EUROPEAN
COMMISSION

Brussels, 9.12.2020
COM(2020) 796 final

2020/0349 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

{SEC(2020) 545 final} - {SWD(2020) 543 final} - {SWD(2020) 544 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

Europe faces a security landscape in flux, with evolving and increasingly complex security threats. Criminals exploit the advantages that the digital transformation, new technologies[1], globalisation and mobility bring about, including the inter-connectivity and blurring of the boundaries between the physical and digital world.[2] Recent events[3] have once again shown that terrorism remains a significant threat to the freedom and way of life of the European Union and its citizens. The COVID-19 crisis adds to this, as criminals have quickly seized opportunities to exploit the crisis by adapting their modes of operation or developing new criminal activities.[4] Although the full impact of the COVID-19 crisis on security is not yet apparent, it is expected to shape the landscape of serious and organised crime in the EU in mid- and long-term.[5]

These evolving security threats call for effective EU level support to the work of national law enforcement authorities. These threats spread across borders, cut across a variety of crimes that they facilitate, and manifest themselves in poly-criminal organised crime groups[6] that engage in a wide range of criminal activities. As action at national level alone does not suffice to address these transnational security challenges, Member States' law enforcement authorities have increasingly made use of the support and expertise that Europol, the EU agency for law enforcement cooperation, offers to counter serious crime and terrorism. Europol is the centrepiece for EU-level support to Member States in countering serious crime and terrorism. The agency offers support and expertise to national law enforcement authorities 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. Since the entry into application of the 2016 Europol Regulation[7], the operational importance of the agency's tasks has changed substantially. For example, the operational support provided by Europol's European Counter-Terrorism Centre has increased fivefold over recent years (from 127 operational cases supported in 2016 to 632 cases in 2019). The Centre is now part of almost every major counter-terrorism investigation in the EU.

---

1 This includes developments such as 5G mobile networks, artificial intelligence, the internet of things, drones, anonymisation and encryption, 3D printing and biotechnology. For example, in July 2020, French and Dutch law enforcement and judicial authorities, alongside Europol and Eurojust, presented the joint investigation to dismantle EncroChat, an encrypted phone network used by criminal networks involved in violent attacks, corruption, attempted murders and large-scale drug transports (https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe).

2 The integration of digital systems in many criminal activities and the expansion of the online trade in illicit goods and services is transforming serious and organised crime. See Europol, Serious and Organised Threat Assessments 2017.

3 The attack in Paris on 25.09.2020, the attack in Conflans-Sainte-Honorine on 16.10.2020, the attack in Nice on 29.10.2020 and the attack in Vienna on 02.11.2020.

4 www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis. This is notably the case on cybercrime, fraud, counterfeiting and organised property crime.

5 https://www.europol.europa.eu/publications-documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu.

6 More than 5,000 organised crime groups were under investigation in Europe in 2017 – a 50% rise compared to 2013. 45% of the organised crime groups were involved in more than one criminal activity. The share of these polycriminal groups increased sharply. Organised crime groups often engage in more than one criminal activity. They are highly flexible and able to shift from one criminal activity to another. Europol, Serious and Organised Threat Assessments 2017.

7 Regulation (EU) 2016/794 (11.5.2016).

The threat from terrorism in Europe remains high.[8] In a joint statement by the EU Home Affairs Ministers of 13 November 2020 on the recent terrorist attacks in Europe, Ministers "*invite the Commission to submit a proposal revising the Europol mandate with a strong legal basis for the handling of large datasets. Europol and especially its European Counter Terrorism Centre are of fundamental importance for effectively supporting the Member States in their prevention and prosecution of terrorist crimes, and need to be bolstered.*"[9]

The threat environment also changes type of the support Member States need and expect from Europol to keep citizens safe, in a way that was not foreseeable when the co-legislators negotiated the current Europol mandate. The December 2019 Council Conclusions acknowledge "*the urgent operational need for Europol to request and receive data directly from private parties*", calling on the Commission to consider adapting the schedule for the review of the Europol Regulation "*in view of the need for European law enforcement to address ongoing technological developments*".[10] There is a pressing social need to counter serious crimes prepared or committed with the use of cross-border services offered by private parties[11], notably cybercrimes. Whereas this challenge is partially addressed by the e-evidence package[12], there are situations where Europol's support is necessary to counter the threats posed by cybercrime and cyber-enabled crimes effectively, notably when private parties seek to report such crimes.

A July 2020 European Parliament Resolution also calls for reinforcing Europol, stating that "*strengthening Europol's capacity to request the initiation of cross-border investigations, particularly in cases of serious attacks against whistleblowers and investigative journalists who play an essential role in exposing corruption, fraud, mismanagement and other wrongdoing in the public and private sectors, should be a priority."*[13]

Given the changing security landscape, Europol needs to have the capabilities and tools to support Member States effectively in countering serious crime and terrorism. In response to pressing operational needs, and calls by the co-legislators for stronger support from Europol, the Commission Work Programme for 2020 announced a legislative initiative to "*strengthen the Europol mandate in order to reinforce operational police cooperation*". This is also a key action of the July 2020 EU Security Union Strategy.[14] In line with the call by the Political Guidelines[15] to "*leave no stone unturned when it comes to protecting our citizens*", this legislative initiative addresses those areas where stakeholders ask for reinforced support from Europol to help Member States keeping citizens safe.

---

8 A total of 119 completed, failed and foiled terrorist attacks were reported by 13 EU Member States, with 10 deaths and 27 injuries (Europol, European Union Terrorism Situation and Trend Report, 2020).

9 https://www.consilium.europa.eu/fr/press/press-releases/2020/11/13/joint-statement-by-the-eu-home-affairs-ministers-on-the-recent-terrorist-attacks-in-europe/.

10 https://www.consilium.europa.eu/media/41586/st14755-en19.pdf. Regulation (EU) 2016/794 foresees an evaluation assessing the impact, effectiveness and efficiency of Europol by May 2022.

11 The term 'private parties' refers to organisations with a legal personality other than public authorities. This includes, but is not limited to, undertakings established under civil law, even if they are owned or controlled by a public authority.

12 The Commission adopted on 17 April 2018 the so-called "e-evidence package" consisting of a Regulation (COM(2018) 225 final) and a Directive (COM(2018) 226 final). The package is under negotiation by the co-legislators.

13 European Parliament resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing (2020/2686(RSP)).

14 COM(2020) 605 final (24.7.2020).

15 https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

To that end, this proposal seeks to strengthen the mandate of Europol within the mission and tasks of the agency as laid down in the Treaty[16], notably by:

- enabling Europol to cooperate effectively with private parties, addressing lack of effective cooperation between private parties and law enforcement authorities to counter the use of cross-border services, such as communication, banking, or transport services, by criminals;
- enabling Europol to effectively support Member States and their investigations with the analysis of large and complex datasets, addressing the big data challenge for law enforcement authorities;
- strengthening Europol's role on research and innovation, addressing gaps relevant for law enforcement;
- strengthening Europol's cooperation with third countries in specific situations and on a case-by-case basis for preventing and countering crimes falling within the scope of Europol's objectives;
- clarifying that Europol may request, in specific cases where Europol considers that a criminal investigation should be initiated, the competent authorities of a Member State to initiate, conduct or coordinate an investigation of a crime which affects a common interest covered by a Union policy, without the requirement of a cross-border dimension of the crime concerned;[17]
- strengthening Europol's cooperation with the European Public Prosecutor's Office (EPPO);
- further strengthening the data protection framework applicable to Europol;
- further strengthening parliamentary oversight and accountability of Europol.

This legislative initiative is linked to a legislative proposal amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters to enable Europol to enter data into the SIS. Subject to consultation of the Member States, this would enable Europol to enter data into the SIS on the suspected involvement of a third country national in an offence in respect of which Europol is competent.

This legislative initiative is part of a package of measures presented by the Commission on 9 December 2020 to reinforce the Union's response to the threat posed by terrorism.

- **Consistency with existing policy provisions in the policy area**

This legislative initiative takes account of a wide range of EU policies in the area of internal security that have been adopted or launched since the entry into force of the 2016 Europol Regulation.

[16] See Article 88 of the Treaty on the Functioning of the European Union.

[17] According to Article 3(1) of Regulation (EU) 2016/794, one of Europol's objectives is to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combatting forms of crime which affect a common interest covered by a Union policy. This corresponds to Europol's mission as set out in Article 88 TFEU. Article 6(1) of Regulation (EU) 2016/794 sets out that "*in specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation.*"

As regards cooperation with private parties, this legislative initiative takes account of the related initiatives for the removal of terrorist content online[18] and to improve cross-border access to electronic evidence.[19] Once adopted, and based on the Commission's proposals, the e-evidence package would provide national law enforcement and judicial authorities with European Production Orders and European Preservation Orders to obtain digital evidence from service providers for criminal investigations, irrespective of the Member State in which the provider is established or the information is stored.

As regards limits in the sharing of third-country sourced information on suspects and criminals, the assessment of options to strengthen this information sharing takes account of the on-going work towards the interoperability[20] of EU information systems for security, border and migration management and the EU legal framework on large scale IT systems. This includes existing or planned EU information systems, namely the Schengen Information System,[21] the EU Entry/Exit System,[22] the European Travel Information and Authorisation System,[23] and the proposed upgrading of the Visa Information System[24] and of the Eurodac system.[25]

This legislative initiative also takes account of Europol's cooperation with other Union bodies or agencies, notably the European Public Prosecutor's Office[26], Eurojust[27] as the EU agency for criminal justice cooperation, ENISA as the European Agency for Cyber Security[28], the European Anti-Fraud Office (OLAF)[29], and the European Border and Coast Guard Agency (Frontex).[30]

- **Consistency with other Union policies**

This legislative initiative also takes account of other relevant Union EU policies that have been adopted or launched since the entry into force of the Europol Regulation.

This legislative initiative takes full account of the relevant EU data protection legislation (see section 3 below on fundamental rights).

As regards innovation, this legislative initiative takes account of EU security-related funding under Horizon 2020,[31] the Internal Security Fund,[32] the proposed Horizon Europe[33] and the proposed Digital Europe programme.[34] It also takes account of the European strategy for data[35] and the White Paper on Artificial Intelligence[36] as the first pillars of the new digital

18 COM(2018) 640 final (12.9.2018).
19 COM(2018) 225 final and COM(2018) 226 final (17.4.2018) ("e-evidence package").
20 Regulation (EU) No 2019/818 (20.5.2020).
21 Regulation (EU) No 2018/1862 (28.11.2018).
22 Regulation (EU) No 2017/2226 (30.11.2017).
23 Regulation (EU) No 2018/1240 (12.9.2018).
24 COM(2018) 302 final (16.5.2018).
25 COM(2020) 614 final (23.9.2020).
26 Council Regulation (EU) No 2017/1939 (12.10.2017).
27 Regulation (EU) No 2018/1727 (14.11.2018).
28 Regulation (EU) No 2019/881 (17.4.2019).
29 Regulation (EU, Euratom) No 883/2013 (11.9.2013).
30 Regulation (EU) 2019/1896 (13.11.2019).
31 Regulation (EU) No 1291/2013 (11.12.2013).
32 Regulation (EU) No 513/2014 (16.4.2014). See also the Commission proposal for the Internal Security Fund for the next multiannual financial framework (COM(2018) 472 final (13.6.2018)).
33 COM(2018) 435 final (7.6.2018).
34 COM(2018) 434 final (6.6.2018).
35 COM(2020) 66 final (19.2.2020).
36 COM(2020) 65 final (19.2.2020).

strategy of the Commission, as well as the on-going work in preparation of governance of common European data spaces.

As regards Europol's cooperation with third countries, this legislative initiative takes account of the Union's external policies, notably the work of EU delegations and counter-terrorism/security experts in third countries and common security and defence policy missions and operations.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The legal basis of the legislative initiative is Article 88 of the Treaty on the Functioning of the European Union (TFEU). Article 88(1) TFEU stipulates that Europol's mission shall be to support and strengthen action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy. It provides for Europol to be governed by a Regulation to be adopted in accordance with the ordinary legislative procedure.

• Subsidiarity

According to the principle of subsidiarity laid down in Article 5(3) TEU, action at EU level should be taken only when the aims envisaged cannot be achieved sufficiently by Member States alone and can therefore, by reason of the scale or effects of the proposed action, be better achieved by the EU.

Member States are responsible for the maintenance of law and order and the safeguarding of internal security.[37] Indeed, the Union shall respect Member States' essential state functions, including maintaining law and order and safeguarding national security.[38] As serious crime and terrorism are often of a transnational nature, action at national level alone cannot counter them effectively. This is why Member States choose to work together within the framework of the EU to tackle the threats posed by serious crime and terrorism. They seek to coordinate their law enforcement action and cooperate in addressing shared security challenges. They decide to pool resources at EU level and share expertise. As the EU agency for law enforcement cooperation, Europol is a strong expression of this endeavour by the Member States to keep their citizens safe by working together. Europol provides a framework for Member States to coordinate their law enforcement action. Member States use their liaison officers at Europol and the information exchange channel the agency provides to exchange information and cooperate in their criminal investigations. Member States pool resources by tasking Europol to process their information in its databases and provide joint analysis. They use the growing expertise that Europol brings together on a variety of aspects of policing. This has made Europol the most visible and effective component of EU-level support for Member States' law enforcement authorities.

Evolving security threats, driven by the way criminals exploit the advantages that the digital transformation and new technologies bring about, also call for effective EU level support to the work of national law enforcement authorities. There are of course differences in the way individual Member States, their regions and local communities confront specific types of crime. This is why their law enforcement authorities can choose where to seek EU-level support from Europol and what joint initiatives to participate in. In any case, law enforcement

[37] Article 72 TFEU.
[38] Article 4(2) TEU.

authorities across all Member States, regions and local levels face the same evolving security threats. Consequently, there is a need for EU action to step up the support to Member States in fighting serious crime and terrorism to keep pace with these threats.

Indeed, Member States alone would not be able to effectively tackle all the challenges addressed by this proposal:

- As regards the **lack of effective cooperation between private parties and law enforcement authorities** to counter the abuse of cross-border services by criminals, national authorities cannot alone analyse multi-jurisdictional or non-attributable data sets effectively, as it is very resource intensive to sift through large data sets in order to identify the data relevant for the respective jurisdiction or jurisdictions, in particular when the Member States concerned have not yet been identified. Alternatively, if the national law enforcement authorities obtain smaller data sets targeted to their respective jurisdiction, they fall short of the entire intelligence picture. Furthermore, Member States cannot effectively address these problems through an intergovernmental cooperation, by which the Member State of establishment were to receive the data, analyse and then distribute it to the Member States concerned. This would not only entail disproportionate resource implications for the Member States of establishment, but also legal difficulties in situations, where the criminal activity has no or limited link to the jurisdiction of that Member State.
- As regards the **big data challenge for law enforcement**, Member States cannot detect such cross-border links through their own analysis of the large datasets at national level, as they lack the corresponding data on other crimes and criminals in other Member States. Moreover, some Member States might not always have the necessary IT tools, expertise and resources to analyse large and complex datasets.
- As regards **gaps on research and innovation relevant for law enforcement**, not all Member States are able to exploit fully the opportunities of new technologies for fighting crime and terrorism, and to overcome the challenges posed by the use of these technologies by criminals and terrorists, given the investment, resources and skills this requires.
- As regards **limitations in law enforcement cooperation with third countries**, Europol can play a key role in expanding its cooperation with third countries to counter crime and terrorism while ensuring coherence with other EU external polices and tools.
- As regards **crimes which affect a common interest covered by a Union policy**, Member State might require support to effectively investigate such crimes.

- **Proportionality**

  According to the principle of proportionality laid down in Article 5(4) TEU, there is a need to match the nature and intensity of a given measure to the identified problem. All problems addressed in this legislative initiative call, in one way or another, for **EU-level support** for Member States to tackle these problems effectively:

- As regards the **lack of effective cooperation between private parties and law enforcement authorities** to overcome the challenges posed by the use of cross-border services by criminals, such as communication, banking, or transport services, these problems can be tackled more effectively and efficiently at EU level than at national level, by analysing multi-jurisdictional or non-attributable data sets at EU level in order to identify the data relevant for the respective Member States

concerned, and by creating an EU level channel for requests containing personal data to private parties.

- As regards the **big data challenge for law enforcement**, these problems can be tackled more effectively and efficiently at EU level than at national level, by assisting Member States in processing large and complex datasets to support their criminal investigations with cross-border leads. This would include techniques of digital forensics to identify the necessary information and detect links with crimes and criminals in other Member States.
- As regards **gaps on research and innovation relevant for law enforcement**, and given the significant technical and financial investments required, these problems can be tackled more effectively and efficiently at EU level than at national level, by creating synergies and achieving economies of scale. For that to bring most added value in terms of EU funding for security research, there is a need to close the gap on the coordination of research and innovation needs on the side of law enforcement. Moreover, innovation and the development of new technologies often rely on the availability of large amounts of data, which can be realised better at EU level. By promoting the development of EU tools to counter serious crime and terrorism, an EU approach to innovation takes account of the cross-border dimension of many of today's security threats, as well as the need for cross-border cooperation among law enforcement authorities to tackle these threats.
- As regards **uncertainties around the use of mechanisms by Europol to exchange personal data with third countries**, the limitations in Regulation (EU) 2016/794, which might prevent effective cooperation with third countries, can be addressed effectively at EU level.
- As regards **crimes which affect a common interest covered by a Union policy**, support from the EU level might be required to effectively investigate such crimes.

As the EU agency for law enforcement cooperation, Europol would be well positioned to provide this EU-level support. Indeed, Europol has proven very effective in supporting national law enforcement authorities in countering serious crime and terrorism. The stakeholder consultation carried out in the preparation of the impact assessment showed a very high level of satisfaction with Europol. There are clear synergies and economies of scale for Member States resulting, for example, from the joint processing of information by Europol, or from the expertise that the specialised Centres[39] pool and offer to Member States. Member States expect, and operationally need, the same level of support from Europol when it comes to evolving security threats.

Law enforcement cooperation at EU-level through Europol does not replace different national policies on internal security and does not substitute the work of national law enforcement authorities. Differences in the legal systems and traditions of the Member States, as acknowledged by the Treaties,[40] remain unaffected by this EU level support.

- **Choice of the instrument**

Given that Europol's mandate is set out in Regulation (EU) 2016/794, the strengthening of Europol's mandate has to take the form of a Regulation.

[39] European Cybercrime Centre, European Migrant Smuggling Centre, European Counter Terrorism Centre and European Financial and Economic Crime Centre.

[40] Article 67(1) TFEU.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Stakeholder consultations**

To ensure that the general public interest is properly considered in the Commission's approach to strengthening Europol's mandate, the Commission services identified relevant stakeholders and consulted them throughout the preparation of this legislative initiative. The Commission services sought views from a wide range of subject matter experts, national authorities, civil society organisations, and from members of the public on their expectations and concerns relating to enhancing Europol's capabilities in supporting Member States to effectively prevent and investigate crime.

During the consultation process, the Commission services applied a variety of methods and forms of consultation. They included:

- the consultation on the Inception Impact Assessment, which sought views from all interested parties;
- targeted stakeholder consultation by way of a questionnaire;
- expert interviews; and
- targeted thematic stakeholder workshops that focused on subject matter experts, including practitioners at national level. Taking into account the technicalities and specificities of the subject, the Commission services focused on targeted consultations, addressing a broad range of stakeholders at national and EU level.

The diversity of perspectives proved valuable in supporting the Commission to ensure that its legislative initiative addresses the needs, and took account of the concerns, of a wide range of stakeholders. Moreover, it allowed the Commission to gather necessary and indispensable data, facts and views on the relevance, effectiveness, efficiency, coherence and EU added value of this legislative initiative.

Taking into consideration the Covid-19 pandemic and the related restrictions and inability to interact with relevant stakeholders in physical settings, the consultation activities focused on applicable alternatives such as online surveys, semi-structured phone interviews, as well as meetings via video conference.

Stakeholders are generally supportive of strengthening Europol's legal mandate to support Member States in preventing and combatting serious crime and terrorism. Member States have supported the preferred policy options explicitly in various Council fora as well as in a October 2020 Declaration of the Home Affairs Ministers of the EU ('*Ten points on the Future of Europol*'). At the same time, Member States are conscious of the importance of their national sovereignty in the area of law enforcement from an operational and procedural perspective. The European Parliament has supported a strong role for Europol, while recalling in a July 2020 European Parliament Resolution that "*a strengthened mandate should go hand-in-hand with adequate parliamentary scrutiny*". The European Parliament is expected to require detailed justification for the necessity of any new data processing capability at Europol, as well as strong data protection safeguards. Indeed, discussions with all stakeholders showed the importance of providing for appropriate safeguards to ensure fundamental rights, and in particular the right to protection of personal data.

The results of the consultation activities were incorporated throughout the impact assessment and the preparation of the legislative initiative.

- **Collection and use of expertise**

The Commission contracted an external consultant to conduct a study into the practice of direct exchanges of personal data between Europol and private parties. The work on the study took place between September 2019 and August 2020, and involved desk research, and stakeholder consultations by way of scoping interviews, targeted questionnaires, a survey, semi-structured interviews, and a workshop. The findings of the study are available online.[41]

- **Impact assessment**

In line with its "Better Regulation" policy, the Commission conducted an impact assessment.[42]

A number of legislative and non-legislative policy options have been considered. Following a pre-selection where some options had to be discarded, the following **policy options have been assessed in full detail**:

(1) Policy options addressing objective I: effective cooperation between private parties and law enforcement

- policy option 1: allowing Europol to process data received directly from private parties
- policy option 2: allowing Europol to exchange personal data with private parties to establish jurisdiction
- policy option 3: allowing Europol to directly query databases managed by private parties

(2) Policy options addressing objective II: analysing large and complex datasets to detect cross-border links

- policy option 4: enabling Europol to analyse large and complex datasets
- policy option 5: introducing a new category of data subjects (persons not related to a crime) whose data Europol can process

(3) Policy options addressing objective III: use of new technologies for law enforcement

- policy option 6: regulating Europol's support to the EU security research programme, the innovation lab at Europol, and Europol's support to the EU innovation hub
- policy option 7: enabling Europol to process personal data for the purpose of innovation in areas relevant for its support to law enforcement

Furthermore, the following policy options, which respond to calls by the co-legislators for a reinforced role of Europol and raise less of a policy choice notably due to legal constraints, were analysed in separate annexes to the impact assessment, given their relevance and for reasons of completeness:

[41] https://ec.europa.eu/home-affairs/news/commission-publishes-study-practice-direct-exchanges-personal-data-between-europol-and-private_en.

[42] [add links to the summary sheet and to the opinion of the Regulatory Scrutiny Board].

- policy option 8: enabling Europol to issue 'discreet check' alerts in the Schengen Information System
- policy option 9: introducing a new alert category in the Schengen Information System to be used exclusively by Europol
- policy option 10: targeted revision of the provisions on self-assessment of the adequate level of safeguards
- policy option 11: targeted revision aligning the provision on the transfer of personal data in specific situations with the provision of the Data Protection Law Enforcement Police Directive
- policy option 12: seeking best practices and guidance on the application of provisions of the Europol Regulation
- policy option 13: strengthening the mechanism for requesting the initiation of investigations
- policy option 14: enabling Europol to request the initiation of criminal investigations in cases affecting only one Member State that concern forms of crime which affect a common interest covered by a Union policy, without the requirement of a cross-border dimension of the crime concerned

Following a detailed assessment of the impact of all policy options, the **package of preferred policy options** consists of policy option 2, policy option 4, policy option 7, policy option 9, policy option 11, policy option 12 and policy option 14. These preferred policy options are reflected in this legislative initiative.

The package of preferred policy options (policy option 2, policy option 4 and policy option 7, policy option 9, policy option 11, policy option 12 and policy option 14) respond effectively to the identified problems and would provide Europol with strong tools and capabilities to step up its support to Member States in countering emerging threats, in full compliance with fundamental rights.

Socially and economically, the ultimate beneficiaries of all preferred options are the citizens, who will directly and indirectly benefit from lower crime rates, reduced economic damages, and less security related costs. In terms of efficiency, the main beneficiaries are national law enforcement authorities. The preferred options should create significant economies of scale at the EU level, as they will shift tasks, which can be performed more efficiently at the EU level, from the national level to Europol. The preferred policy options provide for efficient solutions to challenges which would otherwise have to be addressed at higher costs by means of 27 individual national solutions, or to challenges which could not be addressed at the national level at all in view of their transnational nature.

- **Fundamental rights**

Given the importance of the processing of personal data for the work of law enforcement in general, and for the support activities provided by Europol in particular, this legislative initiative puts a particular focus on the need to ensure full compliance with **fundamental rights** as enshrined in the Charter of Fundamental Rights, and notably the rights to the **protection of personal data**[43] and to respect for private life.[44]

[43] Article 8 of the Charter of Fundamental Rights of the European Union (hereinafter, 'the Charter').
[44] Article 7 of the Charter.

As almost all problems, objectives and policy options addressed in the accompanying impact assessment involve the processing of personal data, any resulting limitation on the exercise of the fundamental right to the protection of personal data must be limited to what is strictly necessary and proportionate. Other fundamental rights may also be affected, such as the fundamental right to non-discrimination in the context of research and innovation. The **thorough consideration of fundamental rights** in the accompanying impact assessment, and notably of the rights to the protection of personal data and to respect for private life, is based on a detailed assessment of policy options in terms of their limitations on the exercise of fundamental rights set out in annex 5 of the accompanying impact assessment.

The assessment of fundamental rights in annex 5 of the accompanying impact assessment applies the Commission's Operational guidance on taking account of fundamental rights in Commission impact assessments,[45] the handbook by the Fundamental Rights Agency on Applying the Charter of Fundamental Rights,[46] and the guidance[47] provided by the European Data Protection Supervisor on assessing necessity and proportionality. Based on this guidance, **annex 5 of the accompanying impact assessment on fundamental rights**:

- describes the policy options discarded at an early stage due to their serious adverse impact on fundamental rights;
- sets out a step-by-step assessment of necessity and proportionality;
- outlines the rejected policy options if a less intrusive but equally effective option is available; and
- provides for a complete list of detailed safeguards for those policy options where a limitation on the exercise of fundamental rights is necessary, also due to the absence of a less intrusive but equally effective option.

Moreover, chapter 8 of the accompanying impact assessment provides an assessment of the **accumulated impact** of the preferred policy options on fundamental rights.

4. BUDGETARY IMPLICATIONS

This legislative initiative would have an impact on the budget and staff needs of Europol. It is estimated that an additional budget of around EUR 180 million and around 160 additional posts would be needed for the overall MFF period to ensure that Europol has the necessary resources to enforce its revised mandate. The new tasks for Europol proposed in this legislative initiative would therefore require additional financial and human reinforcements compared to the resources earmarked in the Commission proposal of May 2020 for the Multiannual Financial Framework 2021-2027, which plan for a 2% yearly increase of the EU contribution to Europol. These estimates as well as the overall budget and number of posts are subject to the outcome of the negotiations on the Multiannual Financial Framework 2021-2027. This contribution should also stabilise the resource needs of Europol over the period of the legislative financial statement. This legislative initiative also open the possibility for Member States to contribute directly to Europol's budget, where necessary and required by existing or new tasks.

---

45 SEC(2011) 567 final (6.5.2011).

46 European Union Agency for Fundamental Rights: Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level (2018).

47 European Data Protection Supervisor: Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit (11.4.2017); European Data Protection Supervisor: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019).

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The monitoring and evaluation of Europol's reinforced mandate would largely be performed by the applicable mechanisms under the existing Europol Regulation. Article 68 foresees an evaluation which assesses, in particular, the impact, effectiveness and efficiency of Europol and of its working practices and may address the possible need to modify the structure, operation, field of action and tasks of Europol, and the financial implications of any such modification. Further to this evaluation, the Commission will draw data through its representation in Europol's Management Board meetings and its supervision, along with the Member States, of Europol's work (Article 11).

- **Detailed explanation of the specific provisions of the proposal**

This legislative initiative proposes the following **new tasks** for Europol:

- Enabling Europol to cooperate effective with **private parties**: the legislative initiative sets out rules for Europol to exchange personal data with private parties and analyse this data with a view to identifying all Member States concerned and providing them with the information necessary to establish their jurisdiction, also with regard to terrorist content online. To this end, Europol should be able to receive personal data from private parties, inform such private parties of missing information, and ask Member States to request other private parties to share further additional information. These rules also introduce the possibility for Europol to act as a technical channel for exchanges between Member States and private parties. These new legal grounds respond to the problems private parties and law enforcement authorities face when cooperating on crimes where the offender, the victims and the relevant IT infrastructure are under multiple jurisdictions in the EU and beyond, and would also enable Europol to support law enforcement authorities in their interactions with private parties on the removal of terrorist content online and other relevant issues. [Article 26]
- Enabling Europol to exchange personal data with private parties related to **crisis response**: The legislative initiative sets out rules for Europol to support Member States in preventing the large scale dissemination, via online platforms, of terrorist content related to on-going or recent real-world events depicting harm to life or physical integrity, or calling for imminent harm to life or physical integrity. To this end Europol will be enabled to exchange personal data with private parties, including hashes, IP addresses or URLs related to such content. [Article 26a]
- Enabling Europol to **process large and complex datasets**: The legislative initiative sets out rules for Europol to verify if personal data received in the context of preventing and countering crimes falling within the scope of Europol's objectives complies with the categories of data subjects whose data may be processed by the Agency.[48] To that end, the legislative initiative would introduce the possibility to carry out a pre-analysis of personal data received with the sole purpose of determining whether such data falls into the categories of data subjects. The

[48] Article 18(5) of Regulation (EU) 2016/794 limits the processing of personal data by Europol to the categories of data subjects listed in annex II of that Regulation. The categories of data subjects cover: (1) suspects, (2) convicted persons, (3) persons regarding whom there are factual indications or reasonable grounds to believe that they will commit, (4) persons who might be called on to testify in investigations or in subsequent criminal proceedings, (5) victims, (6) contacts and associates of a criminal, and (7) persons who can provide information on a crime.

Commission proposes these new legal grounds following its analysis of the Decision of the European Data Protection Supervisor on "Europol's big data challenge".[49] [Article 18(5a)]

- Enabling Europol to **effectively support criminal investigations in Member States or by the EPPO** by way of analysis of large and complex datasets: The legislative initiative sets out new rules to enable Europol, in justified cases where it is necessary to support effectively a specific criminal investigation in a Member State or by the EPPO, to process data the national authorities or the EPPO acquired in the context of that criminal investigation in accordance with procedural requirements and safeguards applicable under national criminal law. To that end, and where a Member State or the EPPO requests Europol's analytical support for a specific criminal investigation, the legislative initiative would introduce the possibility for Europol to process all data contained in an investigative case file provided by the Member State or the EPPO for this investigation for as long as Europol supports that specific criminal investigation. This may include information provided by a trusted third country[50] in the context of a specific criminal investigation, provided that this information is necessary for Europol's support of the specific criminal investigation in a Member State. Moreover, the legislative initiative provides for the possibility for a Member State or the EPPO to request Europol to store the investigative case file and the outcome of its operational analysis for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to that criminal investigation are on-going in a Member State. The Commission proposes these new legal grounds following its analysis of the Decision of the European Data Protection Supervisor on "Europol's big data challenge".[51] [Article 18a]
- Strengthening Europol's role on **research and innovation**: (a) Assisting the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation that are relevant to Europol's objectives. [Article 4(4a)] (b) Supporting Member States in the use of emerging technologies in preventing and countering crimes falling within the scope of Europol's objectives, and implementing innovation activities including with the processing of personal data where necessary. [Article 33a] (c) Supporting the screening of specific cases of foreign direct investments into the Union that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes falling within the scope of Europol's objectives. [Article 4(4b)]
- Enabling Europol to enter data into the **Schengen Information System**, subject to consultation of the Member States, on the suspected involvement of a third country national in an offence in respect of which Europol is competent. [Article 4(1)(r)]

---

[49] See the EDPS Decision on the own initiative inquiry on Europol's big data challenge: https://edps.europa.eu/sites/edp/files/publication/20-09-18_edps_decision_on_the_own_initiative_inquiry_on_europols_big_data_challenge_en.pdf.

[50] A third country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of Regulation (EU) 2016/794 or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of Regulation (EU) 2016/794, or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of Regulation (EU) 2016/794.

[51] See the EDPS Decision on the own initiative inquiry on Europol's big data challenge: https://edps.europa.eu/sites/edp/files/publication/20-09-18_edps_decision_on_the_own_initiative_inquiry_on_europols_big_data_challenge_en.pdf.

- Strengthening Europol's **cooperation with third countries** in preventing and countering crimes falling within the scope of Europol's objectives: The legislative initiative provides for the possibility for the Executive Director of Europol to authorise categories of transfers of personal data to third countries in specific situations and on a case-by-case basis, where such categories of transfers are required. [Article 25(5)]
- Strengthening Europol's cooperation with the **European Public Prosecutor's Office** (EPPO), in line with the rules on the transmission of personal data to Union bodies that are applicable to Europol. [Article 20a]
- Strengthening Europol's cooperation with the **European Anti-Fraud Office (OLAF)** to detect fraud, corruption and any other illegal activity affecting the financial interests of the Union, in line with the rules on the transmission of personal data to Union bodies that are applicable to Europol. [Article 21(8)]
- Enabling **joint operational analysis** between Europol and Member States in specific investigations. [Article 20(2a)]
- Further strengthening **parliamentary oversight and accountability** of Europol by introducing new reporting obligations for Europol to the Joint Parliamentary Scrutiny Group. [Article 51]

To further **strengthen the data protection framework** applicable to Europol, this legislative initiative:

- proposes that Article 3 on definitions and Chapter IX of Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of operational personal data by the Union institutions, bodies, offices and agencies become applicable to Europol, while as regards administrative personal data other chapters of Regulation 2018/1725 apply to Europol. [Article 27a].
- aligns the wording on the processing of special categories of personal data (sensitive data) by adding biometric data to the special categories of data. [Article 30]
- introduces a new provision on the processing of personal data for research and innovation to take due account of the stronger role Europol will play in these areas and the impact thereof on the processing of personal data and provide for additional safeguards. [Article 33a]
- introduces a new provision on keeping records of categories of data processing activities to reflect current practice. [Article 39a]
- outlines in more detail the designation, position and tasks of the Data Protection Officer of Europol to highlight the importance of this function, in line with the approach taken during the modernisation of the EU data protection acquis, which introduced the function of the Data Protection Officer as a key component of the EU data protection architecture. [Articles 41a to c]

This legislative initiative also provides for the following **legal clarifications** and **codification of existing tasks** of Europol:

- Supporting Member States' **special intervention units** through the ATLAS network as a cooperation platform of 38 special intervention units of Member States and associated countries. [Article 4(1)(h)]

- Supporting Member States through the coordination of law enforcement authorities' response to cyberattacks. [Article 4(1)(m)]
- Supporting Member States in investigations against **high-risk criminals**. [Article 4(1)(q)]
- Supporting the **evaluation and monitoring mechanism** with expertise, analysis, reports and other relevant information to verify the application of the Schengen acquis as established by Council Regulation (EU) No 1053/2013. [Article 4(1)(s)]
- Facilitating and supporting a coordinated, coherent, multi-disciplinary and multi-agency response to serious crime threats by way of the **European Multidisciplinary Platform Against Criminal Threats**. [Article 4(2)]
- Supporting the Commission and the Member States in carrying out effective risk assessments by way of providing **threats assessment analysis** based on the information Europol holds on criminal phenomena and trends. [Article 4(3)]
- Clarifying that Europol staff may provide **operational support** to Member State's law enforcement authorities **on the ground** in operations and investigations. [Article 4(5)]
- Clarifying that Europol also may request, in specific cases where Europol considers that a criminal investigation should be initiated, the competent authorities of a Member State to initiate, conduct or coordinate an investigation of a **crime which affects a common interest covered by a Union policy**, without the requirement of a cross-border dimension of the crime concerned. [Article 6(1)]
- Supporting Member States in informing the public about individuals wanted under national law in relation to a criminal offence in respect of which Europol is competent, by way of the Europol website on **Europe's most wanted fugitives**. [Article 18(f)]
- Clarifying that Member States may make the **result of operational and forensic analysis** provided by Europol available to their relevant authorities, including prosecutors and criminal courts, throughout the whole lifecycle of criminal proceedings, in accordance with the applicable use restrictions and national criminal procedural law. [Article 20(3)]
- Clarifying that Europol staff may **give evidence**, which came to their knowledge in the performance of their duties or the exercise of their activities, in criminal proceedings in the Member States. [Article 20(5)]

2020/0349 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The European Union Agency for Law Enforcement Cooperation (Europol) was established by Regulation (EU) 2016/794 of the European Parliament and of the Council[52] 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. Criminals and terrorists exploit the advantages that the digital transformation and new technologies bring about, including the inter-connectivity and blurring of the boundaries between the physical and digital world. The COVID-19 crisis has added to this, as criminals have quickly seized opportunities to exploit the crisis by adapting their modes of operation or developing new criminal activities. Terrorism remains a significant threat to the freedom and way of life of the Union and its citizens.

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

[52] 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) As Europe faces increasing threats from organised crime groups and terrorist attacks, an effective law enforcement response must include the availability of well-trained interoperable special intervention units specialised in the control of crisis situations. In the Union, the law enforcement units of the Member State cooperate on the basis of Council Decision 2008/617.[53] Europol should be able to provide support to these special intervention units, including by providing operational, technical and financial support.

(5) In recent years large scale cyber attacks targeted public and private entities alike across many jurisdictions in the Union and beyond, affecting various sectors including transport, health and financial services. Cybercrime and cybersecurity cannot be separated in an interconnected environment. The prevention, investigation and prosecution of such activities is supported by coordination and cooperation between relevant actors, including the European Union Agency for Cybersecurity ('ENISA'), competent authorities for the security of network and information systems ('NIS authorities') as defined by Directive (EU) 2016/1148[54], law enforcement authorities and private parties. In order to ensure the effective cooperation between all relevant actors at Union and national level on cyber attacks and security threats, Europol should cooperate with the ENISA through the exchange of information and by providing analytical support.

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

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

(8) The Schengen Information System (SIS), established in the field of police cooperation and judicial cooperation in criminal matters by Regulation (EU) 2018/1862 of the European Parliament and of the Council[5556], is an essential tool for maintaining a high

---

53 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).

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

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

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

level of security within the area of freedom, security and justice. Europol, as a hub for information exchange in the Union, receives and holds valuable information from third countries and international organisations on persons suspected to be involved in crimes falling within the scope of Europol's mandate. Following consultation with the Member States, Europol should be able to enter data on these persons in the SIS in order to make it available directly and in real-time to SIS end-users.

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

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

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

(12) It is possible for the Union and the Members States to adopt restrictive measures relating to foreign direct investment on the grounds of security or public order. To that end, Regulation (EU) 2019/452 of the European Parliament and of the Council[57] establishes a framework for the screening of foreign direct investments into the Union that provides Member States and the Commission with the means to address risks to security or public order in a comprehensive manner. As part of the assessment of expected implications for security or public order, Europol should support the screening of specific cases of foreign direct investments into the Union that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes.

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

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

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

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

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

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

the data in the context of a criminal investigation in accordance with procedural requirements and safeguards applicable under its national criminal law.

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

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

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

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

(22) Europol and the European Public Prosecutor's Office ('EPPO') established by Council Regulation (EU) 2017/1939[58], should put necessary arrangements in place to optimise their operational cooperation, taking due account of their respective tasks and mandates. Europol should work closely with the EPPO and actively support the investigations and prosecutions of the EPPO upon its request, including by providing analytical support and exchanging relevant information, as well as cooperate with it, from the moment a suspected offence is reported to the EPPO until the moment it determines whether to prosecute or otherwise dispose of the case. Europol should,

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

without undue delay, report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence. To enhance operational cooperation between Europol and the EPPO, Europol should enable the EPPO to have access, on the basis of a hit/no hit system, to data available at Europol, in accordance with the safeguards and data protection guarantees provided for in this Regulation. The rules on the transmission to Union bodies set out in this Regulation should apply to Europol's cooperation with the EPPO. Europol should also be able to support criminal investigations by the EPPO by way of analysis of large and complex datasets.

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

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

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

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

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

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

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

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

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

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

data to Europol within this period. If the resubmitted personal data has been part of a larger set of personal data, Europol should only keep the personal data if and in so far as it has been resubmitted by a national unit, contact point or authority concerned.

(33) Any cooperation of Europol with private parties should neither duplicate nor interfere with the activities of the Financial Intelligence Units ('FIUs'), and should only concern information that is not already to be provided to FIUs in accordance with Directive 2015/849 of the European Parliament and of the Council[59]. Europol should continue to cooperate with FIUs in particular via the national units.

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

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

(36) Regulation (EU) 2018/1725 of the European Parliament and of the Council[60] [61]sets out rules on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies but it did not apply to Europol. To ensure uniform and consistent protection of natural persons with regard to the processing of personal data, Regulation (EU) 2018/1725 should be made applicable le to Europol in accordance with Article 2(2) of that Regulation, and should be complemented by specific provisions for the specific processing operations that Europol should perform to accomplish its tasks.

(37) Given the challenges that the use of new technologies by criminals pose to the Union's security, law enforcement authorities are required to strengthen their technological capacities. To that end, Europol should support Member States in the use of emerging technologies in preventing and countering crimes falling within the scope of Europol's

[59] 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).

[60] 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).

[61] 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).

objectives. To explore new approaches and develop common technological solutions for Member States to prevent and counter crimes falling within the scope of Europol's objectives, Europol should be able to conduct research and innovation activities regarding matters covered by this Regulation, including with the processing of personal data where necessary and whilst ensuring full respect for fundamental rights. The provisions on the development of new tools by Europol should not constitute a legal basis for their deployment at Union or national level.

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

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

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

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

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

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

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

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

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

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

HAVE ADOPTED THIS REGULATION:

Article 1

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

(1) Article 2 is amended as follows:

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

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

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

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

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

(2) Article 4 is amended as follows:

(a) paragraph 1 is amended as follows:

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

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

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

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

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

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

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

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

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

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

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

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

_____

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

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

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

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

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

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

"4a. Europol shall assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation activities that are relevant to achieve the objectives set out in Article 3. When Europol assists the Commission in identifying key research themes, drawing up and implementing a Union framework programme, the Agency shall not receive funding from that programme.

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

---

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

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

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

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

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

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

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

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

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

(5) Article 18 is amended as follows:

(a) paragraph 2 is amended as follows:

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

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

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

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

(f) supporting Member States in informing the public about suspects or convicted individuals who are wanted based on a national judicial decision relating to a criminal offence in respect of which Europol is competent, and facilitate the provision of information by the public on these individuals.”

(b) the following paragraph 3a is inserted:

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

(c) paragraph 5 is replaced by the following:

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

(d) the following paragraph 5a is inserted:

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

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

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

(6) The following Article 18a is inserted:

"Article 18a

Information processing in support of a criminal investigation

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

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

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

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

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

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

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

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

The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Such personal data shall be functionally separated from other data and may only be

accessed where necessary for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process.

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

(7) Article 20 is amended as follows:

(a) the following paragraph 2a is inserted:

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

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

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

(c) the following paragraph 5 is added:

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

(8) The following Article 20a is inserted:

"Article 20a

Relations with the European Public Prosecutor's Office

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

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

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

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

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

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

(10) Article 24 is replaced by the following:

"Article 24

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

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

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

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

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

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

(11) Article 25 is amended as follows:

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

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

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

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

(12) Article 26 is amended as follows:

(a) paragraph 2 is replaced by the following:

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

(b) paragraph 4 is replaced by the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Transfers shall not be systematic, massive or structural."

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

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

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

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

(e) paragraphs 9 and 10 are deleted;

(13) the following Article 26a is inserted:

"Article 26a

Exchanges of personal data with private parties in crisis situations

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

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

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

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

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

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

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

(14) the following Article 27a is inserted:

"Article 27a

Processing of personal data by Europol

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

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

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

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

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

_____

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

(15) Article 28 is deleted;

(16) Article 30 is amended as follows:

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

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

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

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

(c) paragraph 4 is deleted;

(d) paragraph 5 is replaced by the following:

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

(17) Article 32 is replaced by the following:

"Article 32

Security of processing

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

(18) Article 33 is deleted;

(19) the following Article 33a is inserted:

"Article 33a

Processing of personal data for research and innovation

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

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

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

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

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

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

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

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

(20) Article 34 is amended as follows:

(a) paragraph 1 is replaced by the following:

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

(b) paragraph 3 is deleted;

(21) Article 35 is amended as follows:

(a) paragraphs 1 and 2 are deleted;

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

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

(b) paragraphs 4 and 5 are deleted.";

(22) Article 36 is amended as follows:

(a) paragraphs 1 and 2 are deleted;

(b) paragraph 3 is replaced by the following:

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

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

(23) Article 37 is amended as follows:

(a) paragraph 1 is replaced by the following:

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

(b) paragraph 2 is deleted;

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

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

(d) paragraphs 8 and 9 are deleted.";

(24) the following Article 37a is inserted:

"*Article 37a*

Right to restriction of processing

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

(25) Article 38 is amended as follows:

(a) paragraph 4 is replaced by the following:

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

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

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

(26) Article 39 is amended as follows:

(a) paragraph 1 is replaced by the following:

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

(b) paragraphs 2 and 3 are deleted;

(27) The following Article 39a in inserted:

"*Article 39a*

Records of categories of processing activities

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

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

(b) the purposes of the processing;

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

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

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

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

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

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

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

(28) Article 40 is amended as follows:

(a) the title is replaced by the following:

"Logging"

(b) paragraph 1 is replaced by the following:

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

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

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

(29) Article 41 is replaced by the following:

"Article 41

Designation of the Data Protection Officer

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

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

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

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

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

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

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

"Article 41a

Position of the Data Protection Officer

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

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

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

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

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

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

Article 41b

Tasks of the Data Protection Officer

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

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

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

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

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

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

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

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

(h) cooperating with the EDPS;

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

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

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

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

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

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

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

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

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

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

(32) Article 43 is amended as follows:

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

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

(b) paragraph 5 is replaced by the following:

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

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

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

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

(34) Articles 45 and 46 are deleted;

(35) Article 47 is amended as follows:

(a) paragraph 1 is replaced by the following:

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

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

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

(c) the following paragraph 5 is added:

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

(36) Article 50 is amended as follows:

(a) the title is replaced by:

"Right to compensation";

(b) paragraph 1 is deleted;

(c) paragraph 2 is replaced by the following:

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

(37) Article 51 is amended as follows:

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

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

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

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

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

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

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

(39) Article 61 is amended as follows:

(a) Paragraph 1 is replaced by the following:

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

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

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

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

(c) the following paragraph 3a is inserted:

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

(40) Article 67 is replaced as follows:

"*Article 67*

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

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

arrangement, any exceptional ad hoc release of EUCI to those authorities, shall be subject to the Commission's prior approval.

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

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

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

Article 2

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

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

Done at Brussels,

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

LEGISLATIVE FINANCIAL STATEMENT

1. ARTICLE FRAMEWORK OF THE LEGISLATIVE INITIATIVE

1.1. Title of the legislative initiative

Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation (Europol) amending Regulation (EU) No 2016/794

1.2. Policy area(s) concerned

Policy area: Home Affairs

Activity: Security

12 10 01 : Europol

1.3. The proposal relates to

☐ **a new action**

☐ **a new action following a pilot project/preparatory action**[62]

☒ **the extension of an existing action**

☐ **a merger of one or more actions towards another/a new action**

1.4. Objective(s)

1.4.1. General objective(s)

In response to pressing operational needs, and calls by the co-legislators for stronger support by Europol, the Commission Work Programme for 2020 announced a legislative initiative to "strengthen the Europol mandate in order to reinforce operational police cooperation". This is a key action of the July 2020 EU Security Union Strategy. In line with the call by the Political Guidelines to "leave no stone unturned when it comes to protecting our citizens", the legislative initiative is expected to reinforce Europol to help Member States keeping citizens safe. This draft Commission proposal is part of the Counter-Terrorism package.

The general objectives of this legislative initiative result from the Treaty-based goals:

1 for Europol to support and strengthen action by the Member States' law enforcement authorities 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[63];

2 to endeavour to ensure a high level of security through measures to prevent and combat crime[64].

1.4.2. Specific objective(s)

The specific objectives derive from the general objectives outlined above:

- Specific objective n°1: enabling Europol to cooperate effectively with private parties.

62 As referred to in Article 58(2)(a) or (b) of the Financial Regulation.
63 Article 88 TFEU.
64 Article 67 TFEU

- Specific objective n°2: enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with fundamental rights

- Specific objective n°3: enabling Member States to use new technologies for law enforcement

- Specific objective n°4: providing frontline officers with the result of Europol's analysis of data received from third countries.

- Specific objective n°5: facilitating Europol's cooperation with third countries

- Specific objective n°6: strengthening Europol's capacity to request the initiation of criminal investigations

Specific objective n°1: enabling Europol to cooperate effectively with private parties

The aim is to allow Europol to process data received directly from private parties, to exchange personal data with private parties to establish jurisdiction, as well as to serve as a channel to transmit Member States' requests containing personal data to private parties

Specific objective n°2: enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with fundamental rights.

The aim is to clarify Europol's mandate in a way that enables Europol to fulfil its mandate and support Member States effectively. This concerns Europol's role as service provider handling crime-related data on behalf of the Member States. It also concerns Europol's core task of analysing personal data it received from Member States for preventing and combating crimes falling under Europol's mandate. To do so in compliance with the requirement linked to the categories of data subjects listed in annex II of the Europol Regulation, the agency needs to verify first if the data it received from Member States fall within those categories. If so, Europol is allowed to process the personal data under its legal mandate, including for preventive action and criminal intelligence, while ensuring full compliance with fundamental rights.

Specific objective n°3: enabling Member States to use new technologies for law enforcement.

Responding to the gaps identified at national level on innovation and research relevant for law enforcement, the aim is to enable Europol to provide effective support to Member States on the development and use of new technologies for law enforcement. This will support efforts to strengthen the technological sovereignty and strategic autonomy of the EU in the field of security.

Specific objective n°4: providing frontline officers with the result of Europol's analysis of data received from third countries

The aim is to provide frontline officers with the result of Europol's analysis of data received from third countries on suspects and criminals when and where this is necessary. The underlying goal is to enable frontline officers to take informed decisions when they check a person at the external border or within the area without controls at internal borders.

Specific objective n°5: facilitating Europol's cooperation with third countries

The aim is to facilitate operational cooperation between Europol and third countries including the transfer of personal data where this is necessary for law enforcement and EU internal security, exploiting the full potential of the different legal grounds for data transfers, while ensuing full compliance with EU data protection requirements. In that way, Europol will be able to better support national law enforcement authorities through its cooperation with third countries.

Specific objective n°6: strengthening Europol's capacity to request the initiation of criminal investigations

The aim is to strengthen Europol's capacity to request the initiation of criminal investigations, both at national level and by the EPPO, and in full respect of Member States' prerogatives on maintaining law and order and safeguarding internal security as well as the independence of the EPPO. In doing so, this objective will also strengthen the ability of the EPPO to initiate and effectively conduct criminal investigations and prosecutions for crimes falling under its jurisdiction.

1.4.3. Expected result(s) and impact

Specify the effects which the legislative initiative should have on the beneficiaries/groups targeted.

The proposal will primarily benefit **individuals and society at large** by improving Europol's ability to support Member States in countering crime and protecting EU citizens. Citizens will directly and indirectly benefit from lower crime rates, reduced economic damages, and less security related costs. The proposal does not contain regulatory obligations for citizens/consumers, and does not create additional costs in that regard.

The proposal will create economies of scale for **administrations** as it will shift the resource implications of the targeted activities from the national level to the EU level. Public authorities in Member States will directly benefit from the proposal thanks to economies of scale leading to savings in administrative costs.

The proposal will also have a positive impact on the environmental area to the extent that law enforcement authorities in the EU will be able to fight environmental crimes more effectively.

1.4.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

The following main indicators will allow the monitoring of the implementation and performance of the specific objectives:

Specific objective n°1: enabling Europol to cooperate effectively with private parties.

- Number of contributions received from private parties
- Number of contributions from private parties shared with Member States concerned
- Number of requests to Member States to obtain personal data from private parties
- Number of requests to channel Member States' requests to private parties

Specific objective n°2: enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with fundamental rights

- Number of entities cross-checked for the purpose of verifying if the data received relates to the specific categories of data subjects set out in annex II of the Europol Regulation
- Number of cases where high volumes of personal data is received
- Number of 'information alerts' issued by Europol
- Number of 'hits' generated by 'information alerts'

Specific objective n°3: enabling Member States to use new technologies for law enforcement

- Amount of personal data processed for the purpose of innovation
- Number of digital tools for law enforcement created

Specific objective n°4: providing frontline officers with the result of Europol's analysis of data received from third countries

- Number of Schengen evaluations supported
- Number of 'information alerts' issued by Europol

- Number of 'hits' generated by 'information alerts'

Specific objective n°5: facilitating Europol's cooperation with third countries

- Number of cases where personal data has been transferred subject to appropriate safeguards or for specific situations

Specific objective n°6: strengthening Europol's capacity to request the initiation of criminal investigations and support to the EPPO

- Number of requests by Europol to Member States
- Number of positive replies by Member States
- Number of requests by Europol to the EPPO
- Number of contributions by Europol to the EPPO
- Number of EPPO's cases and investigations supported
- Number of hits in Europol's database generated by EPPO's information

Indicators linked to other amendments including data protection alignment:- Number of international investigations/operations supported (including in the framework of Joint Investigations Teams[65], Operational Task Forces[66], and involving third countries)

- Number and amount of High Value Grants (HVGs) and Low Value Grants (LVGs) awarded
- Number of data protection incidents reported and EDPS Decisions
- Number of requests from private persons to Europol's data protection officer

In line with Article 28 of the FFR and to ensure sound financial management, Europol already monitors progress in the achievement of its objectives with performance indicators. The agency currently has 35 Key Performance Indicators, further complemented by 60 Corporate Performance Indicators. These indicators are reported in Europol's Consolidated Annual Activity Report, which include a clear monitoring of the target by end of year as well as comparison with the previous year. These indicators will be adapted as needed following adoption of the proposal.

Moreover, concerning in particular the specific objective n°4 which foresees the introduction of a new SIS alert category in joint work with eu-LISA, the following indicators are identified for eu-LISA:

- Successful completion of comprehensive pre-launch testing at Central level,

[65] Joint Investigation Team (JIT) is an international cooperation tool based on an agreement between competent authorities - both judicial (judges, prosecutors, investigative judges) and law enforcement - of two or more States, established for a limited duration and for a specific purpose, to carry out criminal investigations in one or more of the involved States. JITs constitute an efficient and effective cooperation tool that facilitates the coordination of investigations and prosecutions conducted in parallel in several States or in cases with a cross-border dimension.

[66] Operational Task Force (OTF) is a temporary group of representatives of Member States, Third Parties and Europol and a specific multi-national/disciplinary project consisting of intelligence and investigative activities against selected High Value Targets. High Value Target (HVT) is a person whose criminal activity fulfils specified risk criteria and therefore constitutes a high risk of serious and organised crime to two or more Member States.

- Successful completion of tests for all Member States National Systems and Agencies

- Successful completion of SIRENE tests for the new category

1.5. Grounds for the legislative initiative

1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the legislative initiative

The roll-out of the implementation of the legislative initiative requires technical and procedural measures at EU and national level, which should start when the revised legislation enters into force. The relevant resources – in particular human resources - should be scaled up over time in line with the increase in demand for Europol's services.

The main requirements following entry into force of the proposal are as follows:

To enable Europol to cooperate effectively with private parties:

- Companies to adapt their internal procedures.

- Europol and Member States to agree on procedure ensuring that Europol requests are in line with national requirements.

- Member States to adapt their national procedure to ensure that they can enforce national request based on need to obtain such information for Europol.

- Europol to set up IT structure for channelling Member States' requests to private parties.

To enable law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with fundamental rights

- Europol to ensure availability of necessary infrastructure and expertise to process large and complex datasets in support of specific criminal investigations by the Member States, and to retain such datasets when necessary for judicial proceedings in the Member States

To enable Member States to use new technologies for law enforcement

- Europol to ensure availability of necessary infrastructure, including the Decryption Platform, and capabilities to support the implementation of innovation projects and to adapt internal procedures.

To provide frontline officers with the result of Europol's analysis of data received from third countries

- Members States to update their national systems and SIRENE workflows ("Supplementary Information Request at the National Entries") to allow for the introduction of a new SIS alert category.

- Europol and eu-LISA to adapt the IT systems to allow for the introduction of a new SIS alert category.

To facilitate Europol cooperation with priority third countries:

-Member States and European Data Protection Supervisor to provide guidance and best practices.

-Europol to make efficient use of possibilities to exchange personal data with third country

To strengthen Europol's capacity to request the initiation of criminal investigations:

-Europol to align its working arrangement (negotiated or concluded) with the EPPO, according to the provisions of the amended Europol Regulation

-Europol to report suspected PIF cases, to provide relevant information, on-the-spot-support, operational analysis, forensic and technical expertise and specialised training, upon request of the EPPO.

-Europol to adapt its internal data processing and operational workflows and procedures to provide the aforementioned support to the EPPO.

-Europol to make the necessary IT arrangements to allow the EPPO to have indirect access to Europol's database on the basis of a hit/no hit system. FTEs to be scaled up in the first years of implementation, as the volume of EPPO investigations and prosecutions increases.

Following entry into application, the implementation of the activities will be rolled-out in a gradual timeline, to follow the expected gradual increase of data flows, demands on Europol's services and activities, as well as necessary time for absorption of new resources.

1.5.2. Added value of Union involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this point 'added value of Union involvement' is the value resulting from Union intervention which is additional to the value that would have been otherwise created by Member States alone.

Serious crime and terrorism are of a transnational nature. Therefore, action at national level alone cannot counter them effectively. This is why Member States choose to work together within the framework of the EU to tackle the threats posed by serious crime and terrorism.

Moreover, evolving security threats, driven by the way criminals exploit the advantages that the digital transformation, globalisation and mobility bring about, also call for effective EU level support to the work of national law enforcement authorities. EU action provides for an effective and efficient way to step up the support to Member States in fighting serious crime and terrorism to keep pace with these threats.

The proposal will create significant economies of scale at an EU level, as it will shift tasks and services, which can be performed more efficiently at an EU level, from the national level to Europol. The proposal therefore provides for efficient solutions to challenges, which would otherwise have to be addressed at higher costs by means of 27 individual national solutions, or to challenges which cannot be addressed at the national level at all in view of their transnational nature.

1.5.3. Lessons learned from similar experiences in the past

The proposal builds on the need to address continuously-evolving transnational security challenges in Europol beyond the national level alone.

Europe faces a security landscape in flux, with evolving and increasingly complex security threats. Criminals exploit the advantages that the digital transformation, new technologies,

globalisation and mobility bring about, including the inter-connectivity and blurring of the boundaries between the physical and digital world. The COVID-19 crisis only added to this, as criminals quickly seized the opportunities to exploit the crisis by adapting their modes of operation or developing new criminal activities.

These evolving security threats call for effective EU level support to the work of national law enforcement authorities. Member States' law enforcement authorities have increasingly made use of the support and expertise that Europol offers to counter serious crime and terrorism.

This proposal also builds on the lessons learned and progress achieved since the entry into application of the 2016 Europol Regulation, while recognising that the operational importance of the agency's tasks has already changed substantially. The new threat environment has changed the support Member States need and expect from Europol to keep citizens safe, in a way that was not foreseeable when the co-legislators negotiated the current Europol mandate.

Previous reviews of Europol's mandate and the growing demand for services by Member States has also shown that Europol's tasks need to be backed by adequate financial and human resources.

1.5.4. Compatibility with the Multiannual Financial Framework and possible synergies with other appropriate instruments

The proposal responds to the changing security landscape as it will equip Europol with the necessary capabilities and tools to support Member States effectively in countering serious crime and terrorism. The Communication "Europe's moment: Repair and Prepare for the Next Generation"[67] underlined the necessity of building a more resilient Union as the COVID-19 crisis "*revealed a number of vulnerabilities and a significant increase in certain crimes, such as cybercrime. This shows the need to reinforce the EU Security Union*".

The proposal is fully in line with the Commission Work Programme for 2020 which announced a legislative initiative to "strengthen the Europol mandate in order to reinforce operational police cooperation"[68].

This strenghtening of Europol's mandate is one of the key actions identified in the July 2020 EU Security Union Strategy[69]. A more effective Europol will ensure that the agency can fully perform its tasks and can assist in reaching the strategic priorities for the Security Union.

In line with the call by the Political Guidelines[70] to "*leave no stone unturned when it comes to protecting our citizens*", this proposal addresses those areas where stakeholders ask for reinforced support by Europol to help Member States keeping citizens safe.

Moreover, the proposal takes account of a range of Commission initiatives, including the legislative initiative on the removal of terrorist content online[71]. The proposed objective to strengthen Europol's support for innovation takes account of the European strategy for data[72] and the White Paper on Artificial Intelligence.[73]

67 COM(2020) 456 (27.5.2020)
68 COM(2020) 440 final – Annexes 1 to 2 (27.5.2020)
69 COM(2020) 605 final (24.7.2020).
70 https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.
71 COM(2018) 640 final (12.9.2018).
72 COM(2020) 66 final (19.2.2020).
73 COM(2020) 65 final (19.2.2020).

The proposal will also create synergies with the activities of relevant authorities at EU level and in particular Eurojust, the European Public Prosecutor's Office and OLAF by strenghtening overall cooperation with Europol, in line with the bodies' respective mandates and competences.

1.5.5. Assessment of the different available financing options, including scope for redeployment

The Multiannual Financial Framework proposal for 2021-2027 recognises the need to reinforce Europol in order to increase support to Member States' law enforcement authorities in 2021.

Since 2016 and the last revision of Europol's mandate, the trend has been towards an exponential growth of the agency's data flows and of the demand on its services[74], leading to yearly budget and staff reinforcements above the levels initially programmed.

Since the proposal will introduce important new tasks in Europol Regulation and will also clarify, codify and detail other tasks, hereby extending Europol's capabilities within the context of the treaties, it therefore cannot be covered by a stable level of resources. The proposal needs to be backed by financial and human reinforcements.

[74] Europol's 2019 operational indicators show that: the number of operations has tripled since 2014; the deployment of mobile office on the spot has more than doubled; the number of messages exchanged via the SIENA network has increased by 300%; the number of objects inserted in the Europol Information System has increased by more than 500%.

1.6. Duration and financial impact of the legislative initiative

☐ **limited duration**

☐ Proposal/initiative in effect from [DD/MM]YYYY to [DD/MM]YYYY

☐ Financial impact from YYYY to YYYY

☒ **unlimited duration**

Implementation with a start-up period from 2022 to 2027

followed by full-scale operation.

1.7. Management mode(s) planned[75]

☐ **Direct management** by the Commission through

☐ executive agencies

☐ **Shared management** with the Member States

☒ **Indirect management** by entrusting budget implementation tasks to:

☐ international organisations and their agencies (to be specified);

☐the EIB and the European Investment Fund;

☒ bodies referred to in Articles 70 and 71;

☐ public law bodies;

☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

Comments

The baseline for the EU contribution to Europol's budget has been identified based on the MFF Fiche n°68[76] and on the Working Document III accompanying the Draft Budget 2021. The information is this LFS is without prejudice to the adoption of the MFF 2021-2027 and the Budget 2021.

In the absence of a voted MFF 2021-2027 and Budget 2021, the estimated financial impact of the legislative initiative includes only the resources needed in addition to Europol's baseline EU contribution (additional costs compared to the baseline – Fiche n°68).

[75] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

[76] Working document of the commission services – Decentralised agencies and EPPO.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

The monitoring and reporting of the proposal will follow the principles outlined in Europol's Regulation[77], Financial Regulation[78] and in line with the Common Approach on decentralised agencies[79].

Europol must notably send each year to the Commission, the European Parliament and the Council a Single Programming Document containing multi-annual and annual work programmes and resources programming. The Document sets out the objectives, expected results and performance indicators to monitor the achievement of the objectives and the results. Europol must also submit a Consolidated Annual Activity Report to the management board. This report notably includes information on the achievement of the objectives and results set out in the Single Programming Document. The report must also be sent to the Commission, the European Parliament and the Council.

Moreover, as outlined in Article 68 of Europol's Regulation, the Commission must commission an evaluation of Europol by 1 May 2022 and every five years after that. This evaluation will assess, in particular, the impact, effectiveness and efficiency of Europol and of its working practices. The evaluation reports must be submitted to the specialised Joint Parliamentary Scrutiny Group, which politically monitors Europol's activities in fulfilling its mission, including as regards the impact of those activities on the fundamental rights and freedoms of natural persons. The reports are also submitted to the Council, the national parliaments and Europol's Management Board. Where appropriate, the main findings of the evaluation reports are made public.

To regularly monitor the provision of information by the Member States, Europol will also report annually to the Commission, European Parliament, the Council and national parliaments on the information provided by each Member State as concerns the information Europol needs to fulfil its objectives, including information relating to forms of crime the prevention or combating of which is considered a priority by the Union. The reports are drawn up on the basis of the quantitative and qualitative evaluation criteria defined by Europol's Management Board.

Finally, the proposal includes a provision requiring an assessment of the impact on fundamental rights two years after their entry into application.

[77] Regulation (EU) 2016/794

[78] https://www.europol.europa.eu/sites/default/files/documents/decision_of_the_europol_management_board_on_the_adoption_of_the_financial_regulation_applicable_to_europol_.pdf

[79] https://europa.eu/european-union/sites/europaeu/files/docs/body/joint_statement_and_common_approach_2012_en.pdf

2.2. Management and control system(s)

2.2.1. Justification of the management mode(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed

Considering that the proposal impacts the annual EU contribution to Europol, the EU budget will be implemented via indirect management.

Pursuant to the principle of sound financial management, the budget of Europol shall be implemented in compliance with effective and efficient internal control[80]. Europol is therefore bound to implement an appropriate control strategy coordinated among appropriate actors involved in the control chain.

Regarding ex-post controls, Europol, as a decentralised agency, is notably subject to :

- internal audit by the Internal Audit Service of the Commission

- annual reports by the European Court of Auditors, giving a statement of assurance as to the reliability of the annual accounts and the legality and regularity of the underlying transactions

- annual discharge granted by the European Parliament

- possible investigations conducted by OLAF to ensure, in particular, that the resources allocated to agencies are put to proper use.

As partner DG to Europol, DG HOME will implement its Control Strategy on decentralised agencies to ensure reliable reporting in the framework of its Annual Activity Report (AAR). While decentralised agencies have full responsibility for the implementation of their budget, DG HOME is responsible for regular payment of annual contributions established by the Budgetary Authority.

Finally, the European Ombudsman provides a further layer of control and accountability at Europol.

2.2.2. Information concerning the risks identified and the internal control system(s) set up to mitigate them

The following risks are identified:

- strained operational resources due to increasing data flows and constantly evolving criminal activities landscape

- fragmentation of Europol's core business due to multiplication of tasks and requests

- lack of adequate levels of financial and human resources to match operational needs

- lack of ICT resources, resulting in delays in necessary core system developments and updates

- risks related to Europol's processing of personal data and the need to regularly evaluate and adapt procedural and technical safeguards in order to ensure the protction of personal data and fundamental rights.

- depedencies between the preparations to be done by eu-LISA with regard to Central SIS and the preparations to be done by Europol with regard to setting up a technical interface to transmit data to SIS

[80] Article 30 of Europol's Financial Regulation

Europol implements a specific Internal Control Framework based on the Internal Control Framework of the European Commission and on the original Committee of Sponsoring Organisations' integrated internal control framework. The Single Programming Document must provide information on the internal control systems, while the Consolidated Annual Activity Report (CAAR) must contain information on the efficiency and effectiveness of the internal control systems, includind as regards risk assessment. The CAAR 2019 reports that, based on the analysis of the internal control components and principles which have been monitored in the course of 2019, using both quantitative and qualitative elements, the Europol Internal Control System is assessed as present and functioning in an integrated manner across the agency.

Another level of internal supervision is also provided by Europol's Internal Audit Capability, on the basis of an annual audit plan notably taking into consideration the assessment of risks in Europol. The Internal Audit Capability helps Europol in accomplishing its objectives by bringing a systematic and disciplined approach to evaluate the effectiveness of risk management, control, and governance processes, and by issuing recommendations for their improvement.

Moroever, the EDPS and Europol's data protection officer (an independent function attached directly to the Mangement Board Secretariat) supervise Europol's processing of personal data.

Finally, as partner DG of Europol, DG HOME runs an annual risk management exercise to identify and assess potential high risks related to agencies' operations, including Europol. Risks considered as critical are reported annually in DG HOME management plan and are accompanied by an action plan stating the mitigating action.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio of "control costs ÷ value of the related funds managed"), and assessment of the expected levels of risk of error (at payment & at closure)

The ratio of "control costs/value of the related funds managed" is reported on by the Commission. The 2019 AAR of DG HOME reports 0.28% for this ratio in relation to Indirect Management Entrusted Entities and Decentralised Agencies, including Europol.

The European Court of Auditors confirmed the legality and regularity of Europol's annual accounts for 2019, which implies an error rate below 2%. There are no indications that the error rate will worsen in the coming years.

Moreover, article 80 of Europol's Financial Regulation provides for the possibility for the agency to share an internal audit capability with other Union bodies functioning in the same policy area if the internal audit capability of a single Union body is not cost-effective.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures, e.g. from the Anti-Fraud Strategy.

The measures related to combating fraud, corruption and any other illegal activities are outlined, inter alia, in article 66 of Europol's Regulation and under Title X of Europol's Financial Regulation.

Europol shall notably participate in fraud prevention activities of the European Anti-fraud Office and inform the Commission without delay on cases of presumed fraud and other financial irregularities – in line with its internal anti-fraud strategy.

An update to the Europol anti-fraud strategy is planned to be proposed for adoption to the Management Boad in 2020.

Moreover, as partner DG, DG HOME has developed and implemented its own anti-fraud strategy on the basis of the methodology provided by OLAF. Decentralised agencies, including Europol, fall within the scope of the strategy. DG HOME 2019 AAR concluded that the fraud prevention and detection processes worked satisfactorily and therefore contributed to the assurance on the achievement of the internal control objectives.

3. ESTIMATED FINANCIAL IMPACT OF THE LEGISLATIVE INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[81]	from EFTA countries[82]	from candidate countries[83]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
5	12 10 01	Diff./non-diff.	NO	NO	NO	YES/NO

New budget lines requested

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./non-diff.	from EFTA countries	from candidate countries	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation

[81] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

[82] EFTA: European Free Trade Association.

[83] Candidate countries and, where applicable, potential candidates from the Western Balkans.

	[XX.YY.YY.YY]		YES/NO	YES/NO	YES/NO	YES/NO

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

In the absence of a voted MFF 2021-2027 and Budget 2021, the estimated financial impact of the legislative initiative includes only the resources needed in addition to Europol's baseline EU contribution (additional costs compared to the baseline – Fiche n°68).

EUR million (to three decimal places)

Heading of multiannual financial framework	Number	Heading 5 –Security and Defence

[Body]:Europol			Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Title 1:	Commitments	(1)							
	Payments	(2)							
Title 2:	Commitments	(1a)							
	Payments	(2a)							
Title 3:	Commitments	(3a)							
	Payments	(3b)							
TOTAL appropriations for Europol	Commitments	=1+1a +3a	**15,987**	**23,946**	**29,427**	**30,965**	**40,019**	**37,524**	**177,867**
	Payments	=2+2a +3b	**15,987**	**23,946**	**29,427**	**30,965**	**40,019**	**37,524**	**177,867**

Heading of multiannual financial framework	**5**	'Administrative expenditure'

EUR million (to three decimal places)

		Year **2021**	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
DG: HOME									
• Human Resources		0,835	0,835	0,835	0,835	0,835	0,835	0,835	5,845
• Other administrative expenditure		0,268	0,518	0,268	0,518	0,268	0,518	0,268	**2,626**
TOTAL DG HOME	Appropriations								

TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	1,103	1,353	1,103	1,353	1,103	1,353	1,103	**8,471**

EUR million (to three decimal places)

		Year **2021**	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments								
	Payments								

3.2.2. Estimated impact on Europol's appropriations

☐ The proposal/initiative does not require the use of operational appropriations

☒ The proposal/initiative requires the use of operational appropriations, as explained below:

In the absence of a voted MFF 2021-2027 and Budget 2021, the estimated financial impact of the legislative initiative includes only the resources needed in addition to Europol's baseline EU contribution (additional costs compared to the baseline – Fiche n°68).

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs			Year		Year		Year		Year		Year		Year		TOTAL	
			2022		**2023**		**2024**		**2025**		**2026**		**2027**			
⇩	Type	Average cost [84]	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost
SPECIFIC OBJECTIVE NO 1																
Enabling Europol to cooperate effectively with private parties																
- Output	Personal data forwarded to Member States concerned - 75%			3,453		5,669		7,192		8,172		9,636		9,306		43,428
- Output	Europol used as channel to transmit Member States request - 25%			1,151		1,890		2,397		2,724		3,212		3,102		14,476

[84] Due to their specific operational nature, it is not possible to identify a precise, unit costs per output, nor exact expected volume of outputs, notably as some outputs are related to law enforcement activities reactive to unpredictable criminal activities.

Subtotal for specific objective N°1				**4,604**		**7,559**		**9,589**		**10,896**		**12,848**		**12,409**		**57,905**
SPECIFIC OBJECTIVE NO 2																	
Enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with fundamental rights																	
- Output	Investigative case files supported in ongoing investigations - 90%			0,534		0,977		1,272		1,443		1,641		1,774		7,639
- Output	Investigative case files stored for judicial proceedings - 10%			0,059		0,109		0,141		0,160		0,182		0,197		0,849
Subtotal for specific objective N°2				**0,593**		**1,085**		**1,413**		**1,603**		**1,823**		**1,971**		**8,488**
SPECIFIC OBJECTIVE NO 3																	
enabling Member States to use new technologies for law enforcement																	
- Output	Innovation projects implemented - 75%			3,290		3,470		6,365		5,668		8,206		7,272		34,269
- Output	IT solutions tested in Europol's IT environment - 25%			1,097		1,157		2,122		1,889		2,735		2,424		11,423
- Output																-
Subtotal for specific objective N°3				**4,387**		**4,626**		**8,486**		**7,557**		**10,941**		**9,696**		**45,693**
SPECIFIC OBJECTIVE NO 4																	

Providing frontline officers with the result of Europol's analysis of data received from third countries																
- Output	Alerts in the Schengen Information System created - 50%			1,526		2,737		2,386		2,592		3,289		2,855		15,385
- Output	24/7 follow-up provided to MS - 50%			1,526		2,737		2,386		2,592		3,289		2,855		15,385
- Output																-
Subtotal for specific objective N°4				**3,052**		**5,474**		**4,772**		**5,183**		**6,579**		**5,710**		**30,770**
SPECIFIC OBJECTIVE NO 5																
Facilitating Europol's cooperation with third countries																
- Output	Operations with third countries supported - 75%			1,147		1,648		1,251		1,307		1,916		1,863		9,132
- Output	Information exchanged with third countries - 25%			0,382		0,549		0,417		0,436		0,639		0,621		3,044
- Output																-
Subtotal for specific objective N°5				**1,529**		**2,197**		**1,668**		**1,743**		**2,554**		**2,484**		**12,175**
SPECIFIC OBJECTIVE NO 6																
Strengthening Europol's capacity to request the initiation of criminal investigations																
- Output	Initiation of criminal investigations requested - 25%			0,456		0,751		0,875		0,996		1,318		1,314		5,709
- Output	Investigations of the EPPO			1,367		2,252		2,624		2,987		3,955		3,941		17,127

	supported - 75%														
Subtotal for specific objective N°6			**1,823**		**3,003**		**3,498**		**3,983**		**5,274**		**5,255**		**22,836**
TOTAL COSTS			**15,987**		**23,946**		**29,427**		**30,965**		**40,019**		**37,524**		**177,867**

3.2.3. Estimated impact on Europol's human resources

3.2.3.1. Summary

☐ The proposal/initiative does not require the use of appropriations of an administrative nature

☒ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**	**TOTAL**
Temporary agents - Baseline (Draft Budget Request 2021)[85]	102,859	102,859	102,859	102,859	102,859	102,859	**617,153**
Temporary agents – Additional compared to the baseline (cumulative)	5,937	14,384	19,067	22,830	25,171	26,342	**113,730**
Temporary agents[86] - TOTAL	108,796	117,242	121,925	125,688	128,030	129,201	**730,883**
Contract staff - Baseline[87]	20,962	20,962	20,962	20,962	20,962	20,962	**125,772**
Seconded National Experts - Baseline (Draft Budget Request 2021)[88]	6,729	6,729	6,729	6,729	6,729	6,729	**40,374**
TOTAL only additional costs	5,937	14,384	19,067	22,830	25,171	26,342	**113,730**
TOTAL – including baseline and additional costs	136,487	144,933	149,616	153,379	155,721	156,892	**897,029**

Staff requirements (FTE):

	Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**

[85] Staff levels indicated in Draft Budget 2021, calculated on the basis of the average staff unit costs to be used for LFS, indexed to the correction coefficient for the Netherlands (111,5%).

[86] It is not possible at this stage to provide the detailed allocation between temporary agent – AD and temporary agents – AST. The costs estimates for staff have been made on the basis of the average costs for temporary agent, indexed to the correction coefficient for the Netherlands (111,5%).

[87] The authorized levels of contract staff will be reinforced in the 2021 EU contribution of Europol and will stay stabilised at this level for the entire MFF 2021-2027. No increase of contract agents is foreseen in the LFS.

[88] Staff levels indicated in Draft Budget 2021, calculated on the basis of the average staff unit costs to be used for LFS, indexed to the correction coefficient for the Netherlands (111,5%).

Temporary agents – Baseline (Draft Budget Request 2021)	**615**	**615**	**615**	**615**	**615**	**615**
Temporary agents – Additional compared to the baseline (cumulative)	**71**	**101**	**127**	**146**	**155**	**160**
Temporary agents – TOTAL	**686**	**716**	**742**	**761**	**770**	**775**
Contract staff	**235**	**235**	**235**	**235**	**235**	**235**
Seconded National Experts	**71**	**71**	**71**	**71**	**71**	**71**
TOTAL	**992**	**1022**	**1048**	**1067**	**1076**	**1081**

Recruitement dates are planned at mid-year. The amounts have been adapted accordingly: the costs of newly recruited staff have been estimated at 50% of the average costs for their recruitment year.

The human ressources necessary to implement the objectives of the new mandate have been estimated in cooperation with Europol. The estimates take into consideration the expected increase in workload as stakeholders make more use of Europol's services over time, as well as the time needed for Europol to absorb resources in order to avoid a situation where the agency would not be able to fully implement its EU contribution and commit appropriations in due time.

No increase in contract agents is foreseen in the LFS. The Commission intends to propose to increase its recommendation for the level of contract agents from 191 to 235 to provide IT and administrative support to the operational activities. The maximum level of contract agents will be set at 235 in 2021 and should be stabilised at this level for the entire MFF 2021-2027.

Details of the staff increase

Specific objective	Additional staff	Allocation in Europol
Specific objective n°1	Additional staff needed to analyse additional data coming from private parties. Estimated FTEs needed – additional FTE to be hired per year (not-cumulative): 2022: +27; 2023: +13; 2024: +10; 2025: +9; 2026: +1; 2027: +2	Operations Directorate : * Europol Cybercrime Centre (EC3) * European Counter-Terrorism Centre – Operations (CT) and EU Internet Referral Unit (IRU) Capabilities Directorate - ICT

Specific objective n°2	Additional staff needed to manage, process and analyse large and complex datasets and maintain IT systems, including in the context of EU Policy Cycle for organised and serious international crime and investigations in "high-value targets". Additional staff is also needed for the Data Protection Function to ensure large and complex data is processed in full compliance with fundamental rights. Estimated FTEs needed – additional FTE to be hired per year (not-cumulative): 2022: +4; 2023: +2; 2024: +2; 2025: +1; 2026: +1; 2027: +1	Operations Directorate - *Europol Cybercrime Centre (EC3) * European Counter-Terrorism Centre – Operations (CT) and EU Internet Referral Unit (IRU)
Specific objective n°3	Additional staff needed to run Europol's innovation lab, support the EU innovation hub for internal security, and to support the management of security research. Estimated FTEs needed – additional FTE to be hired per year (not-cumulative): 2022: +12; 2023: +10; 2024: +5; 2025: +5; 2026: +1; 2027: +0	Operations Directorate : Europol Cybercrime Centre (EC3) Capabilities Directorate - ICT Innovation Lab
Specific objective n°4	Additional staff needed to create alerts in the Schengen Information System and to provide 24/7 follow up to Member States in case of a hit. FTEs to be scaled up in the first years of implementation, to follow expansion of the new system's users. The need of 24/7 support implies necessary human resources (shift work). Additional staff is also needed to support Schengen evaluations. Estimated FTEs needed – additional FTE to be hired per year (not-cumulative): 2022: +15; 2023: +2; 2024: +5; 2025: +0; 2026: +0; 2027: +0	Operations Directorate : *Operational Centre (24/7) * European Counter-Terrorism Centre – Operations (CT) and EU Internet Referral Unit (IRU) Capabilities Directorate – ICT
Specific objective n°5	Additional staff needed to make use of its mechanism to exchange personal data with third countries where necessary. No additional staff is foreseen for the activities related to best practices and guidance. Estimated FTEs needed – additional FTE to be hired per year (not-cumulative): 2022: +5; 2023: +0; 2024: +2; 2025: +0; 2026: +3; 2027: +0	Capabilities Directorate - ICT
Specific objective n°6	Additional staff needed to coordinate with the Member States and to support Member States in their investigation (incl. on-the-spot-support, access to criminal databases and analytical tools, operational analysis, forensic and technical expertise).	Operations Directorate : - European Serious & Organised Crime Centre (ESOCC) - European Counter-

	Additional staff is also needed to coordinate with EPPO and to actively support EPPO in its investigations and prosecutions. Estimated FTEs needed – additional FTE to be hired per year (not-cumulative): 2022: +8; 2023: +3; 2024: +2; 2025: +4; 2026: +3; 2027: +2	Terrorism Centre – Operations (CT) - European Financial & Economic Crime Centre (EFECC) Capabilities Directorate - ICT

3.2.3.2. Estimated requirements of human resources for the parent DG

☐ The proposal/initiative does not require the use of human resources.

☒ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full amounts (or at most to one decimal place)

		Year **2022**	Year **2023**	Year **2024**	Year **2025**	Year **2026**	Year **2027**
• **Establishment plan posts (officials and temporary staff)**							
XX 01 01 01 (Headquarters and Commission's Representation Offices)		5	5	5	5	5	5
XX 01 01 02 (Delegations)							
XX 01 05 01 (Indirect research)							
10 01 05 01 (Direct research)							
• **External staff (in Full Time Equivalent unit: FTE)**[89]							
XX 01 02 01 (AC, END, INT from the 'global envelope')		1	1	1	1	1	1
XX 01 02 02 (AC, AL, END, INT and JPD in the Delegations)							
XX 01 04 ***yy***[90]	- at Headquarters[91]						
	- in Delegations						
XX 01 05 02 (AC, END, INT – Indirect research)							
10 01 05 02 (AC, END, INT – Direct research)							
Other budget lines (specify)							
TOTAL							

XX is the policy area or budget title concerned.

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

89 AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT = agency staff; JPD = Junior Professionals in Delegations .

90 Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

91 Mainly for the Structural Funds, the European Agricultural Fund for Rural Development (EAFRD) and the European Fisheries Fund (EFF).

Officials and temporary staff	Represent the Commission in the Management Board of the Agency. Draw up Commission opinion on the annual work programme and monitor its implementation. Monitor implementation of the budget. Assist the Agency in developing its activities in line with EU policies, including by participating in experts meetings.
External staff	One SNE will support the officials and temporary staff in the above tasks and assist the Agency in developing its activities in line with EU policies, including by participating in experts meetings.

Description of the calculation of cost for FTE units should be included in the Annex V, section 3.

3.2.4. Compatibility with the current multiannual financial framework

☐ The proposal/initiative is compatible the current multiannual financial framework.

☐ The proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

Explain what reprogramming is required, specifying the budget lines concerned and the corresponding amounts. The proposal includes additional financial and human resources for Europol compared to what is currently foreseen in the MFF proposal (Fiche N°68). The budgetary impact of the additional financial resources for Europol will be offset through a compensatory reduction from programmed spending under Heading 4.

☐ The proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework[92].

Explain what is required, specifying the headings and budget lines concerned and the corresponding amounts. […]

3.2.5. Third-party contributions

The proposal/initiative does not provide for co-financing by third parties.

The proposal/initiative provides for the co-financing estimated below:

EUR million (to three decimal places)

	Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)			Total
Specify the co-financing body								
TOTAL appropriations co-financed								

[92] See Articles 11 and 17 of Council Regulation (EU, Euratom) No 1311/2013 laying down the multiannual financial framework for the years 2014-2020.

3.3. Estimated impact on revenue

☒ The proposal/initiative has no financial impact on revenue.

☐ The proposal/initiative has the following financial impact:

☐ on own resources

☐ on other revenue

☐ please indicate, if the revenue is assigned to expenditure lines

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative[93]						
		Year **N**	Year **N+1**	Year **N+2**	Year **N+3**	Enter as many years as necessary to show the duration of the impact (see point 1.6)		
Article …….								

For miscellaneous 'assigned' revenue, specify the budget expenditure line(s) affected.

[…]

Specify the method for calculating the impact on revenue.

[…]

[93] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.

Legislative Proposal - Information Note Template
COM (2020) 796 final

Information Note

1. Proposal
Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

2. Date of Commission document
9.12.2020

3. Number of Commission document
COM (2020) 796 final

4. Number of Council document:
N/A

5. Dealt with in Brussels by
Justice and Home Affairs Council (JHA)
Law Enforcement Working Party (LEWP)
The lead DG is the Directorate-General for Migration and Home Affairs (DG HOME).

6. Department with primary responsibility
Department of Justice

7. Other Departments involved
N/A

8. Background to, short summary and aim of the proposal
Europol is the European Union's law enforcement agency. It offers support and expertise to law enforcement authorities of the EU Member States to combat serious international crime and terrorism. Europol also works with many non-EU partner States and international organizations in particular in the fight against terrorism, cybercrime and people smuggling. In 2016 a new regulation for Europol (EU 2016/794) was adopted, including by Ireland, which extended Europol's role and responsibilities to allow for a coordinating role in investigations. The Europol Regulation defines Europol's role, enhances the supply of information by Member States to it, reinforces the data protection regime applicable to Europol and improves its governance structures. The EU is now facing a growing and evolving threat of transnational criminal and terrorist activity, bolstered by technological innovation, mobility and, more recently Covid-19. National-level action by Member States is not of itself always sufficient. There is now a proposal on the table for a new Regulation to

amend Regulation 2016/794 to strengthen the mandate of Europol to assist the national law enforcement authorities of Member States in addressing crime and terrorism where they manifest across borders. The primary focus of the new Regulation includes:

- *enabling Europol to cooperate effectively with private parties, addressing lack of effective cooperation between private parties and law enforcement authorities to counter the use of cross-border services (e.g. communication, banking, transport services) by criminals;*
- *enabling Europol to effectively support Member States and their investigations with the analysis of large and complex datasets, addressing the big data challenge for law enforcement authorities;*
- *strengthening Europol's role on research and innovation, addressing gaps relevant for law enforcement;*
- *strengthening Europol's cooperation with third countries in specific situations and on a case-by-case basis for preventing and countering crimes falling within the scope of Europol's objectives;*
- *clarifying that Europol may request, in specific cases where Europol considers that a criminal investigation should be initiated, the competent authorities of a Member State to initiate, conduct or coordinate an investigation of a crime which affects a common interest covered by a Union policy, without the requirement of a cross-border dimension of the crime concerned;*
- *strengthening Europol's cooperation with the European Public Prosecutor's Office (EPPO);*
- *further strengthening the data protection framework applicable to Europol;*
- *further strengthening parliamentary oversight and accountability of Europol.*

9. Legal basis of the proposal

The legal basis of the legislative initiative is Article 88 of the Treaty on the Functioning of the European Union (TFEU).

10. Voting Method

QMV

11. Role of the EP

Co-decision

12. Category of proposal

Major significance

13. Implications for Ireland & Ireland's Initial View

Ireland fully supports the strengthening of Europol's legal mandate to support Member States in preventing and combatting serious crime and terrorism in the manner proposed. This legislative initiative takes account of a wide range of EU policies in the area of internal security that have been adopted or launched since the entry into force of the 2016 Europol Regulation.

14. Impact on the public

The public will directly and indirectly benefit from lower crime rates, reduced economic damages, and less security related costs. Law enforcement cooperation at EU-level through Europol does not replace different national policies on internal security and does not substitute the work of national law enforcement authorities. Differences in the legal systems and traditions of the Member States, as acknowledged by the Treaties, will remain unaffected by this EU level support.

15. Have any consultations with Stakeholders taken place or are there any plans to do so?
N/A

16. Are there any subsidiarity issues for Ireland?
None identified.

17. Anticipated negotiating period
Negotiations will commence under the current Presidency (Portugal).

18. Proposed implementation date
Budgetary projections indicate an expectation that implementation will occur by 2022.

19. Consequences for national legislation
None identified to date.

20. Method of Transposition into Irish law
This is a proposal for a Regulation. Given that Europol's mandate is set out in Regulation (EU) 2016/794, the strengthening of Europol's mandate must take the form of a Regulation. Regulations have direct legal application and do not need to be transposed into domestic law.

21. Anticipated Transposition date
N/A.

22. Consequences for the EU budget in Euros annually

The proposal is estimated to impact the annual EU contribution to Europol as set out in the table below. In the absence of a voted Multiannual Financial Framework 2021-2027 and Budget 2021, the estimate includes only the resources needed in addition to Europol's baseline EU contribution.

Total appropriations for Europol	*2022*	*2023*	*2024*	*2025*	*2026*	*2027*	*Total*
EUR million (to three decimal places)	*15,987*	*23,946*	*29,427*	*30,965*	*40,019*	*37,524*	*177,867*

23. Contact name, telephone number and e-mail address of official in Department with primary responsibility

Ms. Eileen Leahy, Principal Officer, Economic, Transnational and Organised Crime Policy, exleahy@justice.ie, Telephone 01 602 8327

Date: 11 January 2021