jurisdictions, Europol should be able to receive personal data directly from private parties ***for the purpose of providing Member States with the information necessary to establish jurisdiction and to investigate these crimes under their respective jurisdictions, in accordance with the safeguards and data protection guarantees provided for in this Regulation, including reports relating to moderated content that can reasonably be assumed to be linked to the criminal activities within the remit of Europol***.

(29) To ensure that Member States receive quickly the relevant ***without undue delay the*** information necessary to initiate investigations to prevent and combat serious crime and terrorism, Europol should be able to process and analyse such data sets***datasets*** in order to identify the relevant Member States***' national units concerned*** and forward to the national law enforcement authorities concerned the information and analysis necessary***those national units the personal data and any results relevant to establish jurisdiction and*** to investigate these crimes under their respective jurisdictions. ***Europol should also be able to forward the personal data and results relevant to establish jurisdiction to contact points and third countries concerned with which Europol has concluded 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, or where appropriate safeguards with regard to the protection of personal data exist or are provided for in a legally binding instrument. Where the third country concerned is not subject to such an agreement or decision, or in the absence of such appropriate safeguards, Europol should be able to transfer the result of its analysis and verification of such data to the third country concerned where the conditions laid down in this Regulation are fulfilled.***

(29a) In certain cases and subject to clear conditions, both of which are set out in this Regulation, it may be necessary and proportionate for Europol to transfer personal data to private parties which are not established within the Union or in a 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 or in the case of which appropriate safeguards with regard to the protection of operational personal data exist or are provided for in a legally binding instrument in accordance with this Regulation. In such cases, the transfer should be subject to prior authorisation by the Executive Director.

(30) To ensure that it***Europol*** can identify all relevant national law enforcement authorities***units*** concerned, Europol***it*** should be able to inform private parties when the information received from them is insufficient to enable Europol to identify the law enforcement authorities***national units*** 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***should be able to*** inform private parties of missing information, as far as this is strictly necessary for the identification of the relevant law enforcement authorities***sole purpose of identifying the national units concerned***. Special safeguards should apply to such transfers in particular when***where*** 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 ***compared to the level of protection provided under Directive (EU) 2016/680***.

(31) Member States, third countries, international organisation, including the International Criminal Police Organisation (Interpol),***organisations*** 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***send a reasoned request to*** Member States, via their national units, to request***provide it with the necessary personal data from*** private parties which are established or have a legal representative in their territory to share ***to identify the national units concerned. The request should be reasoned and as targeted as possible for Europol to identify the national units concerned. The relevant*** personal data***, which should be the least sensitive possible and strictly limited to what is necessary and proportionate, should be provided to*** with Europol in accordance with those Member States' applicable laws. ***Member States should assess Europol's request and decide in accordance with their national laws whether or not to accede to it. Data processing by private parties should remain subject to their obligations under the applicable rules, notably with regard to data protection, when processing such requests from competent law enforcement authorities. Private parties should provide the data to the competent law enforcement authorities which have issued the request for further transmission to Europol.*** 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 ***or legally represented in*** their jurisdiction. Irrespective of their jurisdiction with regard ***to*** 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 ***personal data received directly from private parties*** 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***national units*** concerned, and cannot reasonably expect to identify further Member States***national units*** 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 ***or transfer to a national unit or transfer to a contact point of a third country or an authority of a third country*** has taken place, unless a national unit, contact point or authority concerned resubmits ***in compliance with Union and national law,*** 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***those*** personal data if and in so far as it has***which have*** 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'***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.

[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).

(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 ***or send removal orders concerning such content on the basis of Regulation (EU) 2021/784 of the European Parliament and of the Council***[10] to online service providers or ***when they*** exchange information with private parties in the context of cyber attacks***cyberattacks***. 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. ***Europol should ensure by technical means that any such infrastructure is strictly limited to providing a channel for such interactions between the law enforcement authorities and a private party, and that it provides for all necessary safeguards against access by a private party to any other information in Europol's systems, which is not related to the exchange with that private party.***

[10] ***Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (OJ L 172, 17.5.2021, p. 79).***

(35) Terrorist attacks trigger the large scale***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***, thereby allowing for the glorification and provision of training for terrorism, and eventually the radicalisation and recruitment of others. Moreover, the increased use of the internet to record or share child sexual abuse material perpetuates the harm for the victims, as the material can easily be multiplied and circulated. In order to prevent and counter the crimes falling within the scope of Europol's objectives, Europol should be able to support . the*** Member States***' actions in*** can effectively ***addressing*** the dissemination of such***terrorist*** content in the context of such crisis situations stemming from ongoing or recent real-world events, ***and of child sexual abuse material, and to support the actions of online service providers in line with their obligations under Union law as well as in their voluntary actions. To that end,*** Europol should be able to exchange ***relevant*** personal data with private parties, including hashes, IP addresses or URLs related to such content, ***with private parties established in the Union or in a third country that is subject to an adequacy decision, or, in the absence thereof, an international agreement pursuant to Article 218 TFEU, or an operational cooperation agreement concluded between Europol and the third country prior to the entry into force of Regulation (EU) 2016/794. Those exchanges should only take place when*** 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***or to allow its removal, in particular*** where there is an anticipated potential for exponential multiplication and virality across multiple online service providers. ***Nothing in this Regulation should be understood as precluding the Member States from using removal orders as laid down in Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online as an instrument to address terrorist content online.***

(35a) In order to avoid duplication of effort and possible interferences with investigations and to minimise the burden to the hosting service providers affected, Europol should assist, exchange information and cooperate with the competent authorities with regard to transmissions and transfers of personal data to private parties to address online crisis situations and the dissemination of child sexual abuse material.

(36) Regulation (EU) 2018/1725 of the European Parliament and of the Council[11] [12]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***. While Regulation (EU) 2018/1725 has been applicable to the processing of administrative personal data by Europol that are unrelated to criminal investigations, such as staff data, Article 3(2) and Chapter IX of that Regulation, which regulate the processing of operational personal data, have so far not applied*** 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 ***chapter IX of 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. ***Therefore, the supervisory powers of the EDPS over Europol's operational work should be reinforced, in line with the relevant powers applicable to the processing of administrative personal data that apply to all Union bodies and agencies under Chapter VI of Regulation (EU) 2018/1725. To that end, when it comes to the processing of personal data by Europol for operational purposes, the EDPS should be able to order Europol to bring processing operations into compliance with the provisions of this Regulation, to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation, and to impose an administrative fine in the case of non-compliance.***

---

[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).

[12] 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).

(36a) Processing of data for the purposes of this Regulation could entail the processing of special categories of personal data as set out in Regulation (EU) 2016/679. The processing of photographs should not be systematically considered as processing of special categories of personal data, since photographs are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

(36b) The prior consultation mechanism is an important safeguard for new types of processing operations. This should not apply to specific individual operational activities, such as operational analysis projects, but to the use of new IT systems for the processing of personal data and any substantial changes thereto that would involve a high risk to the rights and freedoms of data subjects. The time-period for providing the written advice by the EDPS on such consultations should not be subject to suspensions. In case of processing activities of substantial significance for Europol's performance of tasks, which are particularly urgent, Europol may exceptionally initiate processing already after the prior consultation has been launched, even if the time limit for providing written advice by the EDPS has not yet expired. Substantial significance for Europol's performance of tasks leading to such urgency may arise, when processing is necessary to prevent and fight an immediate threat of a criminal offence in respect of which Europol is competent and to protect vital interests of a person. The Data Protection Officer of Europol should be involved in assessing the urgency and necessity of such processing before the time limit for the EDPS to respond to prior consultation expires. The Data Protection Officer should oversee the processing in question. The EDPS should be able to exercise all of its powers with respect to such processing.

(37) Given the challenges that the use of new technologies by criminals pose to the Union's security***posed to the Union's security by the rapid technological development and the exploitation of new technologies by criminals***, 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 ***to identify, secure and analyse the data needed to investigate crimes. Europol should be able to support Member States in the use of emerging technologies and in exploring*** new approaches and develop***developing*** common technological solutions for Member States to ***better*** prevent and counter ***terrorism and*** crimes falling within the scope of Europol's objectives, ***while ensuring that the development, use and deployment of new technologies is guided by the principles of transparency, explainability, fairness, accountability and does not undermine fundamental rights and freedoms and is in compliance with Union law. To that end,*** Europol should be able to conduct research and innovation activities***projects*** regarding matters covered by this Regulation ***within the binding general scope of research and innovation projects defined by the Management Board, which should be updated where appropriate and made available to the EDPS. Those projects are allowed to include***, including with the processing of personal data ***only*** where necessary***the processing of personal data is strictly required, where the objective of the relevant project cannot be attained through the use of non-personal data, such as synthetic or anonymous data,*** and whilst ensuring full respect for fundamental rights***, notably non-discrimination. The processing of special categories of personal data for research purposes should only be allowed where it is strictly necessary. Given the sensitivity of such processing, appropriate additional safeguards, including pseudonymisation, should be applied. To prevent bias in algorithmic decision-making Europol should be allowed to process personal data outside the categories of data subjects listed in Annex II of Regulation (EU) 2016/794. Europol should keep logs of all personal data processing in the context of its research projects for the purpose of and only as long as necessary for verifying the accuracy of the outcome of the data processing***. The provisions on the development of new tools by Europol should not constitute a legal basis for their deployment at Union or national level. ***To drive innovation and reinforce synergies in research and innovation, Europol should step up its cooperation with relevant networks of Member States' practitioners and other Union agencies within their respective competences in this area, and support related forms of cooperation such as secretarial support to the 'EU Innovation Hub for Internal Security' as a collaborative network of innovation labs.***

(38) Europol should play a key role in assisting Member States to develop new technological solutions based on artificial intelligence ***relevant to achieve Europol's objectives***, which would benefit national law enforcement authorities throughout the Union ***in full respect for fundamental rights and freedoms, including non-discrimination***. Europol should play a key role in promoting ***the development and deployment of*** ethical, trustworthy and human centric artificial intelligence subject to robust safeguards in terms of security, safety***, transparency, explainability*** 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. ***It should inform or consult its Management Board, depending on specific criteria that should be set out in relevant guidelines. Europol should not process data for research and innovation without the consent of the Member State, Union body, third country or international organisation that submitted the data to Europol, unless that Member State, Union body, third country or international organisation has granted its prior authorisation to such processing for the purpose of research and innovation.*** For each project, Europol should carry out, prior to the processing, an assessment of the***a data protection*** impact of the envisaged processing operations on the***assessment to ensure full respect with data*** protection of personal data and all other fundamental rights, including of any bias in the outcome ***and freedoms of data subjects***. This should include an assessment of the appropriateness***, necessity and proportionality*** of the personal data to be processed for the specific purpose of the project. Such***, including the requirement of data minimisation and*** 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***of any potential bias in the outcome and in the personal data to be processed for the specific purpose of the project as well as the measures envisaged to address those risks***. 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 ***provided to it by this Regulation***, Europol should provide the Joint Parliamentary Scrutiny Group ***(JPSG) and the Member States with detailed*** with annual information on the ***development, deployment, use and effectiveness*** use of these tools and capabilities and the result thereof***, in particular about research and innovation projects as well as new activities or the establishment of any new specialised centres within Europol. Moreover, two representatives of the JPSG, one for the European Parliament and one for the national parliaments to reflect the dual constituency of the JPSG, should be invited to at least two ordinary Management Board meetings per year to address the Board on behalf of the JPSG and to discuss the consolidated annual activity report for the previous year, the single programming document for the following year and the annual budget, JPSG written questions and answers, as well as external relations and partnerships, while respecting the different roles and responsibilities of the two bodies in accordance with this Regulation. The Management Board, together with the representatives of the JPSG, may determine other matters of political interest to be discussed. In line with the oversight role of the JPSG, the two JPSG representatives should not have voting rights in the Management Board. Planned research and innovation activities should be set out in the single programming document containing Europol's multiannual programming and annual work programme and transmitted to the Joint Parliamentary Scrutiny Group***.

(40a) Following a proposal from the Executive Director, the Management Board should appoint a Fundamental Rights Officer who should be responsible to support Europol in safeguarding the respect for fundamental rights in all its activities and tasks, notably Europol's research and innovation projects and its exchanges of personal data with private parties. The Fundamental Rights Officer may be a member of Europol's existing staff who received special training in fundamental rights law and practice. The Fundamental Rights Officer should cooperate closely with the Data Protection Officer within the scope of their respective competences. To the extent that data protection matters are concerned, full responsibility should lie with the Data Protection Officer.

(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 [...].***8 March 2021***[13]

(46) This Regulation ***fully*** respects the fundamental rights ***and safeguards,*** 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***enhanced*** safeguards***, democratic oversight and accountability mechanisms,*** to ensure ***that the activities and tasks of Europol are carried out in*** full compliance with fundamental rights as enshrined in the Charter***, notably the*** of Fundamental rights ***to equality before the law, to non-discrimination, and to an effective remedy before the competent national court against any of the measures taken pursuant to this Regulation***. 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.

---

[13] ***OJ C 143, 23.4.2021, p. 6.***

(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 ***personal*** data;;"

(c) the following points (q) to (u) are added:

"(q) 'investigative case file***data*** ' means a dataset or multiple datasets ***data*** that a Member State, the EPPO or a third country ***is authorised to process in*** acquired in the context of an on-going criminal investigation ***related to one or more Member States***, in accordance with procedural requirements and safeguards under the applicable ***Union law or*** national criminal law, and***, that it*** submitted to Europol in support of that criminal investigation ***and that contains personal data outside the categories of data subjects listed in Annex II***.

(r) 'terrorist content' means terrorist content as defined in Article 2(7) of Regulation (EU) 2021/784 of the European Parliament and of the Council[14]***.***

[14] ***Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2029 on addressing the dissemination of terrorist content online (OJ 172, 17.5.2021, p. 79).***

(s) 'online child sexual abuse material' means material constituting child pornography as defined in point (c) of Article 2 of Directive 2011/93/EU of the European Parliament and of the Council [15] ***or pornographic performance as defined in point (e) of Article 2 of that Directive***"

"***(t) 'online crisis situation' means the dissemination of online content stemming from an ongoing or recent real world event which depicts harm to life or to physical integrity or calls for imminent harm to life or to physical integrity and aims to, or has the effect of seriously intimidating a population, where there is a link or a reasonable suspicion of a link to terrorism or violent extremism and where there is an anticipated potential of exponential multiplication and virality across multiple online services;***"

"***(u) 'category of transfers of personal data' means a group of transfers of personal data which all relate to the same specific situation, and which consist of the same categories of personal data and the same categories of data subjects.***"

(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;;***(h bis) support Member States' special intervention units as referred to in Council Decision 2008/617/JHA by providing administrative and financial support.***"

---

[15] ***Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).***

(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 ***falling*** within their competence;;***competences"***"

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

"(m) support Member States' actions***, while respecting the right to privacy and the protection of personal data,*** 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 ***by:***

i. ***assisting competent authorities, upon their request, in responding to cyberattacks of suspected criminal origin,***

ii. ***cooperating with Member States with regard to removal orders for*** terrorist content online***by competent authorities in accordance with Article 14 of Regulation (EU) 2021/784, and***

iii. making referrals of ***online 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***that*** content with their own terms and conditions;**.**"

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

"(q) support Member States in identifying persons whose involvement in crimes***criminal activities*** 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 ***regarding those persons***;

(r) enter data ***support Member States in processing data transmitted by third countries or international organisations to Europol on persons involved in terrorism or in serious and organised crime and propose the possible entry by the Member States, at their discretion and subject to their verification and analysis, of information alerts in the interest of the Union*** into the Schengen Information System, in accordance with Regulation (EU) 2018/1862 of the European Parliament and of the Council*, following consultation with the[16]***. A periodic reporting mechanism shall be put in place in order to inform other*** 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***and Europol on the outcome of the verification and analysis and on whether or not the data has been inserted in the SIS, within a period of 12 months from the communication by Europol of its information to the Member States; The Management Board shall further specify the criteria on the basis*** of which Europol is competent and of which it is aware on the basis of ***issues proposals for possible entry of alerts into the Schengen Information System. Member States shall inform Europol of any*** information received from***alert issued and of any hit on such information alerts, and may inform, through Europol, the*** third countries***country*** or international organisations within the meaning of Article 17(1)(b)***organisation from which the information leading to the alert originates on hits on such alerts, in accordance with the***

[16] ***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).;***

procedure set out in Regulation (EU) 2018/1862 of the European Parliament and the Council.;

(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 ***through the provision of expertise and analyses, where relevant***;

(t) proactively monitor and contribute to research and innovation activities relevant to achieve***achieving*** the objectives set out in Article 3, support ***by supporting*** related activities of Member States, and implement ***and implementing*** its research and innovation activities regarding matters covered by this Regulation, including ***projects for*** the development, training, testing and validation of algorithms for the development of ***specific*** tools ***for the use of law enforcement, and disseminate the results of these activities to the Member States in accordance with Article 67, and contribute to creating synergies between the research and innovation activities of Union bodies and agencies, that are relevant for Europol's objectives as set out in Article 3, including through the EU Innovation Hub for internal security, and in close cooperation with Member States***.

(u) support***, upon their request,*** Member States' actions in preventing the dissemination of***addressing*** 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***in particular by providing private parties with the information necessary to identify relevant*** online service providers***content***.

(v) support Member States' actions in addressing the dissemination of online child sexual abuse material;

(w) cooperate, in accordance with Article 12 of Directive 2019/1153, with Financial Intelligence Units (FIUs), through the Europol national unit or, if allowed by the relevant Member State, by means of direct contact between the FIUs and Europol, in particular through exchanges of information and the provision of analysis to Member States to support cross-border investigations into the money laundering activities of transnational criminal organisations and terrorism financing;

(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 ***based on the information it holds on criminal phenomena and trends to*** support~~ing~~ 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 ***Member States and the*** Commission in identifying key research themes***,. Europol shall assist the Commission in*** 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. ***Where relevant, Europol may disseminate the results of its activities as part of its contribution to creating synergies between the research and innovation activities of Union bodies and agencies in accordance with Article 4(1)(t).***

Europol shall take all necessary measures to avoid conflicts of interest. 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.

Where appropriate, Europol may consult the Joint Research Centre when defining and conceptualising research and innovation activities regarding matters covered by this Regulation.

4b. Europol shall support the ***Member States in 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***, including software,*** 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) paragraph 5is amended as follows:

“***Europol shall not apply coercive measures in carrying out its tasks.*** Europol staff may assist***provide operational support to*** the competent authorities of the Member States ***during investigative measures***, at their request and in accordance with their national law, in ***particular by facilitating cross-border information exchange, providing forensic and technical support and being present when investigative measures are taken. Europol staff shall not have the power to execute***the taking of investigative measures.“

(ea) the following paragraph 5a is added:

"***5a. Europol shall respect the fundamental rights and freedoms enshrined in the Charter in the performance of its tasks.***"

(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."

(-3) In Article 6, the following paragraph 1a is inserted

"***1a. "Without prejudice to paragraph 1, where the Executive Director considers that a criminal investigation should be initiated into a specific crime which affects a common interest covered by a Union policy but affects only one Member State, he or she may propose to the competent authorities of the Member State concerned via the national unit to initiate, conduct or coordinate such criminal investigation.***"

(3a) In Article 6, paragraph 2 is replaced by the following:

"***2. The national units shall inform Europol or the Executive Director without delay of the decision of the competent authorities of the Member States concerning any request or proposal made pursuant to paragraphs 1 and 1a, respectively.***"

(3c) In Article 6, paragraph 4 is replaced by the following:

"***4. Europol shall immediately inform Eurojust and, where relevant, the EPPO, of any request or proposal made pursuant to paragraphs 1 and 1a and of any decision of a competent authority of a Member State pursuant to paragraph 2;***"

(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[17] are allowed to cooperate with***entitled to reply to duly justified requests made by*** Europol in accordance with Article 12 of Directive (EU) 2019/1153 of the European Parliament and the Council[18], in particular via their national unit ***or, if provided for by the national law of that Member State, by direct contacts between the financial intelligence unit and Europol,*** regarding financial information and analyses, within the limits of their mandate and competence. ***and subject to national procedural safeguards.***

(4a) In Article 11(1), point (a) is replaced by the following:

(a) adopt each year, by a majority of two-thirds of its members and in accordance with Article 12, a single programming document in accordance with Article 32 of Commission Delegated Regulation (EU) 2019/715[19] and the related Commission guidelines for the single programming document containing Europol's multiannual programming and its annual work programme for the following year.

(4b) In Article 11(1) the following point (ua) is added:

"***(ua) appoint a Fundamental Rights Officer who shall not receive any instructions regarding the performance of his or her tasks***"

---

17 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).

18 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)."

19 ***Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (OJ L 122, 10.5.2019, p. 1).***

(4c) In Article 12, paragraph 1 is replaced by the following:

"1. The Management Board shall, by 30 November each year, adopt a single programming document containing Europol's multiannual programming and annual work programme, based on a draft put forward by the Executive Director, taking into account the opinion of the Commission and, as regards the multiannual programming, after having consulted the JPSG. If the Management Board decides not to take into account elements of the opinion of the Commission, Europol shall provide a thorough justification. The same obligation shall apply to the elements raised by the JPSG in accordance with point (c) of Article 51(2). The Management Board shall forward the final single programming document to the Council, the Commission and the JPSG."

(4d) In Article 12(2), the first subparagraph is replaced by the following:

"The multiannual programming shall set out the overall strategic programming, including the objectives, expected results and performance indicators. It shall also set out the resource planning, including the multiannual budget and staff. It shall include the strategy for relations with third countries and international organisations and its planned research and innovation activities."

(4e) In Article 14, paragraph 4 is replaced by the following:

"4. The Management Board may invite any person whose opinion may be relevant for the discussion to attend its meeting as a non-voting observer. Two representatives of the JPSG shall be invited to two ordinary meetings per year of the Management Board as observers without voting rights to discuss the following political matters:

- *the consolidated annual activity report for the previous year,*
- *the single programming document for the following year and the annual budget.*
- *JPSG written questions and answers*
- *external relations and partnership matters.*

The Management Board, together with the representatives of the JPSG, may determine other matters of political interest to be discussed."

(4f) In Article 16, paragraph 3 is replaced by the following:

"***3. The Council and the JPSG may invite the Executive Director to report on the performance of his or her duties.***"

(4g) In Article 16(5), point (d) is replaced by the following:

"***(d) preparing the draft single programming document containing the multiannual programming and annual work programmes and submitting it to the Management Board, after having consulted the Commission and the JPSG;***"

(4h) In Article 16(5), a new point (o bis) is added:

"***(o bis) informing the Management Board regarding the memoranda of understanding signed with private parties;***"

(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 ***projects*** regarding matters covered by this Regulation for the development, training, testing and validation of algorithms for the development of ***specific*** tools ***and other specific research and innovation projects relevant to achieve the objectives set out in Article 3 in accordance with the conditions set out in Article 33a***;

(f) supporting Member States***, upon their request,*** 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***facilitating*** the provision of information***, to the Member States and Europol,*** by the public on these individuals.“

(b) the following paragraph 3a is inserted:

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

(c) paragraph 5 is replaced by the following:

“5. Without prejudice to Article 8(4)***, Article 18(2)(e)*** and Article 18a***, and data processing pursuant to Article 26(6b) where Europol's infrastructure is used for bilateral exchanges and Europol has no access to the content of the data***, 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. In accordance with Article 73 of Regulation (EU) 2018/1725, Europol shall, where applicable and as far as possible, make a clear distinction between the operational personal data of these different categories of data subjects.

"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."

(5a) paragraph 6 is replaced by the following:

"***6. Europol may temporarily process data for the purpose of determining whether such data are relevant to its tasks and, if so, for which of the purposes referred to in paragraph 2.***

The time limit for the processing of such data under this paragraph shall not exceed six months."

(5b) the following paragraphs 6a and 6b are inserted:

"***6a. Prior to the processing of data under paragraph 2 of this Article, and where strictly necessary for the purpose of determining whether personal data complies with the requirements of paragraph 5 of this Article, Europol may temporarily process personal data received pursuant to Article 17(1) and (2) for that sole purpose, including by checking the data against all data that Europol already processes in accordance with paragraph 5.***

Europol may only process personal data pursuant to this paragraph for a maximum period of 18 months, or in justified cases for a longer period where necessary for the purpose of this Article. Europol shall inform the EDPS of any extension of the maximum processing period. The total period of processing shall not exceed a period of three years. Such personal data shall be functionally separated from other data. Where Europol concludes 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 where relevant."

6b. 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 pursuant to paragraphs 6 and 6a, in particular with respect to the provision, access to and use of the data, as well as time limits for the storage and deletion of the data, which may not exceed the respective time-limits set out in paragraphs 6 and 6a, having due regard to the principles referred to in Article 71 of Regulation (EU)2018/1725."

(6) The following Article 18a is inserted:

"Article 18a

Information Processing ***of personal data*** in support of a criminal investigation

1. Where necessary for the support of a specific ***ongoing*** criminal investigation ***within the scope of Europol's objectives as set out in Article 3***, Europol may process personal data outside the categories of data subjects listed in Annex II where:

(a) a Member State or**,** the EPPO ***or Eurojust*** provides an investigative case file***data*** to Europol pursuant to point (a) ***points (a) or (b)*** of Article 17(1) for the purpose of operational analysis in***requesting Europol to*** support of that ***ongoing*** specific criminal investigation within the mandate of Europol

(i) by way of operational analysis pursuant to point (c) of Article 18(2); and***, or***

(ii) in exceptional and duly justified cases, by way of cross-checking pursuant to point (a) of Article 18(2);

(b) Europol assesses that it is not possible to carry out the operational analysis ***or cross-checking in support*** of the investigative case file***specific criminal investigation*** without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded ***and sent to the EDPS for information when Europol ceases to support the related specific criminal investigation***.

1a. The Member State providing the investigative data to Europol shall inform Europol when its authorisation to process that data in the specific criminal investigation in accordance with procedural requirements and safeguards under its applicable national law has ceased to exist. When the EPPO or Eurojust provide investigative data to Europol, they shall inform Europol when the authorisation to process that data in the specific criminal investigation in accordance with procedural requirements and safeguards under the applicable Union law and national law has ceased to exist.

2. Europol may process personal data contained in an investigative case ***investigative data in accordance with Article 18(2)*** for as long as it supports the on-going specific criminal investigation for which the investigative case file ***data*** was provided by a Member State or**,** the EPPO ***or Eurojust*** 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 ***Where a*** Member State or**,** the EPPO***, or Eurojust*** that provided an investigative case file ***data*** to Europol pursuant to paragraph 1, Europol may store that investigative case file ***data*** and the outcome of its operational analysis***processing*** beyond the storage ***processing*** period set out in paragraph 2, ***upon the request of the provider of that investigative data, and*** 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***concerning the*** criminal investigation are on-going in that Member State***for which that data was provided***.

That Member State***, the EPPO, Eurojust, or, with their agreement, another Member State in which judicial proceedings are ongoing with respect to a related criminal investigation,*** may also request Europol to store the investigative case file ***data*** and the outcome of its operational analysis beyond the storage ***processing*** 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 judicial proceedings following ***concerning*** a related criminal investigation are on-going in another ***ongoing in that other*** 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.

3a. Without prejudice to the processing of personal data under Article 18(6a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be processed where necessary and proportionate for the purposes of paragraphs 3 and 4 of this Article.

The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the provision and processing of personal data in accordance with paragraphs 3 and 4.

4. Paragraphs 1 to ***3a***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, ***or in the case of which appropriate safeguards with regard to the protection of personal data exist or are provided for in a legally binding instrument in accordance with Article 25(4a) of this Regulation,*** and such third country provides an investigative case file ***data*** to Europol for operational analysis that ***contributes to*** supports the specific criminal investigation in a Member State or in ***one or more*** Member States that Europol supports***, provided that the third country acquired the data in the context of a criminal investigation in accordance with procedural requirements and safeguards applicable under its national criminal law***. Where a third country provides an investigative case file ***data*** to Europol, *the DPO* ***may where relevant notify the EDPS***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***is an indication*** that such data is ***manifestly*** disproportionate or ***was*** collected in ***obvious*** violation of fundamental rights, Europol shall not process it ***and delete the data. Personal*** . data processed pursuant to this paragraph may only be accessed by Europol where necessary for the support of the specific criminal investigation in a ***one or more*** Member State or in Member States***States for which it was provided***. It shall be shared only within the Union.; “

(6 bis) In Article 19, paragraphs 1 and 2 are amended as follows:

"***1. A Member State, a Union body, a third country or an international organisation providing information to Europol shall determine the purpose or purposes for which it is to be processed, as referred to in Article 18. If it has not done so, Europol, in agreement with the provider of the information concerned, shall process the information in order to determine the relevance of such information as well as the purpose or purposes for which it is to be further processed. Europol may process information for a purpose different from that for which information has been provided only if authorised so to do by the provider of the information. Information provided for the purposes referred to in points (a) to (d) of Article 18(2) may also be processed by Europol for the purpose of Article 18(2)(e) in accordance with the procedures laid down in Article 33a.***

2. Member States, Union bodies, third countries and international organisations may indicate, at the moment of providing information to Europol, any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its transfer, transmission, erasure or destruction. Where the need for such restrictions becomes apparent after the information has been provided, they shall inform Europol accordingly. Europol shall comply with such restrictions."

(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) ***and subject to the rules and safeguards for personal data processing set out in this Regulation***, Member States may determine information to be made directly accessible by Europol to selected other Member States for ***joint operational analysis*** the purpose of enhanced collaboration in specific investigations, without prejudice to any restrictions of Article 19(2) ***and following procedures to be set out in the guidelines referred to in Article 18(7).***";"

(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***,*** ***detecting, investigating and prosecuting*** :;"

(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. ***Upon request by the EPPO in accordance with Article 102 of Regulation (EU) 2017/1939,*** Europol shall actively support the investigations and prosecutions of the EPPO and cooperate with it, ***by providing information and analytical support, until the moment the EPPO determines whether to prosecute or otherwise dispose of the case*** in particular through exchanges of information and by providing analytical support.

3. ***In order to provide information to the EPPO under paragraph 2,*** Europol shall take all appropriate measures to enable the EPPO to have indirect access to information***data related to offences within the EPPO's mandate,*** provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system.***, which only notifies Europol in the case of a hit and without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with*** Article 21***19(2). In the case of a hit, Europol*** shall apply mutatis mutandis***initiate the procedure by which the information that generated the hit may be shared, in accordance*** with the exception of its***decision of the provider of the information to Europol, and only to the extent that the data generating the hit are relevant for the request submitted pursuant to*** 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 ***in accordance with Article 22, Article 25(2) and (3) of Regulation (EU) 2017/1939 and without prejudice to any restrictions indicated in accordance with Article 19(2) of this Regulation by the Member State or Union body, third country or international organisation providing the information in question. Europol shall notify the Member States concerned without delay.***

Where the information concerning criminal conduct in respect of which the EPPO could exercise its competence has been provided to Europol by a Member State that indicated restrictions on the use of such information in accordance with Article 19(2), Europol shall notify the EPPO of the existence of that restriction and refer the matter to the Member State concerned which shall engage directly with the EPPO in order to comply with its obligations pursuant to Article 24(1) and (4) of Council Regulation (EU) 2017/1939. "

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

"8. If during information-processing activities in respect of an individual***a specific*** 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 ***without prejudice to any restrictions indicated by the Member States in accordance with Article 19(2). Europol shall notify the Member States concerned without delay***."

(9a) In Article 23, paragraph 7 is replaced by the following:

"7. Onward transfers of personal data held by Europol by Member States, Union bodies, third countries, international organisations and private parties shall be prohibited, unless Europol has given its prior explicit authorisation."

(9 bis) The title of Section 2 is replaced by the following:

"***Transmission, transfer and exchange of personal data***"

(10) Article 24 is replaced by the following:

"Article 24

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

1. ***In accordance with Article 71(2) of Regulation (EU) 2018/1725 and*** 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 ***or body*** if the ***personal*** data are necessary ***and proportionate*** for the legitimate performance of tasks of the other Union institution, body, office or agency ***or body***.

2. Where the operational personal data are transmitted following a request***Following a request for the transmission of personal data*** from another Union institution, body, office or agency, both the controller and the recipient shall bear the responsibility for the lawfulness of that***Europol shall verify the competence of the other Union institution or body . If doubts arise as to this necessity of the*** transmission. ***of the personal data, Europol shall seek further information from the recipient.***

~~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 ***or body*** 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 ***or body*** 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 1, the introductory phrase and point (a) are replaced by the following:

"1. Subject to any possible restrictions pursuant to Article 19(2) or (3) and without prejudice to Article 67, Europol may transfer personal data to a competent authority of a third country or to an international organisation, insofar as such transfer is necessary for the performance of Europol's tasks, on the basis of one of the following:

(a) a decision of the Commission adopted in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection (‘adequacy decision’)

(-aa) paragraph 3 is deleted

(-abis) The following paragraph 4a. is inserted

"***4a. In the absence of an adequacy decision, the Management Board may authorise Europol to transfer personal data to a competent authority of a third country or to an international organisation where:***

(a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

(b) Europol has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of personal data."

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

"By way of derogation from paragraph 1, the Executive Director may***, in duly justified cases,*** authorise the transfer or categories***a category*** of transfers of personal data to ***a competent authority of a*** third countries or ***country or to an*** international organisations***organisation*** on a case-by-case basis if the transfer is, or the related transfers are:;"

(a bis) In paragraph 5, point (b) is amended as follows:

"***(b) necessary to safeguard legitimate interests of the data subject ;***"

(b) In Paragraph 8, the following sentence is deleted ***is replaced by the following***:

"***8. Europol shall inform the EDPS about categories of transfers under point (b) of paragraph 4a.*** Where a transfer is based on paragraph ***4a or*** 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) In paragraph 1, point (c) is amended as follows:

"***(c) an authority of a third country or an international organisation which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, with which the Union has concluded an international agreement pursuant to Article 218 TFEU or in the case of which appropriate safeguards with regard to the protection of operational personal data exist or are provided for in a legally binding instrument in accordance with Article 25(4a) of this Regulation.***"

(a) paragraph 2 is replaced by the following:

"2. ***Where*** Europol may receive***receives*** personal data directly from private parties***, it may*** and process those personal data in accordance with Article 18 in order to identify all***the*** national units concerned, as referred to in point (a) of paragraph 1. Europol shall forward the personal data and any relevant results from the ***necessary*** processing of that data necessary ***data*** for the purpose of establishing jurisdiction immediately to the national units concerned. Europol may forward the personal data and relevant results from the ***necessary*** 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***If*** Europol has identified and***cannot identify any national units concerned, or has already*** forwarded the relevant personal data to all the ***identified*** respective national units concerned, or ***and*** it is not possible to identify further national units concerned, it shall erase the data, unless a***the*** national unit, contact point or authority concerned resubmits the personal data to Europol in accordance with Article 19(1) within four months after the ***transmission or*** transfer takes place. ***Criteria as to whether the national unit of the Member State of establishment of the relevant private party constitutes a national unit concerned shall be set out in the guidelines referred to in Article 18(7)."***

(a bis) the following paragraph 2a is added:

"***2a. Any cooperation of Europol with private parties shall neither duplicate nor interfere with the activities of Member States' financial intelligence units established pursuant to Directive (EU) 2015/849 of the European Parliament and of the Council, and shall not concern information that is to be provided to financial intelligence units for the purposes of that Directive.***"

(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 ***and the result of its analysis and verification*** 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 ***or in the case of which appropriate safeguards with regard to the protection of operational personal data exist or are provided for in a legally binding instrument in accordance with Article 25(4a) 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***to*** the third country concerned."

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

"5. Europol may***shall not*** transmit or transfer personal data to private parties***, except where,*** on a case-by-case basis, where it is strictly necessary ***and proportionate***, 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***that*** 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 ***or in the case of which appropriate safeguards with regard to the protection of operational personal data exist or are provided for in a legally binding instrument in accordance with Article 25(4a) 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 ***a specific*** criminal offences***offence*** 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,*** 6a and 6b are inserted:

"***-6a. Without prejudice to points (a), (c) and (d) of paragraph 5 and other Union legal acts, transfers or transmissions of personal data under paragraphs 5 and 6 of this Article shall not be systematic, massive or structural.***

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***national*** laws, for the purpose of sharing it with Europol, on the condition that the requested***. Such a request shall be reasoned and as targeted as possible and such*** personal data is***shall be the least sensitive possible and*** strictly limited to what is necessary ***and proportionate*** for Europol with a view to***for the sole purpose of*** 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***, and those exchanges may also cover crimes falling outside the scope of the objectives of Europol. In cases where Member States use this infrastructure for exchanges of personal data on crimes falling within the scope of Europol's objectives, they may grant Europol access to such data***. 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 ***and shall be considered to be a 'processor' within the meaning of Article 87 of Regulation (EU) 2018/1725. Europol shall carry out an assessment of the possible security risks posed by the opening of its infrastructure for use by private parties and, where necessary, implement appropriate preventive and mitigating measures***."

(e) paragraphs 9 and 10 are deleted;

(f) a new paragraph 11 is inserted:

"***11. Europol shall draw up an annual report to the Management Board on the personal data exchanged with private parties pursuant Articles 26, 26a and 26b on the basis of quantitative and qualitative evaluation criteria defined by the Management Board, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks. The report shall take into account the obligations of discretion and confidentiality and the examples shall be anonymized insofar as personal data is concerned. The annual report shall be sent to the European Parliament, the Council, the Commission and national parliaments.***"

(13) the following Article 26a is inserted:

"Article 26a

Exchanges of personal data with private parties in ***online*** 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 ***in*** 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 ***or in the case of which appropriate safeguards with regard to the protection of operational personal data exist or are provided for in a legally binding instrument in accordance with Article 25(4a) of this Regulation***. Where the conditions set out under paragraphs 5 and 6 of Article 25 ***of this Regulation*** are fulfilled, Europol may transfer the result of its analysis and verification of such data with ***to*** 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***addressing*** online content related to terrorism or violent extremism***crisis situations*** 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 ***or in the case of which appropriate safeguards with regard to the protection of operational personal data exist or are provided for in a legally binding instrument in accordance with Article 25(4a) of this Regulation***, the transfer shall be authorised by the Executive Director.

4a. Europol shall assist, exchange information and cooperate with the competent authorities with regard to the transmission or transfer of personal data to private parties under paragraphs 3 or 4 of this Article, in particular to avoid duplication of effort, enhance coordination and avoid interference with investigations in different Member States.

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 ***national*** laws, for the purpose of sharing it with Europol, on the condition that the requested***Such a request shall be reasoned and as targeted as possible and such*** personal data is***shall be the least sensitive possible and*** strictly limited to what is necessary ***and proportionate*** for Europol for preventing the dissemination of***addressing*** online content related to terrorism or violent extremism***crisis situations*** 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***39a***.

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."

(13a) the following Article 26b is inserted:

"***Article 26b***

Exchanges of personal data with private parties to address the online dissemination of child sexual abuse material

1. Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 to address the online dissemination of child sexual abuse material, as set out in point (v) 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 the Member State, or to the 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 or in the case of which appropriate safeguards with regard to the protection of operational personal data exist or are provided for in a legally binding instrument in accordance with Article 25(4a) of this Regulation. Where the conditions set out under paragraphs 5 and 6 of Article 25 of this Regulation are fulfilled, Europol may transfer the result of its analysis and verification of such data to 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 addressing the online dissemination of child sexual abuse material as set out in point (v) 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 or in the case of which appropriate safeguards with regard to the protection of operational personal data exist or are provided for in a legally binding instrument in accordance with Article 25(4a) of this Regulation, the transfer shall be authorised by the Executive Director.

4a. Europol shall assist, exchange information and cooperate with the competent authorities with regard to the transmission or transfer of personal data to private parties under paragraphs 3 or 4 of this Article, in particular to avoid duplication of effort, enhance coordination and avoid interference with investigations in different Member States.

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. Such a request shall be reasoned and as targeted as possible and such personal data shall be the least sensitive possible and strictly limited to what is necessary and proportionate for Europol to address the online dissemination of child sexual abuse material, as set out in point (v) 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 process such requests in accordance with national law 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 39a.

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."

(13bis) In Article 27, paragraphs 1 and 2 are amended as follows:

"1. Insofar as is necessary in order for Europol to perform its tasks, Europol may receive and process information originating from private persons. Personal data originating from private persons may only be processed by Europol on condition that they are received via:

(a) a national unit in accordance with national law;

(b) the contact point of a third country or an international organisation with which Europol has concluded, before 1 May 2017, a cooperation agreement allowing for the exchange of personal data in accordance with Article 23 of Decision 2009/371/JHA; or

(c) an authority of a third country or an international organisation which is the subject of an adequacy decision as referred to in point (a) of Article 25(1), with which the Union has concluded an international agreement pursuant to Article 218 TFEU ***or in the case of which appropriate safeguards with regard to the protection of operational personal data exist or are provided for in a legally binding instrument in accordance with Article 25(4a) of this Regulation.***

2. If Europol receives information, including personal data, from a private person residing in a third country with which there is no international agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA or on the basis of Article 218 TFEU, which is not the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation ***or in the case of which appropriate safeguards with regard to the protection of operational personal data exist or are provided for in a legally binding instrument in accordance with Article 25(4a) of this Regulation***, Europol may only forward that information to a Member State or to a third country concerned with which such an international agreement has been concluded."

(13ter) The title of Chapter VI is amended as follows:

"***DATA PROTECTION***"

(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[20]* 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.

[20] 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)."

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' ***as defined in Article 3 of Regulation (EU) 2018/1725***, unless indicated otherwise ***provided for in this Regulation***.

4. Europol***The Management Board*** shall ***adopt rules to*** determine the time limits for the storage of administrative personal data in its rules of procedure.

(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 the*** 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 ***concerning natural persons'*** sex life or sexual orientation shall be allowed only where strictly necessary and proportionate for ***research and innovation projects pursuant to Article 33a and for operational purposes, within the mandate of Europol, and only for*** preventing or combating crime that falls within Europol's objectives ***as set out in Article 3. Such processing shall also be subject to appropriate safeguards laid down in this regulation with regard to the rights and freedoms of the data subject, and, with the exception of biometric data processed for the purpose of uniquely identifying a natural person, shall be allowed only*** and if those data supplement other personal data processed by Europol.; "

(aa) the following paragraph 2a is inserted:

"***2a. The Data Protection Officer shall be informed without undue delay in the case of processing of personal data pursuant to this Article.***"

(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 ***where necessary*** for the cases outlined in Article ***20(1) and*** 20 (2a)***, or for a research and innovation project involving specifically authorised staff of Member States' competent authorities and Union agencies established on the basis of Title V of the TFEU in accordance with Article 33a(1)(c)***. The Executive Director shall duly authorise a limited number of Europol officials, ***and where relevant also Member State officials***, to have such access if it is necessary for the performance of their tasks"

(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 ***required under Union law or*** strictly necessary and proportionate in individual cases concerning crimes that falls***fall*** 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 ***regarding Europol and in Article 29 of Directive (EU) 2016/680 regarding the Member States*** 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. Europol may process personal data for the purpose of its research and innovation projects as referred to in point (e) of Article 18(2), where the following conditions are met:

(a) the processing of personal data is strictly required and duly justified to achieve the objectives of the project;

(b) as regards special categories of personal data, processing shall be only allowed where it is strictly necessary and accompanied by appropriate safeguards, which may include pseudonymisation.

The processing of personal data by Europol in the context of research and innovation projects shall be guided by the principles of transparency, explainability, fairness, and accountability.

1***2***. 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 ***research and innovation*** project shall be subject to prior authorisation by the Executive Director, ***in consultation with the Data Protection Officer and the Fundamental Rights Officer,*** based on

i. a description of the specific objectives of the project and the way in which the project assists Europol or national law enforcement authorities in its tasks,

ii. a description of the envisaged processing activity**,** setting out the ***objectives, scope and duration of the processing and the*** necessity ***and proportionality*** to process ***the*** personal data, such as for exploring and testing innovative ***technological*** solutions and ensuring accuracy of the project results,

iii. a description of the ***categories of*** personal data to be processed,

iv. a description of ***compliance with the data protection principles laid down in Article 71 of Regulation (EU) 2018/1725, of*** the retention period and conditions for access to the personal data, ***and***

v. a data protection impact assessment***, including*** of the risks to all rights and freedoms of data subjects, including***the risk*** of any bias in the ***personal data to be used for the training of algorithms and in the*** outcome ***of the processing***, and the measures envisaged to address those risks; ***as well as to avoid violations of fundamental rights.***

(b) (b) the Management Board and the EDPS***the EDPS shall be informed prior to the launch of the project; the Management Board*** shall be ***either consulted or*** informed prior to the launch of the project; ***, in accordance with criteria laid down in the guidelines referred to in article 18(7)***

(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 ***specifically*** authorised staff of Europol ***and, subject to technical security measures, specifically authorised staff of Member States' competent authorities and Union agencies established on the basis of Title V of the TFEU,*** shall have access to that data;

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

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

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

(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***2 years*** 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. The Management Board shall establish a binding general scope for the research and innovation projects of Europol. The document shall be updated where appropriate. The document shall be made available to the EDPS for the purpose of its supervisory role.

2***4***. Europol shall keep a complete and detailed description of the process and rationale behind the training, testing and validation of algorithms to ensure transparency ***of the procedure and the algorithms, including their compliance with the safeguards provided for in this Article, and to allow*** and for verification of the accuracy of the results.; ***Upon request, Europol shall make the description available to interested parties, including Member States and the JPSG.***

5. If the data to be processed for a research and innovation project have been provided by a Member State, a Union body, a third country or an international organisation, Europol shall seek consent from that Member State, Union body, third country or international organisation in accordance with Article 19(2), unless the Member State, Union body, third country or international organisation has granted its prior authorisation to such processing for the purpose of Article 18(2)(e), either in general terms or subject to specific conditions. Europol shall not process data for research and innovation without the consent of the Member State, Union body, third country or international organisation. Such consent may be withdrawn at any time.""

(20) Article 34 is amended as follows:

(a) paragraph 1 is replaced by the following:

"1. ***Without prejudice to Article 92 of Regulation (EU) 2018/1725,*** 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***Regulation (EU) 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.; ***Member States providing the data shall communicate the breach to the data subject concerned in accordance with national law.***"

(c) 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***Regulation (EU) 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.; ***Restricted data shall be processed only for the purpose of protecting the rights of the data subject, when it is necessary to protect the vital interest of another person, or for the purposes laid down in Article 82(3) of that Regulation.***"

(ca) paragraphs 4 and 5are amended as follows:

"***4. If personal data as referred to in paragraphs 1 and 3 held by Europol have been provided to it by third countries, international organisations or Union bodies, have been directly provided by private parties or have been retrieved by Europol from publicly available sources or result from Europol's own analyses, Europol shall rectify, erase or restrict such data and, where appropriate, inform the providers of the data.***

5. If personal data as referred to in paragraphs 1 and 3 held by Europol have been provided to Europol by Member States, the Member States concerned shall rectify, erase or restrict such data in collaboration with Europol, within their respective competences."

(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 1 is replaced by the following:

"***1. Europol shall process personal data in a way that ensures that their source, in accordance with Article 17, can be established.***""

(-aa) introductory part of paragraph 2 is replaced by the following:

"***2. The responsibility for the quality of personal data as referred to in point (d) of Article 71(1) of Regulation (EU) 2018/1725 shall lie with:***""

(-ab) point (a) of paragraph 2 is replaced by the following:

"***(a) the Member State or the Union body which provided the personal data to Europol***"

(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.;"

(aa) in paragraph 6, the first subparagraph is replaced by the following:

"***6. In the case of a transfer between Europol and a Union body, the responsibility for the legality of the transfer 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***prior consultation shall not apply to specific individual operational activities that do not include any new type of processing that would involve a high risk to the rights and freedoms of the data subjects***.;"

(b) paragraphs 2 and 3 are deleted***replaced by the following***;

"***2. Europol may initiate processing operations which are subject to prior consultation pursuant to Article 90(1) of Regulation (EU) 2018/1725 unless the EDPS has provided reasoned written advice pursuant to Article 90(4) of Regulation (EU) 2018/1725 within the time periods stipulated therein, which start on the date of receipt of the initial request for consultation and shall not be suspended.***

3. If the envisaged processing has substantial significance for Europol's performance of tasks and is particularly urgent and necessary to prevent and fight an immediate threat of a criminal offence in respect of which Europol is competent and to protect vital interests of a person, Europol may exceptionally initiate processing after the consultation has started but before the time period stipulated in Article 90(4) of Regulation (EU) 2018/1725 has expired. In this case, Europol shall inform the EDPS prior to the start of processing activities. Written advice of the EDPS pursuant to Article 90(4) of Regulation (EU) 2018/1725 shall be taken into account in retrospect, and the way the processing is carried out shall be adjusted accordingly. The Data Protection Officer of Europol shall be involved in assessing the urgency of such processing before the time limit for the EDPS to respond to prior consultation expires. The Data Protection Officer shall oversee the processing in question."

(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.

(h) where applicable, the use of profiling.

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 ***law*** and practices and the ability to fulfil his or her tasks under***the tasks referred to in Article 41b of*** this Regulation ***and in Regulation (EU) 2018/1725***.

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***41b*** 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.
The provisions applicable to the Data Protection Officer shall apply mutatis mutandis to the assistant Data Protection Officer.

3. Europol shall ensure that the Data Protection Officer ***acts independently and*** 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).

6a. The Data Protection Officer shall be appointed 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 Management 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.

6b. After their designation, the Data Protection Officer and the assistant Data Protection Officer shall be registered with the EDPS by the Management Board.

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 ***internal*** 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 ***transmission,*** 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) ***responding to requests from the EDPS; within the sphere of his or her competence,*** cooperating ***and consulting*** with the EDPS***, at the latter's request or on his or her own initiative***;

(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 ***within the sphere of his or her competence***;

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

(ka) ensuring that the rights and freedoms of data subjects are not adversely affected by processing operations;

1a. The Data Protection Officer may make recommendations to the Management Board for the practical improvement of data protection and advise on matters concerning the application of data protection provisions. Furthermore, the Data Protection Officer may, on his or her own initiative or at the request of the Management Board or any individual, investigate matters and occurrences directly relating to his or her tasks which come to his or her notice, and report back to the person who commissioned the investigation or to the Management Board.

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.;“

(30a) the following Article 41c is inserted

"*Article 41c*

Fundamental Rights Officer

1. The Management Board shall, upon proposal by the Executive director, designate a person to act as Fundamental Rights Officer. That person may be a member of the existing staff of Europol who received special training in fundamental rights law and practice.

2. The Fundamental Rights Officer shall perform the following tasks:

(a) advising Europol where he or she deems it necessary or where requested on any activity of Europol without impeding or delaying those activities;

(b) monitoring Europol's compliance with fundamental rights;

(c) providing non-binding opinions on working arrangements;

(d) informing the Executive Director about possible violations of fundamental rights during activities of Europol;

(e) promoting Europol's respect of fundamental rights in the performance of its tasks and activities;

(f) performing any other tasks, where provided for by this Regulation;

3. Europol shall ensure that the Fundamental Rights Officer does not receive any instructions regarding the exercise of those tasks.

4. The Fundamental Rights Officer shall report directly to the Executive Director and draw up annual reports on his or her activities, including the extent to which the activities of Europol respect fundamental rights. These reports shall be made available to the Management Board."

(30b) the following Article 41d is inserted:

"***Article 41d***

Fundamental Rights Training

All Europol staff involved in operational tasks involving personal data processing shall receive mandatory training on the protection of fundamental rights and freedoms, including with regard to the processing of personal data. This training shall be developed in cooperation with the European Union Agency for Fundamental Rights (FRA) and the European Union Agency for Law Enforcement Training (CEPOL)."

(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 ***referred to in Article 41 of Directive (EU) 2016/680*** 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.;"

(aa) in paragraph 3, the following points (j) to (l) are added"

"(j) order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(k) order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation;

(l) impose an administrative fine in the case of non-compliance by Europol with one of the measures referred to in points (c), (e), (f), (j) and (k) of this paragraph, depending on the circumstances of each individual case."

(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***the annual*** report ***on the supervisory activities of the EDPS in relation to Europol*** before it becomes part of the annual report ***of the EDPS***. 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) Article 44 ***is amended as follows***,

(a) 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).;"

(b) paragraph 4 is replaced by the following:

"***4. In cases relating to data originating from one or more Member States, including the cases referred to in Article 47(2), the EDPS shall consult the national supervisory authorities concerned. The EDPS shall not decide on further action to be taken before those national supervisory authorities have informed the EDPS of their position, within a deadline specified by him or her which shall not be shorter than one month and not longer than three months. The EDPS shall take the utmost account of the respective positions of the national supervisory authorities concerned. In cases where the EDPS intends not to follow the position of a national supervisory authority, he or she shall inform that authority, provide a justification and submit the matter to the European Data Protection Board .***"

(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 ***or 37*** 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;***replaced by the following:***

"***Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation in accordance with Article 65 of Regulation 2018/1725 and national laws transposing Article 56 of Directive (EU) 2016/680.***"

(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***paragraph 1*** 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, point (d) is replaced by the following:

"***(d) the consolidated annual activity report on Europol's activities, referred to in point (c) of Article 11(1), including relevant information on Europol's activities in and results obtained in processing large datasets, without disclosing any operational details and without prejudice to any ongoing investigations;***"

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

"(f) annual information about the number of cases in which Europol issued follow-up requests to***pursuant to Article 26(11) on the personal data exchanged with*** private parties or own-initiative requests to Member States of establishment for the transmission of personal data in accordance with Article 26, including ***pursuant to Article 26, Article 26a and Article 26b, including an assessment of the effectiveness of cooperation,*** specific examples of cases demonstrating why these requests were necessary ***and proportionate*** for Europol to fulfil its objectives and tasks***, and, as regards personal data exchanges pursuant to Article 26b, the number of children identified as a result of those exchanges to the extent that this information is available to Europol; examples shall be anonymized insofar as personal data is concerned***;

(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, ***alongside information on the duration and outcomes of the processing,*** including examples of such cases demonstrating why this data processing was necessary ***and proportionate; examples shall be anonymized insofar as personal data is concerned, without disclosing any operational details and without prejudice to any ongoing investigations***;

(g a) annual information about transfers of personal data to third countries and international organisations pursuant to 1 or 4a of Article 25 broken down per legal basis, and on the number of cases in which the Executive Director authorised, pursuant to Article 25(5), the transfer or categories of transfers of personal data related to a specific ongoing criminal investigation to third countries or international organisations, including information on the countries concerned and the duration of the authorisation;

(h) annual information about the number of cases in which Europol issued***proposed the possible entry of information*** alerts in the Schengen Information System in accordance with Article 4(1)(r), and the number of 'hits' these alerts generated***interest of the Union by the Member States in the Schengen Information System in accordance with Article 4(1)(r)***, including specific examples of cases demonstrating why ***the entry of*** these alerts were necessary for Europol to fulfil its objectives and tasks***was proposed; examples shall be anonymized insofar as personal data is concerned***;

(i) annual information about the number of ***research and innovation projects undertaken*** 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 ***18(2)(e),***33a, including information on the purposes of these projects, and ***the categories of personal data processed, the additional safeguards used, including data minimisation,*** the law enforcement needs they seek to address. ***and the outcome of the projects***;

(ia) annual information about the number of cases in which Europol made use of temporary processing in accordance with Article 18(6a) and, where applicable, the number of cases in which the maximum processing period was prolonged;

(ib) annual information on the number and types of cases where special categories of personal data were processed, pursuant to Article 30(2);"

(aa) paragraph 5 is replaced by the following:

"***5. The JPSG may draw up summary conclusions on the political monitoring of Europol's activities, including non binding specific recommendations to Europol, and submit those conclusions to the European Parliament and national parliaments. The European Parliament shall forward them, for information purposes, to the Council, the Commission and Europol.***"

(37a) the following Article 52a is inserted

"***Article 52a***

Consultative Forum

1. A consultative forum shall be established by the JPSG to assist it by providing independent advice in fundamental rights matters upon request. The JPSG and the Executive Director may consult the consultative forum on any matter related to fundamental rights.

2. The JPSG shall decide on the composition of the consultative forum, its working methods and the terms of the transmission of information to the consultative forum."

(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.;"

(38a) In Article 58, paragraph 9 is replaced by the following:

"***For any building projects likely to have significant implications for Europol's budget, Commission Delegated Regulation (EU) 2019/715 shall apply.***"

(38b) Article 60 is amended as follows

(a) paragraph 4 is replaced by the following:

" ***4. On receipt of the Court of Auditors' observations on Europol's provisional accounts for year N pursuant to Article 246 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council***[21]***, Europol's accounting officer shall draw up Europol's final accounts for that year. The Executive Director shall submit them to the Management Board for an opinion.***"

[21] ***Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013 (EU) No 1301/2013, (EU) No 1303/2013. (EU)No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No282/2013, and Decision No 541/2014/EU and repealing Regulation (EU) No 996/2012(OJ L 122, 10.5.2019, p.1)."***

(b) paragraph 9 is replaced by the following:

"***9. The Executive Director shall submit to the European Parliament, at the latter's request, any information required for the smooth application of the discharge procedure for year N, as laid down in Article 106 (3) of Delegated Regulation (EU) 2019/715.***"

(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, ***following authorisation by the Management Board,*** financial support may cover the full investment costs of equipment, ***and*** infrastructure***. The Management Board may specify the criteria under which financial support may cover the full costs in the financial rules in accordance with paragraph 1*** 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."

(40a) Article 68 is amended as follows:

(a) paragraph 1 is replaced by the following:

"***1. By... [five years after entry into force of this amending Regulation] and every five years thereafter, the Commission shall ensure that an evaluation assessing, in particular, the impact, effectiveness and efficiency of Europol and of its working practices is carried out. The evaluation may, in particular, address the possible need to modify the structure, operation, field of action and tasks of Europol, and the financial implications of any such modification.***"

(b) 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, ***evaluating and*** assessing the operational benefits***impact*** of the implementation of the competences provided for in ***this Regulation, in particular with regard to Article 4(1)(r),*** Article 18(2)(e)***, Article 18*** and (5a***6a***), Article 18a, Article 26 and Article 26a***and Articles 18a, 26, 26a and 26b*** with regard to Europol's objectives ***as set out in Article 3***. The report shall cover***assess*** the impact of those competences on fundamental rights and freedoms as enshrined in the Charter***. It shall also provide a cost-benefit analysis of the extension to Europol's mandate*** of Fundamental Rights.."

(42) A new Article 74a is inserted:

"***Article 74a***

Transitional arrangements concerning the processing of personal data in support of a criminal investigation

1. Where a Member State, the EPPO or Eurojust provided personal data outside the categories of data subjects listed in Annex II to Europol prior to the entry into force of Amending Regulation XX, Europol may process that personal data in accordance with Article 18a where:

(a) that Member State, the EPPO or Eurojust informs Europol, within three months from the date of entry into force of Amending Regulation XX, that it is authorised to process that personal data, in accordance with procedural requirements and safeguards under applicable Union or national law, in the on-going criminal investigation for which it requested Europol's support when it initially provided the data;

(b) that Member State, the EPPO or Eurojust requests Europol, within three months from the date of entry into force of Amending Regulation XX, to support that ongoing specific criminal investigation; and

(c) Europol assesses, in accordance with Article 18a(1)(b), that it is not possible to support the specific criminal investigation without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded and sent to the EDPS for information when Europol ceases to support the related specific criminal investigation.

1a. Where a Member State, the EPPO or Eurojust do not fulfil any of the requirements set out in points (a) and (b) of paragraph 1 for personal data outside the categories of data subjects listed in Annex II that they provided to Europol prior to the entry into force of Amending Regulation XX, or where the requirements set out in point (c) of paragraph 1 are not fulfilled, Europol shall not process that personal data in accordance with Article 18a. In that case, and without prejudice to Article 18(5) and Article 74b, Europol shall delete that personal data within four months from the date of entry into force of Amending Regulation XX.

2. Where a third country within the meaning of Article 18a(7) provided personal data outside the categories of data subjects listed in Annex II to Europol prior to the entry into force of Amending Regulation XX, Europol may process that personal data in accordance with Article 18a(7) where:

(a) the third country provided the personal data in support of a specific criminal investigation in one or more Member States that Europol supports;

(b) the third country acquired the data in the context of a criminal investigation in accordance with procedural requirements and safeguards applicable under its national criminal law;

(c) the third country informs Europol, within three months from the date of entry into force of Amending Regulation XX, that it is authorised to process that personal data in the on-going criminal investigation in the context of which it acquired the data;

(d) Europol assesses, in accordance with Article 18a(1)(b), that it is not possible to support the specific criminal investigation referred to in point (a) without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded and sent to the EDPS for information when Europol ceases to support the related specific criminal investigation; and

(e) Europol verifies, in accordance with Article 18a(7), that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in one or more Member States that Europol supports.

2a. Where a third country does not fulfil the requirement set out in point (c) of paragraph 2 for personal data outside the categories of data subjects listed in Annex II that it provided to Europol prior to the entry into force of Amending Regulation XX, or where any of the other requirements set out paragraph 2 are not fulfilled, Europol shall not process that personal data in accordance with Article 18a(7). In that case, and without prejudice to Article 18(5) and Article 74b, Europol shall delete that personal data within four months from the date of entry into force of Amending Regulation XX.

3. Where a Member State, the EPPO or Eurojust provided personal data outside the categories of data subjects listed in Annex II to Europol prior to the entry into force of Amending Regulation XX, it may request Europol, within three months from the date of entry into force of Amending Regulation XX, to store that data and the outcome of Europol's processing of that data where this is necessary for ensuring the veracity, reliability and traceability of the criminal intelligence process. Europol shall keep personal data outside the categories of data subjects listed in Annex II functionally separated from other data and shall only process such data for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings concerning the criminal investigation are on-going for which that data was provided.

4. Where Europol received personal data outside the categories of data subjects listed in Annex II prior to the entry into force of Amending Regulation XX, Europol shall not store that data for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process unless so requested in accordance with paragraph 3. In the absence of such a request, Europol shall delete that personal data within four months from the date of entry into force of Amending Regulation XX."

(43) A new Article 74b is inserted:

"*Article 74b*

Transitional arrangements concerning the processing of personal data held by Europol

Without prejudice to article 74a, for personal data that Europol received prior to the entry into force of Amending Regulation XX, Europol shall be able to verify if that personal data corresponds to one of the categories of data subjects set out in Annex II of this Regulation. To that end, Europol shall be able to carry out a pre-analysis of that personal data for a maximum period of 18 months counting from the day of initial receipt of the data by Europol, or in justified cases, for a longer period with the prior authorisation of the EDPS.

The total period of processing shall not exceed a period of three years counting from the day of initial receipt of the data by Europol."

Article 2

This Regulation shall enter into force on the day 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*