I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2022/991 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 8 June 2022

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 in 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 [1],

Whereas:

(1) The European Union Agency for Law Enforcement Cooperation (Europol) was established by Regulation (EU) 2016/794 of the European Parliament and of the Council [2] to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.

(2) Europe faces a security landscape in flux, with evolving and increasingly complex security threats. Terrorists and other criminals exploit the digital transformation and new technologies, in particular both the inter-connectivity and the blurring of the boundaries between the physical and the digital world, for example by concealing their crimes and their identities through the use of increasingly sophisticated techniques. Terrorists and other criminals have proven their ability to adapt their modes of operation and to develop new criminal activities in times of crisis, including by leveraging technology-enabled tools to multiply and expand the range and scale of their criminal activities. Terrorism remains a significant threat to the freedom and way of life of Union citizens.

(3) Evolving and complex threats spread across borders, cover 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 and cross-border cooperation do not suffice to address those transnational security threats, competent authorities of the Member States 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 increased substantially. Furthermore, the new threat environment changes the scope and type of support Member States need and expect from Europol to keep citizens safe.

[1] Position of the European Parliament of 4 May 2022 (not yet published in the Official Journal) and decision of the Council of 24 May 2022.

[2] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

(4) Additional tasks should therefore be conferred upon Europol by this Regulation to allow Europol to better support competent authorities of the Member States 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 European Union (TEU). Europol's reinforced mandate should be balanced with strengthened safeguards with regard to fundamental rights and increased accountability, liability and oversight, including parliamentary oversight and oversight through the Management Board of Europol ('the Management Board'). To allow Europol to fulfil its reinforced mandate, it should be provided with adequate human and financial resources to support its additional tasks.

(5) As the Union 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 special intervention units of the Member States cooperate on the basis of Council Decision 2008/617/JHA ([3]). Europol should be able to support those special intervention units by providing technical and financial support, complementing the efforts undertaken by Member States.

(6) In recent years, large-scale cyberattacks, including attacks originating in third countries, have targeted public and private entities alike across many jurisdictions within the Union and outside it, affecting various sectors including transport, health and financial services. The prevention, detection, investigation and prosecution of such cyberattacks is supported by coordination and cooperation between relevant actors, including the European Union Agency for Cybersecurity (ENISA) established by Regulation (EU) 2019/881 of the European Parliament and of the Council ([4]), competent authorities on the security of network and information systems within the meaning of Directive (EU) 2016/1148 of the European Parliament and of the Council ([5]), competent authorities of the Member States and private parties. In order to ensure effective cooperation between all relevant actors at Union and national level on cyberattacks and cyber threats, Europol should cooperate with ENISA in particular through the exchange of information and analytical support in areas that fall within their respective competences.

(7) High-risk criminals play a leading role in criminal networks and their criminal activities pose a high risk for 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 the members and the leading members of those networks, their criminal activities and their financial assets.

(8) The threats posed by serious crime require a coordinated, coherent, multi-disciplinary and multi-agency response. Europol should be able to facilitate and support intelligence-led, Member State-driven security initiatives that aim to identify, prioritise and address serious crime threats, such as the European Multidisciplinary Platform Against Criminal Threats (EMPACT). Europol should be able to provide administrative, logistical, financial and operational support to such initiatives.

(9) 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 ([6]), 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 that fall within Europol's objectives. Within the framework of its objectives and its task of supporting the Member States in preventing and combating serious crime and terrorism, Europol should support the Member States in processing data provided by third countries or international organisations to it by proposing the possible entry by Member States of alerts in SIS under a new

([3]) Council Decision 2008/617/JHA of 23 June 2008 on the improvement of cooperation between the special intervention units of the Member States of the European Union in crisis situations (OJ L 210, 6.8.2008, p. 73).

([4]) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

([5]) 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).

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

category of information alerts in the interest of the Union ('information alerts'), in order to make those information alerts available to the end-users of SIS. To that end, a periodic reporting mechanism should be put in place in order to ensure that Member States and Europol are informed about the outcome of the verification and analysis of those data and about whether the information has been entered in SIS. The modalities for Member States' cooperation for the processing of such data and the entry of alerts in SIS, in particular as concerns the fight against terrorism, should be subject to continuous coordination among the Member States. The Management Board should specify the criteria on the basis of which it should be possible for Europol to issue proposals for the entry of such information alerts in SIS.

(10) Europol has an important role to play in support of the evaluation and monitoring mechanism to verify the application of the Schengen *acquis* established by Council Regulation (EU) No 1053/2013 ([7]). Europol should therefore, on request of the Member States, contribute with its expertise, analyses, reports and other relevant information to the evaluation and monitoring mechanism to verify the application of the Schengen *acquis*.

(11) Risk assessments help to anticipate new trends and to address new threats posed by serious crime and terrorism. To support the Commission and the Member States in carrying out effective risk assessments, Europol should provide the Commission and the Member States with threat assessment analyses based on the information it holds on criminal phenomena and trends, without prejudice to Union law on customs risk management.

(12) In order for Union funding for security research to achieve its aim of ensuring that that research develop its full potential and address the needs of law enforcement, Europol should assist the Commission in identifying key research themes and in drawing up and implementing the Union framework programmes for research and innovation that are relevant to Europol's objectives. Where relevant, it should be possible for Europol to disseminate the results of its research and innovation activities as part of its contribution to creating synergies between the research and innovation activities of relevant Union bodies. When designing and conceptualising research and innovation activities relevant to Europol's objectives, Europol should be able, where appropriate, to consult the Joint Research Centre (JRC) of the Commission. Europol should take all necessary measures to avoid conflicts of interest. Where Europol assists the Commission in identifying key research themes and in drawing up and implementing a Union framework programme, Europol should not receive funding from that programme. It is important that Europol is able to rely upon the provision of adequate funding in order to be able to assist the Member States and the Commission in the area of research and innovation.

(13) It is possible for the Union and the Member 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 ([8]) 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 significant implications for security and public order, in particular when such technologies are used by competent authorities of the Member States. Given the involvement of Europol in monitoring emerging technologies and its involvement in developing new ways of using those technologies for law enforcement purposes, in particular through its Innovation Lab and through the EU Innovation Hub for Internal Security, Europol has extensive knowledge regarding the opportunities offered by such technologies as well as the risks associated with their use. It should therefore be possible for Europol to support Member States in the screening of foreign direct investments into the Union and the related risks to security that concern undertakings that provide technologies, including software, used by Europol for the prevention and investigation of crimes that fall within Europol's objectives or critical technologies that could be used to facilitate terrorism. In that 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, whether there is a serious risk that the foreign investor engages in illegal or criminal activities and whether the foreign investor is controlled directly or indirectly by the government of a third country, including through subsidies.

([7]) Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen *acquis* and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen (OJ L 295, 6.11.2013, p. 27).

([8]) 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 79 I, 21.3.2019, p. 1).

(14) Europol provides specialised expertise for combating serious crime and terrorism. Upon request by a Member State, Europol staff should be able to provide operational support to the competent authorities of that Member State 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 during the execution of investigative measures in that Member State. Europol staff should not have the power to execute investigative measures.

(15) 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 combating forms of crime which affect a common interest covered by a Union policy. To strengthen that support, the Executive Director of Europol ('the Executive Director') should be able to propose to the competent authorities of a Member State that they initiate, conduct or coordinate the investigation of a crime which concerns only that Member State but affects a common interest covered by a Union policy. Europol should inform Eurojust and, where relevant, the European Public Prosecutor's Office ('the EPPO') established by Council Regulation (EU) 2017/1939 ([9]), of any such proposal.

(16) Publishing the identity and certain personal data of suspects or convicted individuals who are wanted on the basis of a national judicial decision increases the chances of Member States locating and arresting such individuals. To support Member States in locating and arresting such individuals, Europol should be able to publish on its website information on Europe's most wanted fugitives as regards criminal offences that fall within Europol's objectives. To the same end, Europol should facilitate the provision by the public of information on those individuals to the Member States and Europol.

(17) Once Europol ascertains that personal data that it receives fall within its objectives, it should be able to process those personal data in the following four situations. In the first situation, the personal data received relate to any of the categories of data subjects listed in Annex II of Regulation (EU) 2016/794 ('Annex II'). In the second situation, the personal data received consist of investigative data that contain data that do not relate to any of the categories of data subjects listed in Annex II but have been provided, pursuant to a request for Europol's support for a specific criminal investigation, by a Member State, the EPPO, Eurojust or a third country, provided that that Member State, the EPPO, Eurojust or that third country is authorised to process such investigative data in accordance with procedural requirements and safeguards applicable under Union and national law. In that situation, Europol should be able to process those investigative data for as long as it supports that specific criminal investigation. In the third situation, the personal data received might not relate to the categories of data subjects listed in Annex II and have not been provided pursuant to a request for Europol's support for a specific criminal investigation. In that situation, it should be possible for Europol to verify whether those personal data relate to any of those categories of data subjects. In the fourth situation, the personal data received have been submitted for the purpose of research and innovation projects and do not relate to the categories of data subjects listed in Annex II.

(18) In accordance with Article 73 of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([10]), where applicable and as far as possible, Europol is to make a clear distinction between the personal data that relate to the different categories of data subjects listed in Annex II.

(19) Where Member States use Europol's infrastructure for the exchange of personal data on crimes that do not fall within Europol's objectives, Europol should not have access to those data and should be considered to be a processor pursuant to Article 87 of Regulation (EU) 2018/1725. In those cases, Europol should be able to process data that do not relate to the categories of data subjects listed in Annex II. Where Member States use Europol's infrastructure for the exchange of personal data on crimes that fall within Europol's objectives and where they grant Europol access to those data, the requirements linked to the categories of data subjects listed in Annex II should apply to any other processing of those data by Europol.

([9]) 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).

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

(20) While respecting the principle of data minimisation, Europol should be able to verify whether personal data received in the context of preventing and combating crimes that fall within its objectives relate to one of the categories of data subjects listed in Annex II. 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 relate to any of those categories of data subjects by checking those personal data against data it already holds, without further analysing those personal data. Such pre-analysis should take place prior to, and separate from, Europol's data processing for cross-checking, strategic analysis, operational analysis or the exchange of information, and after Europol has established that the data in question are relevant and necessary for the performance of its tasks. Once Europol has ascertained that those personal data relate to the categories of data subjects listed in Annex II, Europol should be able to process those personal data for cross-checking, strategic analysis, operational analysis or the exchange of information. If Europol concludes that those personal data do not relate to the categories of data subjects listed in Annex II, it should delete those data.

(21) The categorisation of personal data in a given data set may change over time as a result of new information that becomes available in the context of criminal investigations, for example regarding additional suspects. For that reason, Europol should be allowed to process personal data where it is strictly necessary and proportionate for the purpose of determining the categories of data subjects to which the data in question relate for a period of up to 18 months from the moment Europol ascertains that those data fall within its objectives. Europol should be able to extend that period up to three 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 event, after the end of the maximum processing period, Europol should delete the personal data.

(22) The amount of data collected in criminal investigations have been increasing in size and data sets have become more complex. Member States submit large and complex data sets to Europol, requesting Europol's operational analysis to identify links to crimes other than that which is the subject of the investigation in the context of which they were collected and to criminals in other Member States and outside the Union. Since Europol can detect such cross-border links more effectively than the Member States through their own analysis of the data, Europol should be able to support Member States' criminal investigations by processing large and complex data sets to identify such cross-border links provided that the strict requirements and safeguards set out in this Regulation are complied with. Where necessary to support an ongoing specific criminal investigation in a Member State effectively, Europol should be able to process investigative data that the competent authorities of the Member States are authorised to process in that specific criminal investigation in accordance with procedural requirements and safeguards applicable under their national law and subsequently submitted to Europol. That should include personal data in cases where a Member State has not been able to ascertain whether those data relate to the categories of data subjects listed in Annex II. Where a Member State, the EPPO or Eurojust provides Europol with investigative data and requests Europol's support for an ongoing specific criminal investigation, Europol should be able to process those data for as long as it supports that specific criminal investigation, in accordance with procedural requirements and safeguards applicable under Union or national law.

(23) To ensure that any data processing performed in the context of a criminal investigation is necessary and proportionate, Member States should ensure compliance with Union and national law when they submit investigative data to Europol. When submitting investigative data to Europol to request Europol's support for a specific criminal investigation, Member States should consider the scale and complexity of the data processing involved and the type and importance of the investigation. Member States should inform Europol when, in accordance with procedural requirements and safeguards applicable under their national law, they are no longer authorised to process data in the ongoing specific criminal investigation in question. Europol should only process personal data that do not relate to the categories of data subjects listed in Annex II where it assesses that it is not possible to support an ongoing specific criminal investigation without processing those personal data. Europol should document that assessment. Europol should keep such data functionally separate from other data and should only process them where necessary for its support to the ongoing specific criminal investigation in question, such as in case of a new lead.

(24) Europol should also be able to process personal data that are necessary for its support to a specific criminal investigation in one or more Member States where those data are provided by a third country, provided that: the third country is the subject of an adequacy decision in accordance with Directive (EU) 2016/680 of the European Parliament and of the Council [11] ('adequacy decision'); an international agreement with that third country has been concluded by the Union pursuant to Article 218 of the Treaty on the Functioning of the European Union (TFEU) that includes the transfer of personal data for law enforcement purposes ('international agreement'); a cooperation agreement allowing for the exchange of personal data has been concluded between Europol and the third country prior to the entry into force of Regulation (EU) 2016/794 ('cooperation agreement'); or appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument or Europol concludes, based on an assessment of all the circumstances surrounding the transfer of personal data, that those safeguards exist in that third country and provided that the third country obtained 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 investigative data to Europol, Europol should verify that the amount of personal data is not manifestly disproportionate in relation to the specific criminal investigation that Europol supports in the Member State concerned, and, as far as possible, that there are no objective indications that investigative data have been collected in the third country in obvious violation of fundamental rights. Where Europol concludes that those conditions are not met, it should not process the data and should delete them. Where a third country provides investigative data to Europol, Europol's Data Protection Officer should be able to notify the EDPS, where appropriate.

(25) To ensure that a Member State can use Europol's analytical reports in the context of judicial proceedings following a criminal investigation, Europol should be able to store the related investigative data upon request by that Member State, the EPPO or Eurojust, for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process. Europol should keep such data functionally separate from other data and only for as long as the judicial proceedings related to that criminal investigation are ongoing in the Member State. Moreover, there is a need to ensure access of competent judicial authorities as well as the rights of defence, in particular the right of access of suspects or accused persons or their lawyers to the materials of the case. To that end, Europol should log all evidence and the methods by which that evidence has been produced or obtained by Europol to allow for effective scrutiny of evidence by the defence.

(26) Europol should be able to process personal data it received before the entry into force of this Regulation that do not relate to the categories of data subjects listed in Annex II, in accordance with this Regulation, in two situations. In the first situation, 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 requirements set out in the transitional arrangements concerning the processing of personal data received in support of a criminal investigation are complied with. In the second situation, Europol should also be able to verify whether such personal data relate to one of the categories of data subjects listed in Annex II by carrying out a pre-analysis of those personal data within a period of up to 18 months from the date the data were first received, or in justified cases and with the prior authorisation of the EDPS, for a longer period. The maximum period of processing of personal data for the purpose of such pre-analysis should not exceed three years from the date the data were first received by Europol.

(27) Cross-border cases of serious crime or terrorism require close cooperation between the competent authorities of the Member States concerned. Europol provides tools to support such cooperation in investigations, in particular through the exchange of information. To further enhance such cooperation in specific criminal investigations by way of joint operational analysis, Member States should be able to allow other Member States to directly access the information they provided to Europol, without prejudice to any general or specific restrictions they indicated on access to that information. Any processing of personal data by Member States in joint operational analysis should take place in accordance with this Regulation and Directive (EU) 2016/680.

[11] 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).

(28) Europol and the EPPO should conclude a working arrangement setting out the modalities of their cooperation, taking due account of their respective competences. Europol should work closely with the EPPO and actively support investigations of the EPPO upon request by it, including by providing analytical support and relevant information. Europol should also cooperate with the EPPO from the moment a suspected offence is reported to the EPPO until the moment the EPPO 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 which notifies only Europol in the case of a hit, in accordance with this Regulation, including any restrictions indicated by the provider of the information to Europol. If the information is covered by a restriction indicated by a Member State, Europol should refer the matter to that Member State, in order for it to comply with its obligations under Regulation (EU) 2017/1939. The Member State concerned should subsequently inform the EPPO in accordance with its national procedure. The rules on the transmission of personal data to Union bodies set out in this Regulation should apply to Europol's cooperation with the EPPO. Europol should also be able to support the investigations of the EPPO by way of analysis of large and complex data sets in accordance with the safeguards and data protection guarantees provided for in this Regulation.

(29) 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 without undue delay to OLAF any information in respect of which OLAF could exercise its competence. The rules on the transmission of personal data to Union bodies set out in this Regulation should apply to Europol's cooperation with OLAF.

(30) Serious crime and terrorism often have links outside 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. Where it is essential to the investigation into a specific crime that falls within Europol's objectives, the Executive Director should be allowed, on a case-by-case basis, to authorise a category of transfers of personal data to third countries, where that category of transfers relates to the same specific situation, consists of the same categories of personal data and the same categories of data subjects, is necessary and proportionate for the purpose of investigating a specific crime and meets all the requirements of this Regulation. It should be possible for individual transfers covered by a category of transfers to include only some of the categories of personal data and categories of data subjects whose transfer is authorised by the Executive Director. It should also be possible to authorise a category of transfers of personal data in the following specific situations: where the transfer of personal data is necessary in order to protect the vital interests of the data subject or of another person; where the transfer of personal data is essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country; where the purpose of the transfer of personal data is to safeguard the legitimate interests of the data subject; or, in individual cases, is for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions or 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.

(31) Transfers that are not based on an authorisation by the Executive Director, an adequacy decision, an international agreement or a cooperation agreement should be allowed only where appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument or where Europol concludes, based on an assessment of all the circumstances surrounding the transfer of personal data, that those safeguards exist. For the purposes of that assessment, 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, and whether the transfer of personal data is to be subject to confidentiality obligations and to the principle of specificity, ensuring that the data are not processed for purposes other than the transfer. In addition, it is important that Europol take into account whether the personal data could be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. Europol should be able to require additional safeguards.

(32) To support Member States in cooperating with private parties where those private parties hold information relevant for preventing and combating serious crime and terrorism, Europol should be able to receive personal data from private parties and, in specific cases where necessary and proportionate, exchange personal data with private parties.

(33) Criminals increasingly use services offered by private parties to communicate and carry out illegal activities. Sex offenders exploit children and share pictures and videos constituting child sexual abuse material worldwide on online platforms or with peers via number-independent interpersonal communications services. Terrorists use 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 other digital skills of the general public using phishing and social engineering to commit other types of cybercrime such as online scams, ransomware attacks or payment fraud. As a result of the increased use of online services by criminals, private parties hold increasing amounts of personal data, including subscriber, traffic and content data, that is potentially relevant for criminal investigations.

(34) Given the borderless nature of the internet, it is possible that the online service provider and the digital infrastructure in which the personal data are stored are each subject to different national jurisdictions, either within the Union or outside it. Private parties may therefore hold data sets that are relevant for law enforcement and that contain personal data that fall within the competence of multiple jurisdictions as well as personal data that cannot easily be attributed to any specific jurisdiction. The competent authorities of the Member States can find it difficult to effectively analyse such multi-jurisdictional or non-attributable data sets through national solutions. Furthermore, there is currently no single point of contact for private parties who decide to lawfully and voluntarily share data sets with competent authorities of the Member States. Accordingly, Europol should have measures in place to facilitate cooperation with private parties, including with respect to the exchange of information.

(35) To ensure that private parties have a point of contact at Union level to lawfully and voluntarily provide multi-jurisdictional data sets or data sets that cannot easily be attributed 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 crimes under their respective jurisdictions, in accordance with this Regulation. That information could include reports relating to moderated content that can reasonably be assumed to be linked to the criminal activities that fall within Europol's objectives.

(36) To ensure that Member States receive the information necessary to initiate investigations to prevent and combat serious crime and terrorism without undue delay, Europol should be able to process and analyse personal data in order to identify the national units concerned and forward to those national units the personal data and any results of its analysis and verification of such data that are relevant for the purposes of establishing jurisdiction and investigating the crimes concerned under their respective jurisdictions. Europol should also be able to forward the personal data and results of its analysis and verification of such data that are relevant for the purpose of establishing jurisdiction to contact points or authorities of third countries concerned which are the subject of an adequacy decision, or with which an international agreement or a cooperation agreement has been concluded, or where appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument or Europol concludes, based on an assessment of all the circumstances surrounding the transfer of personal data, that those safeguards exist in those third countries. Where the third country concerned is not the subject of an adequacy decision or is not party to an international agreement or to a cooperation agreement or in the absence of a legally binding instrument, or where Europol has not concluded that appropriate safeguards exist, Europol should be able to transfer the result of its analysis and verification of such data to the third country concerned in accordance with this Regulation.

(37) In accordance with Regulation (EU) 2016/794, in certain cases and subject to conditions, it can be necessary and proportionate for Europol to transfer personal data to private parties which are not established within the Union or in a third country which is the subject of an adequacy decision or with which an international agreement or a cooperation agreement has been concluded, or where appropriate safeguards with regard to the protection of personal data are not provided for in a legally binding instrument or Europol has not concluded that appropriate safeguards exist. In such cases, the transfer should be subject to prior authorisation by the Executive Director.

(38) To ensure that Europol can identify all relevant national units concerned, it should be able to inform private parties if the information they provided is insufficient to enable Europol to identify the national units concerned. This would enable those private parties to decide whether it is in their interest to share additional information with Europol and whether they can lawfully do so. To that end, Europol should be able to inform private parties of missing information, as far as this is strictly necessary for the sole purpose of identifying the national units concerned. Special safeguards should apply to transfers of information from Europol to private parties where the private party concerned is not established within the Union or in a third country which is the subject of an adequacy decision or with which an international agreement or a cooperation agreement has been concluded, or where appropriate safeguards with regard to the protection of personal data are not provided for in a legally binding instrument or Europol has not concluded that appropriate safeguards exist.

(39) Where Member States, third countries, international organisations or private parties share with Europol multi-jurisdictional data sets or data sets that cannot be attributed to one or more specific jurisdictions, it is possible that those data sets are linked to personal data held by private parties. In such situations, it should be possible for Europol to send a request to Member States, via their national units, to obtain the personal data held by private parties which are established or have a legal representative in the territory of those Member States. Such a request should only be made where obtaining additional information from such private parties is necessary to identify the national units concerned. The request should be reasoned and as precise as possible. The relevant personal data, which should be the least sensitive possible and strictly limited to what is necessary and proportionate for the purpose of identifying the national units concerned, should be provided to Europol in accordance with the applicable law of the Member States concerned. The competent authorities of the Member States concerned should assess Europol's request and decide in accordance with their national law whether to accede to it. Any data processing by private parties carried out when processing such requests from the competent authorities of the Member States should remain subject to the applicable law, in particular with regard to data protection. Private parties should provide the competent authorities of the Member States with the requested data for their further transmission to Europol. In many cases, it is possible that the Member States concerned are not able to establish a link to their jurisdiction other than by virtue of the fact that the private party holding the relevant data is established or legally represented in their jurisdiction. Notwithstanding whether they have jurisdiction as regards the specific crime, Member States should in any event ensure that their competent authorities can obtain personal data from private parties for the purpose of supplying Europol with the information necessary for it to achieve its objectives, in full compliance with procedural guarantees under their national law.

(40) To ensure that Europol does not keep the personal data received directly from private parties longer than necessary to identify the national units concerned, time limits for the storage of personal data by Europol should apply. Once Europol has exhausted all means at its disposal to identify the national units concerned, and cannot reasonably expect to identify any further national units concerned, the storage of those personal data is no longer necessary and proportionate for the purpose of identifying the national units concerned. Europol should erase the personal data within four months after their last transmission, transfer to a national unit or transfer to the contact point of a third country or an authority of a third country has taken place, unless, in compliance with Union and national law, a national unit, contact point or authority concerned resubmits the personal data as their data to Europol within that period. If the resubmitted personal data were part of a larger set of personal data, Europol should keep only those personal data which have been resubmitted by a national unit, contact point or authority concerned.

(41) Cooperation by Europol with private parties should neither duplicate nor interfere with the activities of the Financial Intelligence Units (FIUs) established pursuant to Directive (EU) 2015/849 of the European Parliament and of the Council ([12]), and should only concern information that is not already to be provided to FIUs in accordance with that Directive. Europol should continue to cooperate with FIUs, in particular via the national units.

([12]) 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).

(42) Europol should be able to provide the support necessary for competent authorities of the Member States to interact with private parties, in particular by providing the necessary infrastructure for such interaction, for example, when competent authorities of the Member States refer terrorist content online, send removal orders concerning such content to online service providers pursuant to Regulation (EU) 2021/784 of the European Parliament and of the Council ([13]) or exchange information with private parties in the context of cyberattacks. Where Member States use Europol infrastructure for exchanges of personal data on crimes that do not fall within Europol's objectives, Europol should not have access to those data. Europol should ensure by technical means that its infrastructure is strictly limited to providing a channel for such interactions between the competent authorities of the Member States and a private party, and that Europol 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.

(43) Terrorist attacks trigger the large scale dissemination of terrorist content via online platforms depicting harm to life or physical integrity, or calling for imminent harm to life or physical integrity, thereby enabling the glorification and provision of training for terrorism, and eventually the radicalisation and recruitment of other individuals. 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 combat the crimes that fall within Europol's objectives, Europol should be able to support Member States' actions in effectively addressing the dissemination of terrorist content in the context of online crisis situations stemming from ongoing or recent real-world events, the online dissemination of online child sexual abuse material, and to support the actions of online service providers in compliance 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, including unique, non-reconvertible digital signatures ('hashes'), IP addresses or URLs related to such content, with private parties established within the Union or in a third country which is the subject of an adequacy decision, or, in the absence of such a decision, with which an international agreement or a cooperation agreement has been concluded or where appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument or Europol concludes, based on an assessment of all the circumstances surrounding the transfer of personal data, that those safeguards exist in that third country. Such exchanges of personal data should only take place for the purposes of removing terrorist content and online child sexual abuse material, in particular where the exponential multiplication and virality of that content and material across multiple online service providers are anticipated. Nothing in this Regulation should be understood as precluding a Member State from using removal orders provided for in Regulation (EU) 2021/784 as an instrument to address terrorist content online.

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

(45) Regulation (EU) 2018/1725 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 applies to the processing of administrative personal data by Europol that are unrelated to criminal investigations, such as staff data, Article 3, point (2), and Chapter IX of that Regulation, which regulate the processing of personal data, do not currently apply to Europol. To ensure the uniform and consistent protection of natural persons with regard to the processing of personal data, Chapter IX of Regulation (EU) 2018/1725 should apply 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 processing operations should be reinforced, in line with the relevant powers applicable to the processing of administrative personal data that apply to all Union institutions, bodies, offices and agencies under Chapter VI of Regulation (EU) 2018/1725. To that end, where Europol processes personal data for operational

([13]) 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).

purposes, the EDPS should be able to order Europol to bring processing operations into compliance with this Regulation and to order the suspension of data flows to a recipient in a Member State, a third country or an international organisation, and should be able to impose an administrative fine in the case of non-compliance by Europol.

(46) 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 of the European Parliament and of the Council ([14]). 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 under Article 3, point (18), of Regulation (EU) 2018/1725 only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

(47) The prior consultation mechanism involving the EDPS provided for by Regulation (EU) 2018/1725 is an important safeguard for new types of processing operations. However, that mechanism should not apply to specific individual operational activities, such as operational analysis projects, but to the use of new information technology (IT) systems for the processing of personal data and any substantial changes to those systems that would involve a high risk to the rights and freedoms of data subjects. The period within which the EDPS should be required to provide written advice on such consultations should not be capable of being suspended. In the case of processing activities of substantial significance for the performance of Europol's tasks, which are particularly urgent, it should be possible for Europol, on an exceptional basis, to already begin processing after the prior consultation has been launched, even if the time limit for providing written advice by the EDPS has not yet expired. Such urgency may arise in situations of substantial significance for the performance of Europol's tasks, when processing is necessary to prevent and fight an immediate threat of a crime that falls within Europol's objectives and to protect the vital interests of the data subject or another person. Europol's Data Protection Officer 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. Europol's Data Protection Officer should oversee such processing. The EDPS should be able to exercise its powers with respect to such processing.

(48) Given the challenges posed by the rapid technological development and the exploitation of new technologies by terrorists and other criminals to the security of the Union, the competent authorities of the Member States need to strengthen their technological capabilities to identify, secure and analyse the data needed to investigate criminal offences. Europol should be able to support Member States in the use of emerging technologies, in exploring new approaches and in developing common technological solutions for Member States to better prevent and counter crimes that fall within Europol's objectives. At the same time, Europol should ensure that the development, use and deployment of new technologies are guided by the principles of transparency, explainability, fairness and accountability, do not undermine fundamental rights and freedoms and are in compliance with Union law. To that end, Europol should be able to conduct research and innovation projects regarding matters covered by this Regulation within the general scope for the research and innovation projects established by the Management Board in a binding document. Such document should be updated where appropriate and made available to the EDPS. It should be possible for those projects to include the processing of personal data only where certain conditions are met, namely that the processing of personal data is strictly necessary, the objective of the relevant project cannot be achieved through the use of non-personal data, such as synthetic or anonymous data, and that full respect for fundamental rights, in particular non-discrimination, is ensured.

The processing of special categories of personal data for research and innovation purposes should only be allowed where it is strictly necessary. Given the sensitivity of such processing, appropriate additional safeguards, including pseudonymisation, should apply. To prevent bias in algorithmic decision-making, Europol should be allowed to process personal data that do not relate to the categories of data subjects listed in Annex II. Europol should keep logs of all personal data processing carried out in the context of its research and innovation projects only for the purpose of verifying the accuracy of the outcome of the data processing and only for as long as necessary for that verification. 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 projects, it is important that Europol step up its cooperation with relevant networks of Member States' practitioners and other Union agencies within their respective competences in that area, and support other related forms of cooperation such as secretarial support to the EU Innovation Hub for Internal Security as a collaborative network of innovation labs.

([14]) Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

(49) Europol should play a key role in assisting Member States in developing new technological solutions based on artificial intelligence that are relevant to the achievement of Europol's objectives and that benefit competent authorities of the Member States throughout the Union. That assistance should be provided while fully respecting 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 that is subject to robust safeguards in terms of security, safety, transparency, explainability and fundamental rights.

(50) Europol should inform the EDPS prior to the launch of its research and innovation projects that involve the processing of personal data. Europol should either inform or consult its Management Board, in accordance with certain criteria that should be set out in relevant guidelines. Europol should not process data for the purpose of research and innovation projects 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 for such processing for that purpose. For each project, Europol should carry out, prior to the processing, a data protection impact assessment to ensure full respect with the right to data protection and all other fundamental rights and freedoms of data subjects. The data protection impact assessment should include an assessment of the appropriateness, necessity and proportionality of the personal data to be processed for the specific purpose of the project, including the requirement of data minimisation and an assessment 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.

(51) 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 manner in which Europol uses additional tools and capabilities provided to it under this Regulation, Europol should provide the Joint Parliamentary Scrutiny Group (JPSG) and the Member States with detailed annual information on the development, use and effectiveness of those tools and capabilities and the result of their use, 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 Management Board on behalf of the JPSG and to discuss the consolidated annual activity report, the single programming document 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 Management Board and the JPSG in accordance with this Regulation. The Management Board, together with the representatives of the JPSG, should be able to 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 JPSG.

(52) Following a proposal from the Executive Director, the Management Board should designate a Fundamental Rights Officer who should be responsible for supporting Europol in safeguarding the respect for fundamental rights in all its activities and tasks, in particular Europol's research and innovation projects and the exchange of personal data with private parties. It should be possible to designate a member of Europol's existing staff who has received special training in fundamental rights law and practice as the Fundamental Rights Officer. 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.

(53) Since the objective of this Regulation, namely 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, cannot be sufficiently achieved by the Member States but can rather, by reason of 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 TEU. 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.

(54) 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 TEU and the TFEU, Ireland has notified its wish to take part in the adoption and application of this Regulation.

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

(56) The EDPS was consulted, in accordance with Article 42(1) of Regulation (EU) 2018/1725, and has delivered an opinion on 8 March 2021 ([15]).

(57) 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 ('the Charter'), in particular the right to respect for private and family life and the right to the protection of personal data as provided for by Articles 7 and 8 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 should include 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, in particular the 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 should be limited to that which is strictly necessary and proportionate, and subject to clear conditions, strict requirements and effective supervision by the EDPS.

(58) Regulation (EU) 2016/794 should therefore be amended accordingly.

(59) In order to allow for the prompt application of the measures provided for in this Regulation, it should enter into force on the day following that of its publication in the *Official Journal of the European Union*,

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 personal data processed by Europol other than operational personal data;'

(c) the following points are added:

'(q) "investigative data" means data that a Member State, the European Public Prosecutor's Office ("the EPPO") established by Council Regulation (EU) 2017/1939 (*), Eurojust or a third country is authorised to process in an ongoing criminal investigation related to one or more Member States, in accordance with procedural requirements and safeguards applicable under Union or national law, that a Member State, the EPPO, Eurojust or a third country submitted to Europol in support of such an ongoing criminal investigation and that contain personal data that do not relate to the categories of data subjects listed in Annex II;

(r) "terrorist content" means terrorist content as defined in Article 2, point (7), of Regulation (EU) 2021/784 of the European Parliament and of the Council (**);

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

([15]) OJ C 143, 23.4.2021, p. 6.

(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, provided that there is a link, or a reasonable suspicion of a link, to terrorism or violent extremism and that the potential exponential multiplication and virality of that content across multiple online services are anticipated;

(u) "category of transfers of personal data" means a group of transfers of personal data where the data relate to the same specific situation, and where the transfers consist of the same categories of personal data and the same categories of data subjects;

(v) "research and innovation projects" means 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 for the achievement of Europol's objectives.

_____

(*) 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).

(**) 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).

(***) 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).';

(2) Article 4 is amended as follows:

(a) paragraph 1 is amended as follows:

(i) the following point is inserted:

'(ha) provide administrative and financial support to Member States' special intervention units as referred to in Council Decision 2008/617/JHA (*);

_____

(*) 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, p. 73).';

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

'(j) cooperate with the Union bodies established on the basis of Title V of the TFEU, with OLAF and the European Union Agency for Cybersecurity (ENISA) established by Regulation (EU) 2019/881 of the European Parliament and of the Council (*), in particular through the exchange of information and provision of analytical support in areas that fall within their respective competences;

_____

(*) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).';

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

'(m) support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including by:

(i) assisting the competent authorities of the Member States, upon their request, in responding to cyberattacks of suspected criminal origin;

(ii) cooperating with competent authorities of the Member States with regard to removal orders, in accordance with Article 14 of Regulation (EU) 2021/784; and

(iii) making referrals of online content to the online service providers concerned for their voluntary consideration of the compatibility of that content with their own terms and conditions;';

(iv) the following points are added:

'(r) support Member States in identifying persons whose criminal activities fall within the forms of crime listed in Annex I and who constitute a high risk for security;

(s) facilitate joint, coordinated and prioritised investigations regarding persons referred to in point (r);

(t) support Member States in processing data provided by third countries or international organisations to Europol on persons involved in terrorism or in serious crime and propose the possible entry by the Member States, at their discretion and subject to their verification and analysis of those data, of information alerts on third-country nationals in the interest of the Union ("information alerts") in the Schengen Information System (SIS), in accordance with Regulation (EU) 2018/1862 of the European Parliament and the Council (*);

(u) support the implementation of the evaluation and monitoring mechanism to verify the application of the Schengen *acquis* under Regulation (EU) No 1053/2013, within the scope of Europol's objectives, through the provision of expertise and analyses, where relevant;

(v) proactively monitor research and innovation activities that are relevant for the achievement of Europol's objectives and contribute to such activities by supporting related activities of Member States and by implementing its own research and innovation activities, including projects for the development, training, testing and validation of algorithms for the development of specific tools for the use by law enforcement authorities, and disseminate the results of the activities to the Member States in accordance with Article 67;

(w) contribute to creating synergies between the research and innovation activities of Union bodies that are relevant for the achievement of Europol's objectives, including through the EU Innovation Hub for Internal Security, and in close cooperation with Member States;

(x) support, upon their request, Member States' actions in addressing online crisis situations, in particular by providing private parties with the information necessary to identify relevant online content;

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

(z) cooperate, in accordance with Article 12 of Directive (EU) 2019/1153 of the European Parliament and of the Council (**), with Financial Intelligence Units (FIUs) established pursuant to Directive (EU) 2015/849 of the European Parliament and of the Council (***), through the relevant Europol national unit or, if allowed by the relevant Member State, by direct contact with the FIUs, in particular through the exchange of information and the provision of analyses to Member States to support cross-border investigations into the money laundering activities of transnational criminal organisations and terrorist financing;

(*) 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).

(**) 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).

(***) 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).';

(v) the following subparagraphs are added:

'In order for a Member State to inform, within a period of 12 months after Europol has proposed the possible entry of an information alert referred to in the first subparagraph, point (t), other Member States and Europol on the outcome of the verification and analysis of the data and on whether an alert has been entered in SIS, a periodic reporting mechanism shall be put in place.

Member States shall inform Europol of any information alerts entered in SIS and of any hit on such information alerts, and may inform, through Europol, the third country or international organisation that provided the data leading to the entry of the information alert on hits on such information alert, in accordance with the procedure set out in Regulation (EU) 2018/1862.';

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

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

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

'Europol shall also provide threat assessment analyses based on the information it holds on criminal phenomena and trends to support the Commission and the Member States in carrying out risk assessments.';

(d) the following paragraphs 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 Europol's objectives.

Where appropriate, Europol may disseminate the results of its research and innovation activities as part of its contribution to creating synergies between the research and innovation activities of relevant Union bodies in accordance with paragraph 1, first subparagraph, point (w).

Europol shall take all necessary measures to avoid conflicts of interest. Europol shall not receive funding from a given Union framework programme where it assists the Commission in identifying key research themes and in drawing up and implementing that programme.

When designing and conceptualising research and innovation activities regarding matters covered by this Regulation, Europol may, where appropriate, consult the Joint Research Centre of the Commission.

4b. Europol shall support the Member States in the screening, as regards the expected implications for security, 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 that provide technologies, including software, used by Europol for the prevention and investigation of crimes that fall within Europol's objectives.

(*) 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 79 I, 21.3.2019, p. 1).';

(e) paragraph 5 is replaced by the following:

'5. Europol shall not apply coercive measures in carrying out its tasks.

Europol staff may provide operational support to the competent authorities of the Member States during the execution of investigative measures, at their request and in accordance with their national law, in particular by facilitating cross-border information exchange, by providing forensic and technical support and by being present during the execution of those measures. Europol staff shall not, themselves, have the power to execute investigative measures.';

(f) the following paragraph is added:

'5a. Europol shall respect the fundamental rights and freedoms enshrined in the Charter of Fundamental Rights of the European Union ("the Charter"), in the performance of its tasks.';

(3) Article 6 is amended as follows:

(a) the following paragraph 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 concerns only one Member State but affects a common interest covered by a Union policy, he or she may propose to the competent authorities of the Member State concerned, via its national unit, to initiate, conduct or coordinate such a criminal investigation.';

(b) paragraph 2 is replaced by the following:

'2. The national units shall inform Europol, with regard to any request made pursuant to paragraph 1, or the Executive Director, with regard to any proposal made pursuant to paragraph 1a, of the decision of the competent authorities of the Member States, without undue delay.';

(c) paragraph 4 is replaced by the following:

'4. Europol shall immediately inform Eurojust and, where relevant, the EPPO, of any request made pursuant to paragraph 1, of any proposal made pursuant to paragraph 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. Each Member State shall ensure that its FIU, within the limits of its mandate and competence and subject to national procedural safeguards, is entitled to reply to duly justified requests that are made by Europol in accordance with Article 12 of Directive (EU) 2019/1153 regarding financial information and financial analyses, either via its national unit or, if allowed by that Member State, by direct contact between the FIU and Europol.';

(5) Article 11(1) is amended as follows:

(a) 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 of this Regulation, a single programming document as referred to in Article 32 of Commission Delegated Regulation (EU) 2019/715 (*).

(*) 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).';

(b) the following points are added:

'(v) designate the Fundamental Rights Officer referred to in Article 41c;

(w) specify the criteria on the basis of which Europol may issue the proposals for possible entry of information alerts in SIS.';

(6) Article 12 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. The Management Board shall, by 30 November of 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 Joint Parliamentary Scrutiny Group (JPSG).

Where the Management Board decides not to take into account the opinion of the Commission referred to in the first subparagraph, in whole or in part, Europol shall provide a thorough justification.

Where the Management Board decides not to take into account any of the matters raised by the JPSG in accordance with Article 51(2), point (c), Europol shall provide a thorough justification.

Once the single programming document has been adopted, the Management Board shall forward it to the Council, the Commission and the JPSG.';

(b) in paragraph 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 multi-annual budget and establishment plan. It shall include the strategy for relations with third countries and international organisations and Europol's planned research and innovation activities.';

(7) 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 attend two ordinary meetings of the Management Board per year as non-voting observers to discuss the following matters of political interest:

(a) the consolidated annual activity report referred to in Article 11(1), point (c), for the previous year;

(b) the single programming document referred to in Article 12 for the following year and the annual budget;

(c) JPSG written questions and answers;

(d) 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 at the meetings referred to in the first subparagraph.';

(8) Article 16 is amended as follows:

(a) paragraph 3 is replaced by the following:

'3. The Council or the JPSG may invite the Executive Director to report on the performance of his or her duties.';

(b) paragraph 5 is amended as follows:

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

'(d) preparing the draft single programming document referred to in Article 12 and submitting it to the Management Board, after having consulted the Commission and the JPSG;';

(ii) the following point is inserted:

'(oa) informing the Management Board of the memoranda of understanding signed with private parties;';

(9) Article 18 is amended as follows:

(a) paragraph 2 is amended as follows:

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

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

(ii) the following points are added:

'(e) research and innovation projects;

(f) supporting Member States, upon their request, in informing the public about suspects or convicted individuals who are wanted on the basis of a national judicial decision relating to a crime that falls within Europol's objectives, and facilitating the provision by the public of information on those individuals to the Member States and Europol.';

(b) the following paragraph is inserted:

'3a. If necessary to achieve the objectives of Europol's research and innovation projects, the processing of personal data for that purpose shall be carried out only in the context of Europol's research and innovation projects with clearly defined purposes and objectives, and shall be in accordance with Article 33a.';

(c) paragraph 5 is replaced by the following:

'5. Without prejudice to Article 8(4), Article 18(2), point (e), Article 18a, and data processing pursuant to Article 26(6c), where Europol's infrastructure is used for bilateral exchanges of personal data 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 the purposes of paragraph 2 of this Article are listed in Annex II.';

(d) the following paragraph is inserted:

'5a. In accordance with Article 73 of Regulation (EU) 2018/1725 of the European Parliament and of the Council (*), Europol shall, where applicable and as far as possible, make a clear distinction between the personal data that relate to the different categories of data subjects listed in Annex II.

(*) 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).';

(e) 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 shall not exceed six months from the receipt of those data.';

(f) the following paragraphs are inserted:

'6a. Prior to the processing of data pursuant to paragraph 2 of this Article, where strictly necessary for the sole purpose of determining whether personal data are in compliance with paragraph 5 of this Article, Europol may temporarily process personal data that have been provided to it pursuant to Article 17(1) and (2), including by checking those data against all data that Europol already processes in accordance with paragraph 5 of this Article.

Europol shall process personal data pursuant to the first subparagraph for a period of up to 18 months from the moment Europol ascertains that those data fall within its objectives 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 processing period. The maximum period of data processing pursuant to the first subparagraph shall be three years. Such personal data shall be kept functionally separate from other data.

Where Europol concludes that personal data referred to in the first subparagraph of this paragraph are not in compliance with paragraph 5, Europol shall delete those data and inform, where relevant, the provider of those deleted data accordingly.

6b. The Management Board, acting on a proposal from the Executive Director, after consulting the EDPS and having due regard to the principles referred to in Article 71 of Regulation (EU) 2018/1725, shall specify the conditions relating to the processing of the data referred to in paragraphs 6 and 6a of this Article, in particular with respect to the provision of, access to and the use of those data, as well as the time limits for the storage and deletion of such data, which shall not exceed those set out in paragraphs 6 and 6a of this Article.';

(10) the following Article is inserted:

'Article 18a

Processing of personal data in support of a criminal investigation

1. Where necessary for the support of an ongoing specific criminal investigation within the scope of Europol's objectives, Europol may process personal data that do not relate to the categories of data subjects listed in Annex II where:

(a) a Member State, the EPPO or Eurojust provides investigative data to Europol pursuant to Article 17(1), points (a) or (b), and requests Europol to support that investigation:

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

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

(b) Europol assesses that it is not possible to carry out the operational analysis pursuant to Article 18(2), point (c), or the cross-checking pursuant to Article 18(2), point (a), in support of that investigation without processing personal data that do not comply with Article 18(5).

The results of the assessment referred to in the first subparagraph, point (b), shall be recorded and sent to the EDPS for information when Europol ceases to support the investigation referred to in the first subparagraph.

2. Where the Member State referred to in paragraph 1, first subparagraph, point (a), is no longer authorised to process the data in the ongoing specific criminal investigation referred to in paragraph 1 in accordance with procedural requirements and safeguards under its applicable national law, it shall inform Europol.

Where the EPPO or Eurojust provides investigative data to Europol and it is no longer authorised to process the data in the ongoing specific criminal investigation referred to in paragraph 1 in accordance with procedural requirements and safeguards applicable under Union and national law, it shall inform Europol.

3. Europol may process investigative data in accordance with Article 18(2) for as long as it supports the ongoing specific criminal investigation for which the investigative data were provided in accordance with paragraph 1, first subparagraph, point (a), of this Article, and only for the purpose of supporting that investigation.

4. Europol may store the investigative data provided in accordance with paragraph 1, first subparagraph, point (a), and the outcome of its processing of those data beyond the processing period set out in paragraph 3, upon request of the provider of those investigative 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 specific criminal investigation for which those data were provided are ongoing.

The providers of investigative data referred to in paragraph 1, first subparagraph, point (a), or, with their agreement, a Member State in which judicial proceedings concerning a related criminal investigation are ongoing, may request Europol to store the investigative data and the outcome of its operational analysis of those data beyond the processing period set out in paragraph 3 for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as judicial proceedings concerning a related criminal investigation are ongoing in that other Member State.

5. Without prejudice to the processing of personal data under Article 18(6a), personal data that do not relate to the categories of data subjects listed in Annex II shall be kept functionally separate from other data and shall only be processed where necessary and proportionate for the purposes of paragraphs 3, 4 and 6 of this Article.

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

6. Paragraphs 1 to 4 of this Article shall also apply where personal data are provided to Europol by a third country as referred to in Article 25(1), point (a), (b) or (c), or in Article 25(4a), and that third country provides investigative data to Europol for operational analysis that contributes to the specific criminal investigation in one or more Member States that Europol supports, provided that the third country obtained 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 investigative data to Europol in accordance with the first subparagraph, the Data Protection Officer may, where appropriate, notify the EDPS thereof.

Europol shall verify that the amount of personal data referred to in the first subparagraph is not manifestly disproportionate in relation to the specific criminal investigation in the Member State concerned. Where Europol concludes that there is an indication that such data are manifestly disproportionate or were collected in obvious violation of fundamental rights, Europol shall not process the data and delete them.

Personal data processed pursuant to this paragraph shall be accessed by Europol only where necessary for the support of the specific criminal investigation for which they were provided. Those personal data shall be shared only within the Union.';

(11) in Article 19, paragraphs 1 and 2 are replaced by the following:

'1. A Member State, a Union body, a third country or an international organisation that provides information to Europol shall determine the purpose or purposes for which that information is to be processed, in accordance with Article 18.

Where a provider of information referred to in the first subparagraph has not complied with that subparagraph, 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 shall process information for a purpose different from that for which information has been provided only if authorised to do so by the provider of the information.

Information provided for the purposes referred to in Article 18(2), points (a) to (d), may also be processed by Europol for the purpose of Article 18(2), point (e), in accordance with 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.';

(12) Article 20 is amended as follows:

(a) the following paragraph is inserted:

'2a. In the framework of operational analysis projects 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 in specific investigations, without prejudice to any restrictions indicated pursuant to Article 19(2), and in accordance with the procedures set out in the guidelines referred to in Article 18(7).';

(b) in paragraph 3, the introductory wording 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, detecting, investigating and prosecuting:';

(13) the following Article is inserted:

'*Article 20a*

Relations with the European Public Prosecutor's Office

1. Europol shall establish and maintain a close relationship with the 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 support the investigations of the EPPO and cooperate with it, by providing information and analytical support, until the EPPO determines whether to prosecute or otherwise dispose of the case.

3. In order to provide information to the EPPO under paragraph 2 of this Article, Europol shall take all appropriate measures to enable the EPPO to have indirect access on the basis of a hit/no hit system to data related to offences that fall within the EPPO's competence, provided for the purposes of Article 18(2), points (a), (b) and (c). That hit/no hit system shall notify only Europol in the case of a hit and without prejudice to any restrictions indicated pursuant to Article 19(2) by the providers of information referred to in Article 19(1).

In the case of a hit, Europol shall initiate the procedure by which the information that generated the hit may be shared, in accordance with the decision of the provider of the information referred to in Article 19(1), and only to the extent that the data generating the hit are relevant for the request submitted pursuant to paragraph 2 of this Article.

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 and Article 25(2) and (3) of Regulation (EU) 2017/1939 and without prejudice to any restrictions indicated pursuant to Article 19(2) of this Regulation by the provider of the information.

Where Europol reports to the EPPO under the first subparagraph, it shall notify the Member States concerned without delay.

Where 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 that information pursuant to Article 19(2) of this Regulation, Europol shall notify the EPPO of the existence of those restrictions and refer the matter to the Member State concerned. The Member State concerned shall engage directly with the EPPO in order to comply with Article 24(1) and (4) of Regulation (EU) 2017/1939.';

(14) in Article 21, the following paragraph is added:

'8. If, while processing information in respect of a specific criminal investigation or a specific project, Europol identifies information relevant to possible illegal activity affecting the financial interest of the Union, Europol shall provide OLAF without delay with that information without prejudice to any restrictions indicated pursuant to Article 19(2) by the Member State that provided the information.

Where Europol provides OLAF with information under the first subparagraph, it shall notify the Member States concerned without delay.';

(15) 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 or private parties shall be prohibited, unless Europol has given its prior explicit authorisation.';

(16) the title of Section 2 is replaced by the following:

'Transmission, transfer and exchange of personal data';

(17) Article 24 is replaced by the following:

'*Article 24*

Transmission of personal data to Union bodies

1. Europol shall only transmit personal data to a Union body in accordance with Article 71(2) of Regulation (EU) 2018/1725, subject to any restrictions pursuant to this Regulation and without prejudice to Article 67 of this Regulation, if those data are necessary and proportionate for the legitimate performance of tasks of the recipient Union body.

2. Following a request for the transmission of personal data from another Union body, Europol shall verify the competence of the other Union body. Where Europol is unable to confirm that the transmission of the personal data is necessary in accordance with paragraph 1, Europol shall seek further information from the requesting Union body.

The requesting Union body shall ensure that the necessity of the transmission of the personal data can be verified.

3. The recipient Union body shall process the personal data referred to in paragraphs 1 and 2 only for the purposes for which they were transmitted.';

(18) Article 25 is amended as follows:

(a) paragraph 1 is amended as follows:

(i) the introductory wording is amended as follows:

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

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

'(a) a decision of the Commission adopted in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection ("adequacy decision");';

(b) paragraph 3 is deleted;

(c) the following paragraph 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 personal data and has concluded that appropriate safeguards exist with regard to the protection of personal data.';

(d) paragraph 5 is amended as follows:

(i) the introductory wording is replaced by the following:

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

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

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

(e) paragraph 8 is replaced by the following:

'8. Europol shall inform the EDPS about categories of transfers under paragraph 4a, point (b). Where a transfer is made in accordance with 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 competent authority referred to in this Article, about the justification for the transfer and about the personal data transferred.';

(19) Article 26 is amended as follows:

(a) in paragraph 1, point (c) is replaced by the following:

'(c) an authority of a third country or an international organisation as referred to in Article 25(1), point (a), (b) or (c), or in Article 25(4a).';

(b) paragraph 2 is replaced by the following:

'2. Where Europol receives personal data directly from private parties, it may process those personal data in accordance with Article 18 in order to identify the national units concerned, as referred to in paragraph 1, point (a), of this Article. Europol shall forward the personal data and any relevant results from the necessary processing of those 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 those data for the purpose of establishing jurisdiction, in accordance with Article 25, to contact points and authorities concerned, as referred to in paragraph 1, points (b) and (c), of this Article. If Europol cannot identify any national units concerned, or has already forwarded the relevant personal data to all the identified respective national units concerned and it is not possible to identify further national units concerned, it shall erase the data, unless 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).';

(c) the following paragraph is inserted:

'2a. Any cooperation by Europol with private parties shall neither duplicate nor interfere with the activities of Member States' FIUs, and shall not concern information that is to be provided to FIUs for the purposes of Directive (EU) 2015/849.';

(d) paragraph 4 is replaced by the following:

'4. Where Europol receives personal data from a private party established in a third country, Europol shall forward those data and the results of its analysis and verification of those data only to a Member State, or to a third country concerned as referred to in Article 25(1), point (a), (b) or (c), or in Article 25(4a).

Without prejudice to the first subparagraph of this paragraph, Europol may transfer the results referred to in the first subparagraph of this paragraph to the third country concerned pursuant to Article 25(5) or (6).';

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

'5. Europol shall not transmit or transfer personal data to private parties, except in the following cases and provided that such transmission or transfer is strictly necessary and proportionate, to be determined on a case by case basis:

(a) the transmission or transfer is undoubtedly in the interests of the data subject;

(b) the transmission or transfer is strictly necessary in the interests of preventing the imminent perpetration of a crime, including terrorism, that falls within Europol's objectives;

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

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

(ii) the fundamental rights and freedoms of the data subjects concerned do not override the public interest that requires those personal data be transmitted or transferred in the case concerned; or

(d) the transmission or transfer is strictly necessary for Europol to notify 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;

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

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

The transmission or transfer referred to in the first subparagraph of this paragraph is subject to any restrictions indicated pursuant to Article 19(2) or (3) and is without prejudice to Article 67.

6. With regard to paragraph 5, points (a), (b) and (d), of this Article, if the private party concerned is not established within the Union or in a third country as referred to in Article 25(1), point (a), (b) or (c), or in Article 25(4a), 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 concerned or of another person;

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

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

(d) necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of a specific crime that falls within Europol's objectives; 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 that falls within Europol's objectives.

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

(f) the following paragraphs are inserted:

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

6b. Europol may request Member States, via their national units, to obtain, in accordance with their national law, personal data from private parties which are established or have a legal representative in their territory, for the purpose of sharing those data with Europol. Such requests shall be reasoned and as precise as possible. Such personal data shall be the least sensitive possible and strictly limited to what is necessary and proportionate for the purpose of enabling Europol to identify the national units concerned.

Notwithstanding the jurisdiction of Member States over a specific crime, Member States shall ensure that their competent authorities can process the requests referred to in the first subparagraph in accordance with their national law for the purpose of supplying Europol with the information necessary for it to identify the national units concerned.

6c. Europol's infrastructure may be used for exchanges between the competent authorities of the Member States and private parties in accordance with the respective national law. Those exchanges may also cover crimes that do not fall within Europol's objectives.

Where Member States use Europol's infrastructure for the exchange of personal data on crimes that fall within Europol's objectives, they may grant Europol access to such data.

Where Member States use Europol's infrastructure for the exchange of personal data on crimes that do not fall within Europol's objectives, Europol shall not have access to those data and shall be considered to be a processor in accordance with Article 87 of Regulation (EU) 2018/1725.

Europol shall assess the security risks posed by allowing the use of its infrastructure by private parties and, where necessary, implement appropriate preventive and mitigating measures.';

(g) paragraphs 9 and 10 are deleted;

(h) the following paragraph is added:

'11. Europol shall prepare an annual report for the Management Board on the personal data exchanged with private parties pursuant to Articles 26, 26a and 26b, on the basis of quantitative and qualitative evaluation criteria established by the Management Board.

The annual report shall include specific examples demonstrating why Europol's requests in accordance with paragraph 6b of this Article were necessary to achieve its objectives and carry out its tasks.

The annual report shall take into account the obligations of discretion and confidentiality and the examples shall be anonymised insofar as personal data are concerned.

The annual report shall be sent to the European Parliament, the Council, the Commission and national parliaments.';

(20) the following Articles are inserted:

'*Article 26a*

Exchange of personal data with private parties in online crisis situations

1. In online crisis situations, Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18.

2. Where Europol receives personal data from a private party established in a third country, Europol shall forward those data and the results of its analysis and verification of those data only to a Member State, or to a third country concerned as referred to in Article 25(1), point (a), (b) or (c), or in Article 25(4a).

Europol may transfer the results of its analysis and verification of the data referred to in paragraph 1 of this Article to the third country concerned pursuant to Article 25(5) or (6).

3. Europol may transmit or transfer personal data to private parties, on a case-by-case basis, subject to any restrictions indicated 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 online crisis situations and the fundamental rights and freedoms of the data subjects concerned do not override the public interest that requires those personal data be transmitted or transferred.

4. Where the private party concerned is not established within the Union or in a third country as referred to in Article 25(1), point (a), (b) or (c), or in Article 25(4a), the transfer shall require authorisation by the Executive Director.

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

6. Europol may request Member States, via their national units, to obtain, in accordance with their national law, personal data from private parties which are established or have a legal representative in their territory, for the purpose of sharing those data with Europol. Such requests shall be reasoned and as precise as possible. Such personal data shall be the least sensitive possible and strictly limited to what is necessary and proportionate for the purpose of enabling Europol to support Member States in addressing online crisis situations.

Notwithstanding the jurisdiction of Member States with regard to the dissemination of the content in relation to which Europol requests the personal data, Member States shall ensure that their competent authorities can process the requests referred to in the first subparagraph in accordance with their national law for the purpose of supplying Europol with the information necessary for it to achieve its objectives.

7. Europol shall ensure that detailed records of all transfers of personal data and the grounds for such transfers are kept in accordance with this Regulation. Upon request of the EDPS, Europol shall make those records available to the EDPS pursuant to Article 39a.

8. 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.

Article 26b

Exchange of personal data with private parties to address the online dissemination of online 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 online child sexual abuse material, as referred to in Article 4(1), point (y).

2. Where Europol receives personal data from a private party established in a third country, Europol shall forward those data and the results of its analysis and verification of those data only to a Member State, or to a third country concerned as referred to in Article 25(1), point (a), (b) or (c), or in Article 25(4a).

Europol may transfer the results of its analysis and verification of the data referred to in the first subparagraph of this paragraph to the third country concerned pursuant to Article 25(5) or (6).

3. Europol may transmit or transfer personal data to private parties, on a case-by-case basis, subject to any restrictions indicated 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 online child sexual abuse material, as referred to in Article 4(1), point (y), and the fundamental rights and freedoms of the data subjects concerned do not override the public interest that requires those personal data be transmitted or transferred.

4. Where the private party concerned is not established within the Union or in a third country as referred to in Article 25(1), point (a), (b) or (c), or in Article 25(4a), the transfer shall require authorisation by the Executive Director.

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

6. Europol may request Member States, via their national units, to obtain, in accordance with their national law, personal data from private parties which are established or have a legal representative in their territory, for the purpose of sharing those data with Europol. Such requests shall be reasoned and as precise as possible. Such personal data shall be the least sensitive possible and strictly limited to what is necessary and proportionate for the purpose of enabling Europol to address the online dissemination of online child sexual abuse material, as referred to Article 4(1), point (y).

Notwithstanding the jurisdiction of Member States with regard to the dissemination of the content in relation to which Europol requests the personal data, Member States shall ensure that the competent authorities of the Member States can process the requests referred to in the first subparagraph in accordance with their national law for the purpose of supplying Europol with the information necessary for it to achieve its objectives.

7. Europol shall ensure that detailed records of all transfers of personal data and the grounds for such transfers are kept in accordance with this Regulation. Upon request of the EDPS, Europol shall make those records available to the EDPS pursuant to Article 39a.

8. 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.';

(21) in Article 27, paragraphs 1 and 2 are replaced by the following:

'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 shall only be processed by Europol provided 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 pursuant to Article 25(1), point (c); or

(c) an authority of a third country or an international organisation as referred to in Article 25(1), point (a) or (b), or in Article 25(4a).

2. Where Europol receives information, including personal data, from a private person residing in a third country other than that referred to in Article 25(1), points (a) or (b), or in Article 25(4a), Europol shall forward that information only to a Member State or to such third country.';

(22) the title of Chapter VI is replaced by the following:

'DATA PROTECTION';

(23) the following Article is inserted:

'*Article 27a*

Processing of personal data by Europol

1. Without prejudice to this Regulation, Article 3 and Chapter IX of Regulation (EU) 2018/1725 shall apply to the processing of personal data by Europol.

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

2. References to "personal data" in this Regulation shall be understood as references to "operational personal data" as defined in Article 3, point (2), of Regulation (EU) 2018/1725, unless otherwise provided for in this Regulation.

3. The Management Board shall adopt rules to determine the time limits for the storage of administrative personal data.';

(24) Article 28 is deleted;

(25) 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 processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health or concerning natural persons' sex life or sexual orientation shall be allowed only where strictly necessary and proportionate for the purposes of research and innovation projects pursuant to Article 33a and for operational purposes, within Europol's objectives, and only for preventing or combating crime that falls within Europol's objectives. 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 if those data supplement other personal data processed by Europol.';

(b) the following paragraph 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.';

(c) paragraph 3 is replaced by the following:

'3. Only Europol shall have direct access to personal data referred to in paragraphs 1 and 2. The Executive Director shall duly authorise a limited number of Europol staff to have such access if it is necessary for the performance of their tasks.

Notwithstanding the first subparagraph, where it is necessary to grant staff of the competent authorities of the Member States or Union agencies established on the basis of Title V of the TFEU direct access to personal data for the performance of their tasks, in the cases provided for in Article 20(1) and (2a) of this Regulation or for research and innovation projects in accordance with Article 33a(2), point (d), of this Regulation, the Executive Director shall duly authorise a limited number of such staff to have such access.';

(d) paragraph 4 is deleted;

(e) 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 or Union bodies, or transferred to third countries or international organisations, unless such transmission or transfer is required under Union law or strictly necessary and proportionate in individual cases concerning crimes that fall within Europol's objectives and in accordance with Chapter V.';

(26) Article 32 is replaced by the following:

'*Article 32*

Security of processing

Mechanisms to ensure that security measures are addressed across information system boundaries shall be established by Europol in accordance with Article 91 of Regulation (EU) 2018/1725 and by the Member States in accordance with Article 29 of Directive (EU) 2016/680.';

(27) Article 33 is deleted;

(28) the following Article 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, provided that the processing of those personal data:

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

(b) as regards special categories of personal data, is strictly necessary and subject to 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.

2. Without prejudice to paragraph 1, for the processing of personal data performed in the context of Europol's research and innovation projects, the following safeguards shall apply:

(a) any research and innovation project requires the 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 objectives of the project and an explanation of how the project assists Europol or competent authorities of the Member States in their 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) an assessment of the compliance with the data protection principles laid down in Article 71 of Regulation (EU) 2018/1725, of the time limits for the storage and conditions for access to the personal data; and

(v) a data protection impact assessment, including the risks to rights and freedoms of data subjects, 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) the EDPS shall be informed prior to the launch of the project;

(c) the Management Board shall be consulted or informed prior to the launch of the project, in accordance with the guidelines referred to in Article 18(7);

(d) any personal data to be processed in the context of the project shall:

(i) be temporarily copied to a separate, isolated and protected data processing environment within Europol for the sole purpose of carrying out that project;

(ii) be accessed only by specifically authorised staff of Europol in accordance with Article 30(3) of this Regulation and, subject to technical security measures, by specifically authorised staff of the competent authorities of the Member States and Union agencies established on the basis of Title V of the TFEU;

(iii) not be transmitted or transferred;

(iv) not lead to measures or decisions affecting the data subjects as a result of their processing;

(v) be erased once the project is concluded or the time limit for the storage of personal data has expired in accordance with Article 31;

(e) the logs of the processing of personal data in the context of the project shall be kept until two years after the conclusion of the project, 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 in a binding document the general scope for the research and innovation projects. Such document shall be updated where appropriate and made available to the EDPS for the purpose of its supervision.

4. Europol shall keep a document containing a detailed description of the process and of the rationale behind the training, testing and validation of algorithms to ensure transparency of the process and the algorithms, including their compliance with the safeguards provided for in this Article, and to allow for verification of the accuracy of the results based on the use of such algorithms. Upon request, Europol shall make that document 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 request consent from that provider of data in accordance with Article 19(2), unless the provider of data has granted its prior authorisation to such processing for the purpose of research and innovation projects, either in general terms or subject to specific conditions.

Europol shall not process data for research and innovation projects without the consent of the provider of the data. Such consent may be withdrawn at any time.';

(29) 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 notify the competent authorities of the Member States concerned of that breach, without undue delay, in accordance with Article 7(5) of this Regulation, 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;

(30) Article 35 is amended as follows:

(a) paragraphs 1 and 2 are deleted;

(b) paragraph 3 is replaced by the following:

'Without prejudice to Article 93 of 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 personal data breach to the data subject concerned in accordance with national law.';

(c) paragraphs 4 and 5 are deleted;

(31) 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 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 that authority, it shall refer the request to Europol without undue delay and within one month of receipt.';

(c) paragraphs 6 and 7 are deleted;

(32) 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 of personal data that relate to him or her referred to in Article 82 of Regulation (EU) 2018/1725 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 that authority, it shall refer the request to Europol without undue delay and within one month of receipt.';

(b) paragraph 2 is deleted;

(c) paragraphs 3, 4 and 5 are replaced by the following:

'3. Without prejudice to Article 82(3) of Regulation (EU) 2018/1725, Europol shall restrict the processing of personal data rather than erase personal data 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, where it is necessary to protect the vital interests of the data subject or of another person, or for the purposes laid down in Article 82(3) of Regulation (EU) 2018/1725.

4. Where personal data 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, have been retrieved by Europol from publicly available sources or result from Europol's own analyses, Europol shall rectify or erase such data or restrict their processing and, where appropriate, inform the providers of the data.

5. Where personal data referred to in paragraphs 1 and 3 held by Europol have been provided to Europol by Member States, the Member States concerned shall rectify or erase such data or restrict their processing in cooperation with Europol, within their respective competences.';

(d) paragraphs 8 and 9 are deleted;

(33) Article 38 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. Europol shall process personal data in a manner that ensures that their source, in accordance with Article 17, can be established.';

(b) in paragraph 2, the introductory wording is replaced by the following:

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

(c) paragraph 4 is replaced by the following:

'4. Europol shall be responsible 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 personal data.';

(d) 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';

(34) Article 39 is replaced by the following:

'*Article 39*

Prior consultation

1. Without prejudice to Article 90 of Regulation (EU) 2018/1725, prior consultation of the EDPS 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.

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

3. Where the processing operations referred to in paragraph 2 of this Article have substantial significance for the performance of Europol's tasks and are particularly urgent and necessary to prevent and combat an immediate threat of a crime that falls within Europol's objectives or to protect vital interests of the data subject or another person, Europol may exceptionally initiate processing after the prior consultation of the EDPS provided for in Article 90(1) of Regulation (EU) 2018/1725 has started and before the period provided for in Article 90(4) of that Regulation has expired. In that case, Europol shall inform the EDPS prior to the start of processing operations.

Written advice of the EDPS pursuant to Article 90(4) of Regulation (EU) 2018/1725 shall be taken into account retrospectively, and the way the processing is carried out shall be adjusted accordingly.

The Data Protection Officer shall be involved in assessing the urgency of such processing operations before the period provided for in Article 90(4) of Regulation (EU) 2018/1725 expires and shall oversee the processing in question.

4. The EDPS shall keep a register of all processing operations that have been notified to him or her pursuant to paragraph 1. The register shall not be made public.';

(35) the following Article is 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 the Data Protection Officer;

(b) the purposes of the processing;

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

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

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

(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 record referred to in paragraph 1 shall be in writing, including in electronic form.

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

(36) Article 40 is replaced by the following:

'*Article 40*

Logging

1. In accordance with Article 88 of Regulation (EU) 2018/1725, Europol shall keep logs of its processing operations. It shall not be possible to modify the logs.

2. Without prejudice to Article 88 of Regulation (EU) 2018/1725, if required by a national unit for a specific investigation related to compliance with data protection rules, the logs referred to in paragraph 1 shall be communicated to that national unit.';

(37) Article 41 is replaced by the following:

'*Article 41*

Designation of the Data Protection Officer

1. The Management Board shall appoint a member of staff of Europol as Data Protection Officer, who shall be designated for that sole position.

2. The Data Protection Officer shall be selected on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to carry out 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 result in a conflict of interest 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 not be dismissed or penalised by the Management Board for performing his or her tasks.

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

(38) the following Articles 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 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.

In order to support the Data Protection Officer in carrying out his or her tasks, a member of staff of Europol may be designated as assistant Data Protection Officer.

3. Europol shall ensure that the Data Protection Officer acts independently and does not receive any instructions regarding the carrying out of his or her tasks.

The Data Protection Officer shall report directly to the Management Board.

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 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 his or her independence.

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

7. The Data Protection Officer shall be appointed for a term of four years and shall be eligible for reappointment.

8. The Data Protection Officer shall be dismissed from his or her post by the Management Board if he or she no longer fulfils the conditions required for the performance of his or her duties and only with the consent of the EDPS.

9. The Data Protection Officer and the assistant Data Protection Officer shall be registered with the EDPS by the Management Board.

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

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, including 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 pursuant to Article 89 of Regulation (EU) 2018/1725 and monitoring the performance of the data protection impact assessment;

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

(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 competent authorities of the Member States, in particular with the 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 EDPS on issues relating to processing, including the prior consultation under Articles 40 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;

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

2. 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.

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 requested the investigation or to the Management Board the results of that investigation.

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

4. 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.

5. If the Data Protection Officer considers that the provisions of this Regulation or of Regulation (EU) 2018/1725 concerning 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 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 period.

If the Executive Director does not resolve the non-compliance of the processing within the specified period, 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 specified period, the Data Protection Officer shall refer the matter to the EDPS.

Article 41c

Fundamental Rights Officer

1. The Management Board shall, upon a proposal of the Executive Director, designate a Fundamental Rights Officer. The Fundamental Rights Officer 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) advise Europol where he or she deems it necessary or where requested on any activity of Europol without impeding or delaying those activities;

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

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

(d) inform the Executive Director about possible violations of fundamental rights in the course of Europol's activities;

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

(f) 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 his or her tasks.

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

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. That training shall be developed in cooperation with the European Union Agency for Fundamental Rights (FRA), established by Council Regulation (EC) No 168/2007 (*), and the European Union Agency for Law Enforcement Training (CEPOL), established by Regulation (EU) 2015/2219 of the European Parliament and of the Council (**).

(*) Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1).
(**) Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA (OJ L 319, 4.12.2015, p. 1.)';

(39) in Article 42, paragraphs 1 and 2 are replaced by the following:

'1. For the purpose of exercising their supervisory function, the national supervisory authorities 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 their Member State to Europol in accordance with the relevant national procedures and to logs as referred to in Article 40 of this Regulation.

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

(40) Article 43 is amended as follows:

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

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

(b) in paragraph 3, the following points are added:

'(j) order the controller or processor to bring processing operations into compliance with 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.';

(c) paragraph 5 is replaced by the following:

'5. The EDPS shall prepare 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 EDPS shall invite the national supervisory authorities to submit observations on that part of the annual report before the annual report is adopted. The EDPS shall take utmost account of those observations and shall refer to them in the annual report.

The part of the annual report referred to in the second subparagraph 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 of the EDPS, and the use of the powers laid down in paragraph 3 of this Article.';

(41) 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) of this Regulation.

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) of this Regulation and be bound by an obligation equivalent to that laid down in Article 43(6) of this Regulation.';

(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 opinion, within a deadline specified by him or her which shall not be shorter than one month and not longer than three months from when the EDPS consults the national supervisory authorities concerned. The EDPS shall take the utmost account of the respective positions of the national supervisory authorities concerned. 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.';

(42) Articles 45 and 46 are deleted;

(43) 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.';

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

'2. Where a complaint relates to a decision referred to in Article 36 or 37 of this Regulation or Article 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 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.';

(44) Article 50 is replaced by the following:

'*Article 50*

Right to compensation

1. 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 (EU) 2018/1725 and Article 56 of Directive (EU) 2016/680.

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 paragraph 1 of this Article shall be referred to the Management Board. The Management Board shall decide on that responsibility by a majority of two-thirds of its members, without prejudice to the right to challenge that decision in accordance with Article 263 TFEU.';

(45) Article 51 is amended as follows:

(a) paragraph 3 is amended as follows:

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

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

(ii) the following points are added:

'(f) annual information pursuant to Article 26(11) on the personal data exchanged with private parties pursuant to Articles 26, 26a and 26b, including an assessment of the effectiveness of cooperation, specific examples of cases demonstrating why those requests were necessary and proportionate for the purpose of enabling Europol to achieve its objectives and carry out its 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;

(g) annual information about the number of cases where it was necessary for Europol to process personal data that do not relate to the categories of data subjects listed in Annex II in order to support Member States in an ongoing 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 that data processing was necessary and proportionate;

(h) annual information about transfers of personal data to third countries and international organisations pursuant to Article 25(1) or Article 25(4a) 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 an ongoing specific criminal investigation to third countries or international organisations, including information on the countries concerned and the duration of the authorisation;

(i) annual information about the number of cases in which Europol proposed the possible entry of information alerts in accordance with Article 4(1), point (t), including specific examples of cases demonstrating why the entry of those alerts was proposed;

(j) annual information about the number of research and innovation projects undertaken, including information on the purposes of those projects, the categories of personal data processed, the additional safeguards used, including data minimisation, the law enforcement needs those projects seek to address and the outcome of those projects;

(k) 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 processing period has been extended;

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

The examples referred to in points (f) and (i) shall be anonymised insofar as personal data are concerned.

The examples referred to in point (g) shall be anonymised insofar as personal data are concerned, without disclosing any operational details and without prejudice to any ongoing investigations.';

(b) 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 those conclusions, for information purposes, to the Council, the Commission and Europol.';

(46) the following Article is inserted:

'*Article 52a*

Consultative Forum

1. The JPSG shall establish a consultative forum to assist it, upon request, by providing it with independent advice in fundamental rights matters.

The JPSG and the Executive Director may consult the consultative forum on any matter related to fundamental rights.

2. The JPSG shall determine the composition of the consultative forum, its working methods and the way in which the information is to be transmitted to the consultative forum.';

(47) in Article 58, paragraph 9 is replaced by the following:

'9. Delegated Regulation (EU) 2019/715 shall apply to any building projects that are likely to have significant implications for Europol's budget.';

(48) 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 (*), Europol's accounting officer shall draw up Europol's final accounts for that year. The Executive Director shall submit those final accounts to the Management Board for an opinion.

(*) 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) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018, p. 1).';

(b) paragraph 9 is replaced by the following:

'9. Upon the request of the European Parliament, the Executive Director shall submit to it any information required for the smooth application of the discharge procedure for year N, in accordance with Article 106(3) of Delegated Regulation (EU) 2019/715.';

(49) Article 61 is replaced by the following:

'*Article 61*

Financial Rules

1. The financial rules applicable to Europol shall be adopted by the Management Board after consultation with the Commission. They shall not depart from Delegated Regulation (EU) 2019/715 unless such a departure is specifically required for the operation of Europol and the Commission has given its prior consent.

2. Europol may award grants related to the achievement of its objectives and tasks.

3. Europol may award grants without a call for proposals to Member States for performance of activities that fall within Europol's objectives and tasks.

4. 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 financial rules referred to in paragraph 1 may specify the criteria under which financial support may cover the full investment costs referred to in the first subparagraph of this paragraph.

5. In respect of the financial support to be given to joint investigation teams' activities, Europol and Eurojust shall jointly establish the rules and conditions upon which applications for such support are to be processed.';

(50) Article 68 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. By 29 June 2027 and every five years thereafter, the Commission shall carry out an evaluation, in particular, of the impact, effectiveness and efficiency of Europol and of its working practices. That 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 is added:

'3. By 29 June 2025, the Commission shall submit a report to the European Parliament and to the Council, evaluating and assessing the operational impact of the implementation of the tasks provided for in this Regulation, in particular in Article 4(1), point (t), Article 18(2), point (e), Article 18(6a), and Articles 18a, 26, 26a and 26b, with regard to Europol's objectives. The report shall assess the impact of those tasks on fundamental rights and freedoms as provided for by the Charter. It shall also provide a cost-benefit analysis of the extension of Europol's tasks.';

(51) the following Articles are inserted:

'*Article 74a*

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

1. Where a Member State, the EPPO or Eurojust provided personal data that do not relate to the categories of data subjects listed in Annex II to Europol before 28 June 2022, Europol may process those personal data in accordance with Article 18a where:

(a) the Member State concerned, the EPPO or Eurojust informs Europol by 29 September 2022, that it is authorised to process those personal data, in accordance with procedural requirements and safeguards applicable under Union or national law, in the ongoing criminal investigation for which it requested Europol's support when it initially provided the data;

(b) the Member State concerned, the EPPO or Eurojust requests that Europol, by 29 September 2022, support the ongoing criminal investigation referred to in point (a); and

(c) Europol assesses, in accordance with Article 18a(1), point (b), that it is not possible to support the ongoing criminal investigation referred to in point (a) of this paragraph without processing personal data that do not comply with Article 18(5).

The assessment referred to in point (c) of this paragraph is recorded and sent to the EDPS for information when Europol ceases to support the related specific criminal investigation.

2. Where a Member State, the EPPO or Eurojust does not comply with one or more of the requirements set out in paragraph 1, points (a) and (b) of this Article, with regard to personal data that do not relate to the categories of data subjects listed in Annex II that it provided to Europol before 28 June 2022, or where a Member State, the EPPO or Eurojust does not comply with paragraph 1, point (c) of this Article, Europol shall not process those personal data in accordance with Article 18a, but shall, without prejudice to Article 18(5) and Article 74b, delete those personal data by 29 October 2022.

3. Where a third country referred to in Article 18a(6) provided personal data that do not relate to the categories of data subjects listed in Annex II to Europol before 28 June 2022, Europol may process those personal data in accordance with Article 18a(6) 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 obtained 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, by 29 September 2022, that it is authorised to process those personal data in the criminal investigation in the context of which it obtained the data;

(d) Europol assesses, in accordance with Article 18a(1), point (b), that it is not possible to support the specific criminal investigation referred to in point (a) of this paragraph without processing personal data that do not comply with Article 18(5) and that assessment is 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(6), that the amount of personal data is not manifestly disproportionate in relation to the specific criminal investigation referred to in point (a) of this paragraph in one or more Member States that Europol supports.

4. Where a third country does not comply with the requirement set out in paragraph 3, point (c) of this Article, with regard to personal data that do not relate to the categories of data subjects listed in Annex II that it provided to Europol before 28 June 2022, or where any of the other requirements set out in paragraph 3 of this Article are not complied with, Europol shall not process those personal data in accordance with Article 18a(6), but shall, without prejudice to Article 18(5) and Article 74b, delete those personal data by 29 October 2022.

5. Where a Member State, the EPPO or Eurojust provided personal data that do not relate to the categories of data subjects listed in Annex II to Europol before 28 June 2022, it may request Europol, by 29 September 2022, to store those data and the outcome of Europol's processing of those data where this is necessary for ensuring the veracity, reliability and traceability of the criminal intelligence process. Europol shall keep personal data that do not relate to the categories of data subjects listed in Annex II functionally separate 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 for which those data were provided are ongoing.

6. Where Europol received personal data that do not relate to the categories of data subjects listed in Annex II before 28 June 2022, Europol shall not store those data for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process unless so requested in accordance with paragraph 5. In the absence of such a request, Europol shall delete those personal data by 29 October 2022.

Article 74b

Transitional arrangements concerning the processing of personal data held by Europol

Without prejudice to Article 74a, for personal data that Europol received before 28 June 2022, Europol may verify whether those personal data relate to one of the categories of data subjects set out in Annex II. To that end, Europol may carry out a pre-analysis of those personal data for a period of up to 18 months from the date the data were first received or, in justified cases and with the prior authorisation of the EDPS, for a longer period.

The maximum period of processing the data referred to in the first subparagraph shall be three years from the day of receipt of the data by Europol.'.

Article 2

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

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

Done at Strasbourg, 8 June 2022.

For the European Parliament	*For the Council*
The President	*The President*
R. METSOLA	C. BEAUNE