Council of the European Union

Brussels, 26 June 2026
(OR. en)

11158/26

Interinstitutional File:
2026/0165 (COD)

ENFOPOL 242
CRIMORG 141
SIRIS 12
COPEN 246
IXIM 147
MIGR 180
SCHENGEN 17
FRONT 125
CODEC 1319
IA 186
JAI 912
CADREFIN 314
CT 86
HYBRID 85

PROPOSAL

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	25 June 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2026) 580 final
Subject:	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) 2018/1726 and Regulation (EU) 2024/982, and repealing Regulation (EU) 2016/794

Delegations will find attached document COM(2026) 580 final.

Encl.: COM(2026) 580 final

EUROPEAN
COMMISSION

Brussels, 24.6.2026
COM(2026) 580 final

2026/0165 (COD)

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) 2018/1726 and Regulation (EU) 2024/982, and repealing Regulation (EU) 2016/794

{SEC(2026) 580 final} - {SWD(2026) 580 final} - {SWD(2026) 581 final} - {SWD(2026) 582 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

The European Union (EU) is facing a profound transformation in its security environment, as serious and organised crime and terrorism grow more transnational, technologically advanced, and interconnected. Criminal networks operate through flexible cross-border ecosystems that combine digital infrastructures, illicit financial flows, logistical networks and online services. Criminal activities are now often designed, coordinated and scaled transnationally from the start, effectively making crime a cross-border issue by default.

Rapid technological advances have accelerated this shift. Encrypted communications, automation tools and cryptocurrencies are no longer simply enablers of criminal activity but core operational assets of modern criminal networks. Combined with digital platforms and online infrastructures, they allow criminals to coordinate operations in real time, scale illicit activities with unprecedented speed, conceal financial flows, rapidly adapt operational models and exploit weaknesses across jurisdictions. At the same time, the boundaries between cybercrime, financial crime and other forms of serious and organised crime are increasingly blurring.

The current threat landscape is further aggravated by the rise of hybrid threats, including cyberattacks, attacks against critical infrastructure, and the instrumentalisation of migration or economic dependencies by hostile state and non-state actors. Such activities increasingly intersect with serious and organised crime networks, creating complex and multidimensional security risks that challenge the distinction between internal and external security.

As highlighted by the European Council in its conclusions of 26-27 June 2025 ([1]), these threats represent a major challenge to the security of Member States and Europeans. Their impact extends beyond immediate security risks, contributing to a growing sense of uncertainty and affecting citizens' trust in the public authorities' ability to ensure a high level of internal security. At the same time, serious and organised crime increasingly penetrates and distorts the legal economy, including through corruption, money laundering and the misuse of legitimate business structures, thereby weakening fair competition and undermining the integrity of markets and public institutions.

In the current security environment, the EU and its Member States have significantly strengthened cooperation and developed critical capabilities to support cross-border law enforcement action ([2]). However, the EU's response has yet to fully match the speed and adaptability of modern criminal activity.

First, the European law enforcement architecture has not sufficiently adapted to the significant increase in the volume, complexity and speed of information relevant to criminal investigations. Information on criminal activities remains fragmented across authorities, jurisdictions and systems and is not properly shared, connected or analysed in an effective and timely manner. This has progressively magnified critical blind spots in the EU's criminal

---

[1] See the conclusions of the European Council of 26-27 June 2025 on the fight against serious and organised crime.

[2] See Section 2.1 on the Consistency with existing policy provisions in the policy area.

intelligence picture and reduced the capacity to identify cross-border criminal links, support investigations effectively at European level and detect emerging threats.

Second, the EU's operational response remains fragmented. In the Schengen area without internal frontiers, where criminal networks operate seamlessly across jurisdictions, law enforcement action remains too often organised primarily along national lines. National authorities often only have partial visibility over criminal networks operating across several Member States and face persistent difficulties in coordinating investigations across borders. As a result, fragmentation remains one of the principal weaknesses of the European security response, reducing the effectiveness and efficiency of national law enforcement action against threats that are inherently transnational and require a stronger collective European approach.

Under this framework, Europol plays a central role as the EU's agency for law enforcement cooperation ([3]). Since its establishment, Europol has evolved from a support platform into a key analytical and operational hub supporting Member States in preventing and combating serious and organised crime and terrorism. Through its unique ability to connect information, generate EU-level criminal intelligence and support coordinated cross-border operations, Europol enables Member States to detect complex criminal networks, identify links across jurisdictions and respond more effectively to rapidly evolving security threats.

President von der Leyen's 2024-2029 Political Guidelines ([4]) announced the aim to further strengthen Europol. This includes a new legislative framework to boost Europol's operational role and support more effective cross-border law enforcement cooperation. This objective is further anchored in ProtectEU – a European internal security strategy ([5]), which defines a step change in how the EU organises its collective response to increasingly complex and interconnected security threats. Achieving this vision requires a comprehensive review of the Europol framework that goes beyond targeted amendments, ensuring Europol's mandate is fully aligned with the operational realities across all areas of serious and organised crime and terrorism.

The need to strengthen EU-level law enforcement cooperation has been consistently underscored by Member States and the European Parliament, particularly during the broad stakeholder consultations conducted in 2025 and 2026. European Police Chiefs ([6]) highlighted the benefits of a more robust and operational Europol, capable of serving as a genuine European force multiplier. Furthermore, evidence from the evaluation of the Europol framework and the Commission report pursuant to Article 68(3) of the Europol Regulation indicated that Europol's current mandate and operational model are no longer fully aligned with the scale and complexity of the evolving security environment. Existing limitations in the availability, integration and processing of information, as well as constraints affecting the depth of Europol's operational engagement, reduces its capacity to support Member States effectively in responding to increasingly interconnected cross-border threats.

The evaluation also highlights a growing structural imbalance between the scale and technological sophistication of criminal networks and the collective capabilities available to

---

[3] 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.

[4] Europe's Choice – Political Guidelines for the next European Commission 2024–2029, July 2024.

[5] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *ProtectEU – a European Internal Security Strategy*, COM(2025) 148 final, 1 April 2025.

[6] Statement from the European Police Chiefs, 29 April 2025.

EU law enforcement authorities. Criminal actors increasingly leverage artificial intelligence, large-scale data exploitation and sophisticated digital infrastructures that no Member State can efficiently match alone. Yet Europol's current mandate and capabilities do not allow it to fully act as the EU-level capability hub needed to reduce fragmentation, pool resources and provide Member States with the advanced operational and technological support needed to respond to the evolving threat environment.

The 2022 reform of Europol's legal framework ([7]) marked an important step in strengthening the Agency's mandate, in particular by enabling the processing of large and complex datasets and reinforcing its analytical capacities. However, the threat landscape and operational demands of Member States have evolved faster than anticipated. The large-scale processing of data, the early operational involvement of Europol in complex cross-border investigations and the provision of advanced technological support are no longer exceptional requirements but have become core features of modern law enforcement cooperation. In 2025, the European Parliament and the Council adopted a targeted amendment to the Europol framework to address specific operational needs. However, it did not tackle the underlying structural challenge: ensuring Europol can operate with the scale, agility, and integration needed to underpin an effective EU-wide response to threats that are increasingly transnational and technologically advanced.

At the same time, the EU's broader security architecture has evolved significantly. Cooperation between Europol and other EU bodies, offices and agencies, including Eurojust ([8]), the European Public Prosecutor's Office ('the EPPO') ([9]), Frontex ([10]), OLAF ([11]) and the Anti-Money Laundering Authority ('AMLA') ([12]), has become increasingly important in ensuring an effective and coherent response to cross-border threats. However, the current framework has yet to provide sufficient operational integration to support this evolving architecture ([13]) and ensure seamless cooperation across the different stages of the security and criminal justice cycle.

This adaptation is not only necessary but also timely. The conditions are now in place to support a more transformative evolution of Europol's framework. Recent and ongoing EU initiatives, in particular the revision of the framework for information exchange between law

---

7 Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, OJ L 169, 27.6.2022, p. 1.

8 Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust).

9 Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO').

10 Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624.

11 Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF).

12 Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA).

13 Including developments arising from the Commission proposal for a Regulation of the European Parliament and of the Council establishing the European Union Customs Authority and amending Regulation (EU) No 952/2013, COM(2023) 258 final, 17.5.2023.

enforcement authorities ([14]), have laid the foundations for improving the availability, quality and timeliness of data at EU level. In parallel, broader developments across the EU security and justice architecture, including strengthened cooperation between relevant EU bodies, offices and agencies, create a better environment for integrated and coordinated action.

This proposal therefore establishes a strengthened legal framework for Europol, reflecting the evolution of cross-border criminal threats and the operational needs of Member States. It aims to strengthen Europol's role as:

- an EU information hub capable of ensuring that Member States law enforcement authorities are provided with a more complete and integrated criminal intelligence picture at EU level;
- an operational hub supporting Member States more effectively and at an earlier stage in cross-border investigations and operational activities; and
- a technology and innovation hub supporting Member States with advanced capabilities, expertise and operational tools.

To achieve these objectives, the proposal builds on the strengths of the existing framework, bringing them to a level of operational excellence, while introducing the structural changes necessary to enable a more effective European response to cross-border crime. It establishes a robust and modern legal framework that equips Europol to:

- respond to current and future security challenges;
- better support Member States in cross-border investigations; and
- strengthen the EU's capacity to deliver a coordinated, efficient and resilient response to serious and organised crime and terrorism, in full compliance with the Charter of Fundamental Rights of the European Union.
- **Consistency with existing policy provisions in the policy area**

The present package of criminal justice initiatives pursues a coherent and complementary objective: strengthening the EU's capacity to prevent, detect, investigate and prosecute serious cross-border crime in an increasingly complex security environment. By modernising the legal frameworks governing cooperation between law enforcement, judicial and other relevant authorities, the package seeks to reinforce the effectiveness, coherence and interoperability of the Union's internal security architecture.

The proposed revisions of the Europol and Eurojust Regulations constitute the core of this effort. Europol and Eurojust perform distinct yet complementary functions within the Area of Freedom, Security and Justice: while Europol supports the prevention and combating of criminal activities, Eurojust facilitates judicial cooperation and ensures effective prosecutorial and judicial follow-up. The package therefore aims to strengthen cooperation and complementarity between the two agencies, as well as with other relevant Union actors in the Justice and Home Affairs and Anti-Fraud Architecture areas, with a view to ensuring a seamless continuum between law enforcement action and judicial follow-up across all stages of the criminal justice chain.

[14] Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA.

In this context, the amendments to the European Investigation Order framework and to the data protection rules applicable in the Justice and Home Affairs domain data protection regime for EU institutions, bodies, offices and agencies ([15]), further contribute to this objective by facilitating effective cross-border cooperation, improving the conditions for information exchange and ensuring a coherent legal framework adapted to operational realities and technological developments. Taken together, the measures proposed in this package will enhance the EU's ability to respond to evolving security threats while fully respecting fundamental rights, the rule of law and the division of responsibilities between the different actors involved.

Furthermore, the proposal for the revision of the Europol Regulation is consistent with the EU's broader internal security framework, in particular ProtectEU and directly contributes to its implementation. By strengthening Europol's role as an information, operational and technology and innovation hub, the proposal supports the closing of criminal intelligence gaps, reinforces cross-border investigations and enhances the use of advanced technological capabilities at EU level.

The proposal is also consistent with recent EU policy developments in internal security, including the counter-terrorism agenda under ProtectEU ([16]), the EU crime priorities for the 2026-2029 EMPACT cycle ([17]), the 2025 EU drugs strategy ([18]) and accompanying action plan against drug trafficking ([19]), and the 2026 Commission proposal for EU-wide rules against firearms trafficking ([20]). These initiatives reflect a broader shift towards more operational, intelligence-led and capability-based EU action against serious and organised crime and terrorism. The proposal also complements the roadmap for lawful and effective access to data for law enforcement, presented by the Commission in June 2025 ([21]), which addresses key challenges related to access to digital evidence.

The proposal is also consistent with the framework for information exchange among national law enforcement authorities and between them and Europol. While recent reforms have strengthened and aligned case management systems and cross-border information exchange practices at national level, their benefits have yet to be fully achieved as regards their integration with Europol services and analytical capabilities. By ensuring that information exchanged and managed at national level can be systematically made available to Europol through its information services and tools, the proposal enables Member States to make full use of Europol services, supporting a more integrated, automated and effective use of information across the EU law enforcement community.

---

15 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.

16 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, ProtectEU: Agenda to prevent and counter terrorism, COM(2026) 101 final, 26 February 2026.

17 Council conclusions on the enhancement of EMPACT and on EU crime priorities for the next EMPACT cycle 2026–2029, approved by the Council on 13 June 2025.

18 COM(2025) 743 final, 4 December 2025.

19 COM(2025) 744 final, 4 December 2025.

20 Proposal for a Directive of the European Parliament and of the Council on combating firearms trafficking and other firearms-related offences, COM(2026) 102 final, adopted by the Commission on 26 February 2026.

21 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Roadmap for lawful and effective access to data for law enforcement, COM(2025) 349 final, 24 June 2025.

The proposal provides Europol with the mandate and tools to address, across the EU, crimes falling within the scope of Europol's competence that involve a hybrid dimension, addressing the needs set out in particular under ProtectEU, the EU preparedness strategy and the Democracy Shield. It allows Europol to use its full operational, analytical and technical toolbox to act within its powers, including serious and organised crime, terrorism and cyber-enabled crime, when such offences involve a hybrid dimension. The proposal establishes EU Centres of Operational Expertise as the model for Europol's operational approach, embedding the prevention and combating of criminal offences with a hybrid dimension as a cross-cutting priority. Criminal activities with a hybrid dimension may arise in relation to any form of crime falling within the scope of Europol's competence. The Centres are established to ensure a horizontal contribution, within their respective fields of expertise, to the prevention and combating of such criminal activities, including where they form part of, contribute to or are linked to a threat with a hybrid dimension

The proposal also strengthens complementarities with the EPPO and Eurojust in the prosecutorial and judicial phases, including by providing structural analytical support to the EPPO in the analysis of complex cross-border financial crime affecting the EU's financial interests. It also supports closer interaction with Frontex in areas where cross-border crime intersects with border management, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice ('eu-LISA')[22] in relation to the development, deployment and technical management of information management services and tools, with AMLA in relation to financial crime, and with the European Union Agency for Cybersecurity ('ENISA')[23] in relation to cybersecurity, in particular ransomware incidents.

The proposal directly contributes to the functioning of the Schengen area where free movement can only be sustained through an equally integrated and effective European security response. By reinforcing EU-level law enforcement cooperation and reducing fragmentation, the proposal helps ensure that security within the Schengen area is delivered with the same level of integration as the freedom of movement it is designed to protect. At the same time, the proposal also aims at deepening Europol's cooperation with Countries associated with the implementation, application and development of the Schengen *acquis*.

- **Consistency with other Union policies**

The proposal is consistent with the EU's broader policy objectives on technological sovereignty and secure digital infrastructure, including the European strategy for data ([24]), the Digital Decade policy programme 2030 ([25]),the strategy on an EU's cloud ([26]) and the

---

22 Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011.

23 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

24 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM(2020) 66 final, 19 February 2020.

25 Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030.

26 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, An EU Strategy for Data Centres and Cloud, COM(2024) [final].

cybersecurity ([27]) initiatives, including the new proposal on the Cloud and AI Development Act (CADA) aimed at strengthening the EU's cloud and AI ecosystem, investment and infrastructure[28]. By enabling Europol and the competent authorities of Member States to process and analyse data securely at scale and to operate in secure, trusted and scalable data-processing environments, including through the use of sovereign cloud capabilities and advanced digital infrastructures, the proposal contributes to building resilient ([29]) and autonomous European technological capacities.

The proposal also supports the EU's policies on innovation, research and competitiveness, including under Horizon Europe ([30]) and the European Innovation Agenda ([31]). By positioning Europol as a central hub for identifying emerging operational needs and shaping future law enforcement capabilities, it supports the development and uptake of advanced technologies, including through joint procurement solutions.

At the same time, the proposal remains fully aligned with the EU's data protection framework, in particular Regulation (EU) 2018/1725 on the protection of personal data by EU institutions, bodies, offices and agencies, ensuring that Europol's strengthened operational role remains anchored in a high level of fundamental rights protection.

The proposal strengthens the EU's anti-money laundering and financial crime framework, including the Anti-Money Laundering Package ([32]) and the establishment of AMLA, while reinforcing the EU's anti-fraud architecture and the protection of the EU's financial interests under Directive (EU) 2017/1371 ([33]). It provides Europol with enhanced capabilities to support complex cross-border financial investigations and to cooperate effectively with the EPPO and with OLAF's administrative and investigative work. By enabling Europol to integrate financial intelligence, analytical capacities and operational resources, the proposal allows it to identify, analyse and trace criminal financial flows and assets, including those affecting the EU budget, in turn reinforcing a systematic "follow the money" approach and ensuring a coordinated, EU-level response to financial crime. This reinforcement of Europol's role is particularly relevant in the context of the ongoing review of the anti-fraud architecture, ensuring that its capabilities are aligned with future EU-level reforms and the evolving needs of cross-border financial crime enforcement.

---

27 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

28 Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act); COM(2026) 502 final.

29 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).

30 Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation.

31 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A New European Innovation Agenda, COM(2022) 332 final, 5 July 2022.

32 Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA), and Regulation (EU) 2024/1624 and Directive (EU) 2024/1640 forming part of the Union anti-money laundering package.

33 Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law (PIF Directive).

The proposal boosts the EU's external security by allowing Europol to carry out joint processing of criminal intelligence with non-EU partner countries, improving the speed and quality of international investigations, while ensuring secure information exchange through channels such as INTERPOL. The proposal also enables Europol to deploy experts in non-EU countries to coordinate operational measures. By focusing Europol's external activities on operational objectives, the proposal maximises their added value for Member States' competent authorities while remaining complementary to the role of the European Union Agency for Law Enforcement Training ('CEPOL') in capacity building in third countries.

The proposal further contributes to the EU enlargement process by deepening operational cooperation with candidate countries and potential candidates. As key partners in addressing transnational crime, terrorism and other cross-border security threats, those countries play an important role in the wider European security architecture and need to be progressively integrated into relevant security cooperation frameworks.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

This proposal is based on Articles 87(2), point (a), and 88 of the Treaty on the Functioning of the European Union (TFEU). Article 88 provides the legal basis for the establishment and functioning of Europol and for the determination of its tasks, structure and operation. Article 87(2), point (a), TFEU provides for the adoption of measures concerning the collection, storage, processing, analysis and exchange of relevant information for the purposes of police cooperation.

• Subsidiarity (for non-exclusive competence)

The challenges addressed by this proposal are inherently cross-border and cannot be effectively tackled by Member States acting alone. The most serious and organised forms of crime are now mainly transnational in nature, with criminal networks operating seamlessly across jurisdictions and digital environments. They exploit the fragmentation of national information, operational action and capabilities. As a result, Member States only have a partial view of criminal activities and face structural limitations in connecting investigations and responding effectively to criminal activities that extend beyond their national jurisdiction.

Action at EU level is therefore more effective and necessary. The scale, speed and cross-border nature of criminal activity require a level of coordination, data aggregation and analytical capacity that cannot be achieved by Member States acting alone. By operating at EU level, Europol is able to combine information from multiple jurisdictions, identify patterns and connections that would otherwise remain undetected, and support the prioritisation and coordination of operational action across borders. In doing so, it enhances the impact of national investigations and ensures that responses to cross-border crime are not fragmented but aligned and mutually reinforcing. It also enables the development and deployment of advanced capabilities that are beyond the reach of individual Member States acting alone, which also enables economies of scale in areas where the development of capabilities is resource-intensive and requires critical mass. By centralising such capacities at EU level and making them available across Member States, the proposal avoids duplication, reduces costs and ensures a consistent and high level of effectiveness.

In a Schengen area, this collective capacity is essential to ensure that the level of law enforcement cooperation is proportionate with the level of integration achieved.

- **Proportionality**

In line with the principle of proportionality, as set out in Article 5 of the Treaty on the European Union, this proposal does not go beyond what is necessary to achieve its objectives.

The proposal introduces a more integrated framework for EU-level support to law enforcement, reflecting the scale and complexity of cross-border crime. It focuses on enabling more effective use of information, strengthening support to cross-border investigations and improving access to shared capabilities, without altering the fundamental balance of competences between the EU and its Member States. In particular, it does not confer any coercive powers on Europol, which remain the exclusive competence of Member States.

Where relevant, the proportionality of the measures is further supported by the analysis carried out in the accompanying impact assessment.

- **Choice of the instrument**

The proposal takes the form of a Regulation that repeals Regulation (EU) 2016/794 establishing Europol. Repealing and replacing the existing framework is necessary in the light of the significant evolution of Europol's mandate and activities, and the resulting need for a corresponding shift in the legal approach. The current Regulation, originally designed as a flexible and broadly framed instrument, is no longer sufficient to support Europol's growing responsibilities or the increasing complexity of its operations, including its expanded role in data processing.

The evolution of Europol's role requires a modernised and fully structured legal framework to clearly define its core responsibilities, remove ambiguities, and provide the legal certainty, predictability, and accountability necessary for it to carry out its reinforced mandate effectively. The revised legal framework needs to allow Europol to perform its enhanced functions efficiently while operating within a clear, robust, and predictable legal environment, and maintaining the operational flexibility needed to respond to evolving threats.

Recasting Regulation (EU) 2016/794 would not suffice to enable Europol's modernisation. The current Regulation does not provide the foundational structure required to integrate substantial operational, analytical, and technological changes, and incremental amendments would be inadequate to establish the coherence, legal certainty, and institutional architecture necessary for a fully modernised Europol. This proposal aims to amend and expand the provisions of Regulation (EU) 2016/794. Since the amendments to be made are substantial in number and nature, the legal act should, for the sake of clarity, be repealed.

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

- **Ex-post evaluations/fitness checks of existing legislation**

The evaluation of Regulation (EU) 2016/794, as amended by Regulation (EU) 2022/991, conducted in parallel with the impact assessment accompanying this proposal, confirms that Europol plays a central and unique role in supporting Member States in preventing and combating serious and organised crime and terrorism, particularly in cross-border investigations. Covering the period 2017-2024, the evaluation found that Europol has significantly strengthened information exchange and operational coordination at Union level.

At the same time, the evaluation highlights some structural limitations that constrain Europol's ability to fully achieve its potential. Persistent information gaps, linked to uneven data contributions by Member States and procedural constraints, limit the development of a complete criminal intelligence picture at EU level. Operational support remains inconsistent and, in some cases, lacks proper integration into national investigations. Meanwhile, cooperation with other Union bodies, offices and agencies is hindered by limitations in institutional frameworks. In addition, the evaluation points to increasing pressure on Europol's resources and capabilities, in particular in the context of more complex, digital and data-intensive forms of crime, requiring scalable technological solutions and enhanced analytical capacity.

These findings reveal a structural gap between Europol's current framework and the evolving threat landscape and underpin the need for this proposal. The detailed evaluation is presented in the accompanying staff working document.

Furthermore, the Commission report pursuant to Article 68(3) of Regulation (EU) 2016/794 ([34]) confirms that Europol has made substantial progress in implementing Regulation (EU) 2022/991. Europol has implemented nearly all of its new data-processing and analytical tasks, including handling large and complex datasets and supporting research and innovation projects through specific frameworks. Europol's expanded capabilities have strengthened cross-border investigations, improved information exchange among Member States, and enhanced analytical support for serious and organised crime and terrorism, all without evidence of negative impacts on fundamental rights due to the safeguards in place. Member States continue to actively engage with Europol's new tools, reflecting a growing operational reliance on its capabilities.

At the same time, the evaluation identifies some structural and operational limitations that constrain the full use of Europol's new capabilities. Complex data protection processes slow down operational uptake and discourage consistent use of the tools in day-to-day investigations. Operational support is unevenly integrated into national investigations, while constraints in analytical capacity and technological scalability limit Europol's ability to process and act on increasing volumes of complex data. The report also notes that the growing scale and sophistication of digital and cross-border crime require more advanced, flexible, and scalable operational solutions to ensure that Europol can respond effectively across Member States.

- **Stakeholder consultations**

A thorough and comprehensive consultation process was carried out to gather input from Member States, Europol, EU agencies, law enforcement networks, and private parties (companies and business associations, as well as non-governmental, civil society and research organisations).

Initial scoping discussions between April and June 2025 involved high-level exchanges with the Standing Committee on Operational Cooperation on Internal Security (COSI), the Europol Management Board, and national police chiefs. These discussions helped identify operational priorities, challenges in cross-border cooperation, and political boundaries that would need to guide the reform of Europol's framework. These were followed by in-depth evidence gathering between July 2025 and February 2026 through a call for evidence, a public consultation and thematic workshops with Member States' experts.

[34] COM(2025) 752 final.

Overall, stakeholders expressed strong support for Europol's added value, particularly in facilitating cross-border information exchange, criminal intelligence analysis and operational coordination. At the same time, they identified important operational shortcomings limiting its effectiveness, in particular legal and procedural constraints related to data processing. Stakeholders also emphasised the need to strengthen Europol's operational support, develop more automated and interoperable systems, and boost technological and analytical capabilities, including through EU-level digital tools and stronger cooperation with EU bodies, offices and agencies. Private-sector stakeholders further underlined the importance of legal certainty in data sharing, particularly in cybercrime.

Consultations also highlighted the importance of ensuring that any strengthening of Europol's role remains fully consistent with fundamental rights, in particular data protection requirements, and respects Member States' responsibilities for national security and law enforcement. Diverging views emerged on a possible further expansion of Europol's competence in relation to hybrid threats, which several stakeholders considered politically sensitive but in principle well covered in Europol's legal framework.

The input received from the stakeholders directly informed the design of the proposal by confirming the need to address information gaps, operational fragmentation and technological capability constraints. It also guided the development of measures to strengthen data exchange, simplify procedures and boost cooperation, while ensuring appropriate safeguards and respecting the limits of Europol's mandate under the Treaty on the Functioning of the European Union.

- **Collection and use of expertise**

The Commission relied on external expertise to support both the evaluation and the impact assessment accompanying this proposal. In particular, an external study carried out between July 2025 and June 2026 provided a comprehensive evidence base drawing on input from Member States, EU bodies, offices and agencies, law enforcement networks and relevant stakeholders. Moreover, the Commission has considered a broad range of contributions, including policy papers submitted during the preparation of this proposal.

- **Impact assessment**

This proposal is supported by an impact assessment, which analysed a range of policy options to address the identified problems related to information gaps, operational fragmentation, and capability constraints.

The impact assessment focused on the issues presenting the most significant political, operational, and fundamental rights implications. Therefore, areas where broad support already existed, including capability and technology development were not covered by the assessment.

Two main policy approaches were considered.

The first approach focused on targeted improvements to the existing operational model by strengthening data availability, boosting cooperation with EU bodies, offices and agencies, and improving the integration of Europol tools and information systems into national investigative workflows. This included measures such as connections with national case management systems and more systematic consultation of Europol systems in relevant investigations.

The second approach envisaged a more structural evolution of Europol's operational model. It aimed to move beyond a framework centred mainly on bilateral information transmission towards the development of shared EU-level communication infrastructures, in particular the EU Police Shared Data Space. It also provided for a more integrated form of operational support embedded directly within national investigative environments, including through the establishment of Europol Support Offices in Member States. In addition, the approach included a substantial modernisation of Europol's data-processing framework and reinforced cooperation with the EPPO.

On this basis, the preferred policy option combines elements of both approaches. It builds on the incremental improvements identified under the first approach, in particular on strengthening data availability, upgrading systems and embedding Europol tools into national investigations. At the same time, it goes beyond the existing model where necessary to address structural limitations by enabling authorised access to national data, reinforcing Europol's operational presence in Member States, and strengthening its cooperation with the EPPO. These measures are designed to be mutually reinforcing. In particular, the incremental improvements under the first approach create the conditions for the more advanced measures to operate effectively.

The preferred policy option is expected to significantly improve the effectiveness of cross-border law enforcement cooperation by reducing information fragmentation, accelerating the identification of operational links across investigations, and strengthening operational coordination between EU bodies, offices and agencies. It is also expected to improve the capacity of national authorities to investigate increasingly digital, cross-border, and data-intensive forms of crime through enhanced analytical support, shared technological capabilities, and more integrated operational support structures. Citizens are expected to benefit through strengthened internal security and more effective prevention and combating of serious and organised crime and terrorism.

The preferred policy option requires significant investments at both EU and Member State level, in particular for the development of shared technological infrastructures, interoperability solutions, operational integration measures, and enhanced analytical and operational capabilities. Estimated one-off costs amount to approximately EUR 255 million for Member States and EUR 240 million for Europol, while annual recurring costs are estimated at approximately EUR 48 million for Member States and EUR 78 million for Europol. Total estimated costs over the 2028-2034 period amount to around EUR 590 million for Member States and EUR 789 million for Europol. At the same time, the use of shared EU-level infrastructures and capabilities is expected to generate considerable efficiencies and economies of scale, including estimated savings of approximately EUR 42 million compared to separate implementation approaches.

The interference with the rights to privacy and protection of personal data arising from the preferred policy option remains both necessary and proportionate. This is justified in the light of its objective: ensuring the effective prevention and combating of serious and organised crime and terrorism in an increasingly digital and cross-border operational landscape. The impact assessment concluded that the current data processing framework no longer reflects the operational realities of modern criminal intelligence and creates structural limitations affecting Europol's ability to support Member States effectively. At the same time, the proposal substantially strengthens and restructures the safeguards framework applicable to Europol's processing activities. In particular, it introduces a more detailed legal and technical framework governing Europol's data environments, processing regimes, access conditions,

separation of processing environments, logging and traceability requirements, storage periods, and supervisory and oversight mechanism.

The impact assessment received a positive opinion from the Commission's independent Regulatory Scrutiny Board on 17 April 2026. The summary sheet of the impact assessment is available at the following link: Executive summary of the Impact assessment - Migration and Home Affairs.

The RSB requested improvements to the impact assessment regarding the policy context, evidence base, intervention logic, impact analysis, and monitoring framework. In response, the impact assessment was revised to better explain the evolution of Europol's mandate and the wider EU security framework, strengthen the evidence base through evaluation findings and operational data, refine the objectives and policy options, deepen the assessment of impacts and safeguards, and reinforce the monitoring and evaluation framework through clearer objectives and indicators.

- **Regulatory fitness and simplification**

The proposal delivers a major simplification of Europol's data-processing rules and related procedures, directly addressing inefficiencies in the current framework. Today, most datasets received by Europol are unstructured, and implementing the existing data categorisation rules and derogations is highly complex and resource intensive. The proposal aligns these rules with Regulation (EU) 2018/1725, eliminating unnecessary complexity that were unique to Europol, while maintaining high data protection standards through this alignment.

Similarly, the prior consultation procedures, which currently can delay operational deployment of new capabilities. The proposal simplifies these procedures, removing procedural bottlenecks and accelerating implementation, while freeing up significant operational resources. Collectively, these changes reduce administrative workload and hence the associated human and financial resources needed for governance.

The proposal also introduces automated and structured data-sharing mechanisms between Member States and Europol and facilitates the integration of Europol tools into national workflows. This approach significantly reduces the administrative burden on Member States, eliminates the need for manual handling of data, accelerates the exchange of criminal intelligence, and allows Member State authorities to focus on core law enforcement tasks rather than administrative processes.

The proposal is also consistent with the Digital Check, as it supports the digital transformation of law enforcement cooperation through interoperable systems, automated data exchange and secure digital infrastructures adapted to the increasingly digital nature of crime.

- **Fundamental rights**

As the proposal involves the processing and exchange of personal data for law enforcement purposes, particular attention has been given to observing the principles, rights and freedoms recognised in the Charter of Fundamental Rights of the European Union, in particular the right to respect for private and family life (Article 7) and the right to the protection of personal data (Article 8), as well as ensuring compliance with the EU's data protection framework, including Regulation (EU) 2018/1725.

The proposal does not introduce new categories of personal data or new processing purposes. Instead, it simplifies the requirements under which lawfully obtained data may be processed

by aligning the rules on data subject categorisation under Europol's legal framework with Regulation (EU) 2018/1725. Europol remains required to distinguish between categories of data subjects. Where such distinction is not possible or where processing outside those categories is necessary for the performance of Europol's tasks, processing may take place subject to the conditions laid down in this Regulation and appropriate oversight, including the involvement of Europol's Data Protection Officer. The proposal preserves the core safeguards of the existing framework, including purpose limitation, necessity and proportionality requirements and independent supervision by the European Data Protection Supervisor.

While such processing may interfere with the rights guaranteed under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, that interference is justified by the objective of preventing and combating serious and organised crime and terrorism and is limited to what is necessary and proportionate for the performance of Europol's tasks. In today's criminal investigations, competent authorities increasingly collect and transmit large volumes of unstructured data originating from a variety of sources, including digital devices, communication services and online platforms. Such datasets often require complex processing and analysis before the information they contain can be organised, interpreted, structured and attributed to specific categories of data subjects. Moreover, even where data subjects can be categorised, the relevance of particular information and the existence of links between persons, investigations, criminal activities and criminal networks might require further analysis on the basis of new leads and information previously not available. The processing of such datasets is therefore necessary to enable Europol to identify relevant information, detect previously unknown connections and provide effective support to Member States in the prevention and combating of serious and organised crime and terrorism, subject to the conditions provided for in this Regulation.

4. BUDGETARY IMPLICATIONS

The proposal has budgetary implications at both EU and Member State level. At EU level, the strengthening of Europol's role as an information, operational and technology hub will require additional human, technical and financial resources estimated at approximately EUR 1.053 billion over the implementation period. These investments relate to enhanced data-processing and analytical capacities, operational support, technological capabilities and secure digital infrastructures. At the same time, and thanks to the above-mentioned simplification and reduction of administrative complexity, the proposal does not require any increase in Europol's spending for governance.

The implementation of the proposal will also entail costs for Member States, estimated at approximately EUR 590 million in payments over the first seven years, in particular for the adaptation of national systems, workflows and technical interfaces necessary to support more integrated and automated cooperation with Europol systems and tools.

The detailed financial implications of the proposal are set out in the legislative financial statement accompanying the proposal. The estimated financial and staffing implications for 2028 and beyond are provided for illustrative purposes only and do not pre-empt decisions on the next multiannual EU budget (2028-2034 multiannual financial framework). The funding sources and the extent of the EU's financial commitment beyond 2027 will depend on the outcome of the interinstitutional negotiations for the 2028-2034 multiannual financial framework. Thereafter they must be determined through the annual budgetary procedure. All appropriations and staffing allocations from 2028 onwards are therefore indicative.

5. OTHER ELEMENTS

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

The implementation of the proposal will follow reinforced governance structures in line with the common approach applicable to decentralised EU agencies, with Europol reporting regularly to the Management Board and the Joint Parliamentary Scrutiny Group. A dedicated Executive Board will assist the Management Board in overseeing the preparation and implementation of the annual and multiannual programming, and more generally in reinforcing supervision of administrative and budgetary management.

Performance, operational outcomes, and compliance with legal and data protection obligations will be monitored and evaluated using established reporting cycles and procedures, complemented where necessary to reflect the new measures. The proposal also strengthens Europol's capacity to generate more structured, automated and comparable statistical reporting at EU level, which will support more effective monitoring of the overall performance of the Regulation.

The Commission will evaluate the functioning and effectiveness of the Regulation in line with standard evaluation requirements and report on its performance.

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

Chapter I – General provisions, objectives and tasks of Europol

Chapter I establishes Europol, defines its objectives, legal status, seat and scope of competence, and sets out the core functions through which Europol supports the competent authorities of the Member States.

It also includes gender-based violence among the forms of crime falling within Europol's competence. This reflects the increasing cross-border and technology-facilitated nature of such conduct and ensures coherence with Directive (EU) 2024/1385, thereby enabling Europol to support Member States more effectively through information exchange, criminal intelligence analysis and operational cooperation.

In contrast to Regulation (EU) 2016/794, which defines Europol's tasks through an extensive and detailed list of activities, the proposed Article 4 structures Europol's competence around its principal functions and responsibilities, namely information processing and criminal intelligence, operational support, strategic and operational analysis, cooperation with Union bodies, offices and agencies, third countries and international organisations, and research and innovation activities. The detailed rules governing the exercise of those functions, including the including the applicable procedures, powers, conditions and safeguards are set out in the relevant substantive chapters.

This approach provides a more coherent, flexible, and clear legal framework. It strengthens transparency and accountability by creating a clearer structure for how Europol is expected to operate and deliver on its mandate, while at the same time preserving the operational flexibility needed for Europol to respond effectively to evolving threats and operational realities.

Chapter II – Operational cooperation

This Chapter establishes a new operational framework for Europol's activities, designed to equip it to support increasingly complex, interconnected, and multidimensional investigations through a multidisciplinary operational model. It moves Europol towards a more structured and continuous form of operational delivery, where operational coordination, criminal intelligence, specialised expertise, analytical capabilities, and operational support are organised within a coherent operational architecture rather than through isolated or case-by-case arrangements.

Article 7 structures Europol's strategic analytical support functions. Article 8 defines the operational capabilities that are required to provide continuous support to Member States, including Europol's key role in identifying operational links, detecting cross-border connections between investigations, and supporting operational coordination across Member States. Article 9 significantly reinforces Europol's role in supporting "follow the money" investigations and asset tracing as a core operational dimension of cross-border investigations. It establishes stronger cooperation mechanisms with national asset recovery offices and financial intelligence units, grants Europol better access to relevant financial and asset-tracing information and introduces the possibility for Europol to request urgent freezing measures where there is an imminent risk of dissipation of criminal assets. It establishes stronger cooperation mechanisms with national asset recovery offices and financial intelligence units, grants Europol better access to relevant financial and asset-tracing information and introduces the possibility for Europol to request urgent freezing measures to Member States where there is an imminent risk of dissipation of criminal assets. Article 11 strengthens Europol's follow-up to cross-border criminal intelligence by ensuring that proposals to launch investigations are systematically channelled to Eurojust for judicial coordination purposes. This will ensure that criminal intelligence requiring investigative follow-up can be taken forward through the appropriate judicial coordination mechanisms at EU level.

Section 2 establishes the permanent operational backbone through which Europol organises and delivers continuous specialised operational support to Member States.

Reflecting the increasingly interconnected and multidimensional nature of serious and organised crime and terrorism, Article 12 establishes the Operational and Analysis Service as Europol's central and permanent 24/7 operational coordination and criminal intelligence hub. The Service is designed to function as Europol's operational nerve centre, ensuring the continuous coordination of information exchange, criminal intelligence analysis, operational support requests, and operational follow-up across Europol's operational architecture. A core function of the Service is to identify operational links across national investigations, bring together information and expertise from different operational areas, support coherent operational responses across the Union, and ensure coherence between the different centres of specialised expertise.

Article 13 creates a common and scalable legal framework for Europol's Centres of specialised expertise as the primary specialised capability and expertise structures within Europol, bringing together criminal intelligence, operational coordination, specialised capabilities, analytical and forensic support, and operational expertise in key areas. It builds on the approach introduced by the European Parliament and the Council through Regulation (EU) 2025/2611 establishing the European Centre against Migrant Smuggling.

Articles 14 to 18 establish the operational framework for the Centres of Operational Expertise. The provisions recognise that the effective delivery of Europol's support requires the concentration of specialised expertise and capabilities in priority crime areas requiring

sustained Union-level action. The Centres constitute the principal organisational mechanism through which Europol prioritises, develops and delivers such operational support and ensures coherence across its activities. Given their central role in the performance of Europol's mandate and in the allocation of operational resources, the basic framework governing the Centres is laid down in this Regulation. Further details on the organisation and functioning of the Centres are to be laid down in implementing rules adopted by the Management Board. This will allow their operational set up to evolve alongside operational priorities and emerging threats.

These provisions also reflect that serious and organised crime increasingly presents a hybrid dimension. The provisions therefore ensure that, where criminal activities related to a crime falling within the scope of Europol's competence involve a hybrid dimension, Europol is able to support Member States through the full range of its operational capabilities. For this reason, this dimension is integrated across all Centres, recognising that criminal activities involving a hybrid dimension may arise across any of the crime areas falling within Europol's mandate and cannot be confined to a single operational domain.

Article 19 ensures that Europol's operational architecture remains capable of evolving over time through the establishment of additional Centres where emerging threats or operational needs require new permanent specialised capabilities at EU level.

Section 3 establishes the core operational cooperation instruments through which Europol supports coordinated operational action. Article 20 sets out the framework for operational task forces as a flexible operational coordination mechanism supporting priority investigations and operational actions in high-value and operationally significant cross-border cases. Article 22 establishes the framework governing Europol deployments for operational, technical, analytical, and forensic support to Member States and, where applicable, non-EU countries. Article 23 establishes the framework for Europol's role in supporting the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

The provisions codify these operational cooperation instruments within a legal framework, clarifying the specific operational purpose and added value of each structure while ensuring their complementarity. The objective is to provide sufficiently broad and flexible operational categories capable of covering most operational support and coordination needs, avoiding the continuous multiplication of *ad hoc* structures while preserving the flexibility needed to respond to evolving operational realities.

Article 21 strengthens the continuum of EU-level support for law enforcement cooperation and judicial cooperation by reinforcing Europol's participation in joint investigation teams.

Article 24 establishes specialised operational and technical expert pools composed of Member State experts to ensure the availability of highly specialised operational, analytical and technical expertise.

Section 4 strengthens the framework governing national structures for cooperation with Europol, recognising that the effectiveness of Europol's operational model ultimately depends on its integration within national law enforcement systems. To this end, Article 25 restructures and significantly expands the role of Europol national units, reinforcing their role as the main operational interface between Europol and the competent national authorities.

A central element of this proposal is the establishment, under Article 26, of Europol support offices within the Europol national units. These offices are designed to ensure the continuous

operational integration of Europol's operational, analytical, technical, and forensic capabilities directly into national investigations and operational activities. To this end, the staff deployed to the offices would support the day-to-day identification of operational needs, facilitate the mobilisation of Europol capabilities and operational instruments in ongoing investigations, assist national authorities in making operational use of Europol systems, analyses, and specialised support, and ensure continuous operational coordination and follow-up between Europol and the competent national authorities throughout the operational life cycle of investigations and operational actions. Reflecting their bridging function between EU-level and national operational environments, the offices are staffed by Europol staff with prior experience in Member State's competent authorities and operate through a dual reporting line ensuring close operational integration with both Europol and the national authorities concerned. This model promotes the continuous circulation of expertise between Europol and the Member States, enabling operational experience acquired at national level to be integrated into Europol's activities while ensuring that knowledge of Europol's capabilities, tools and working methods is subsequently transferred back into national law enforcement structures.

Chapter III – Information management

Articles 28 and 29 strengthen the framework governing Member States' provision of information to Europol. Building on the existing obligations under Regulation (EU) 2016/794 and pursuant to Directive (EU) 2023/977, it updates the framework to support more timely, structured and interoperable information exchange and introduces an annual assessment of Member States' information contributions.

Article 30 sets out Europol's role in the Schengen Information System (SIS), in particular on the operational use of supplementary information, support for information alerts and the operational follow-up to SIS hits. Article 31 sets out Europol's role in relation to the Visa Information System (VIS) and the European travel information and authorisation system (ETIAS).

Article 32 establishes the purposes of information processing activities by Europol, The provision enables Europol to process information in so far as is necessary for fulfilling its tasks and exhaustively determines the purposes for which Europol may process personal data cross-checking aimed at identifying connections or other relevant links with information related to a criminal offence in respect of which Europol is competent; strategic or thematic analysis; operational analysis, facilitating operational information exchange; supporting research and innovation activities and supporting Member States in informing the public about wanted suspects or convicted individuals.

At the same time, the provision aligns Europol's data subject categorisation regime with the approach set out in Regulation (EU) 2018/1725. This marks a fundamental shift with significant operational benefits while maintaining the necessary safeguards applicable across EU entities and also at national level. The constraints imposed by the previous regime on data subject categorisation have emerged as a key operational bottleneck, severely limiting Europol's ability to support Member States effectively. Without this change, the broader modernisation of Europol's operational and technological capabilities would remain structurally hindered.

In particular, it marks a shift from the logic of the previous regime under which Europol should in principle only process personal data falling within one of the data subject categories set out in Annex II, with the processing of personal data outside of these data subject categories as exception. Instead, Article 32 together with Annex II reflects the operational

reality of modern law enforcement where the extraction of information from large and unstructured datasets constitutes a core operational task of law enforcement authorities, and hence also of Europol in support of national authorities. Indeed, Europol operates in an information environment characterised by high volumes of heterogeneous data, which often originate from multiple sources and operational contexts. A substantial share of that information is received in an unstructured form, making categorisation with predefined data subject categories difficult or at times even impossible. Article 32 therefore provides that Europol must distinguish between categories of data subjects "where applicable and as far as possible", in line with Regulation (EU) 2018/1725.

Article 32 explicitly allows Europol to process personal data relating to persons outside the predefined categories of data subjects listed in Annex II, where such processing is necessary and proportionate for the performance of Europol's tasks. This reflects the dynamic nature of police investigations and criminal intelligence activities, where the operational relevance of certain data or their connection to criminal activities may only emerge progressively during operational analysis or through the identification of links across investigations.

Specific safeguards apply to the instances where Europol processes data outside of the categories listed in Annex II, such as obligations for Europol to immediately delete such data once the purpose of processing is fulfilled, inform the Data Protection Officer and keep such data functionally separate from 'categorised' data.

Article 33 preserves the data ownership principle as a core enabler of law enforcement cooperation facilitated by Europol's information processing activities. It ensures that the Member States, EU institutions, bodies, missions, office and agencies, third countries and international organisations providing information to Europol retain control over the purposes for which that information may be processed and over any access restrictions on that information, including as regards its use, transfer, transmission, erasure or destruction. Article 34 sets out the duty to consult or notify the owner of the information where relevant.

Section 2 establishes the legal and technical framework governing Europol's data environment and constitutes a central safeguard accompanying the changes introduced in Article 35 concerning data subject categorisation. The provisions define Europol's data environment to ensure that different processing activities are carried out within clearly regulated technical and operational frameworks accompanied by appropriate safeguards and access conditions.

It sets out clear and precise rules on the functioning of a number of Europol's core services and tools. This includes Europol's cross-matching service (Articles 36-39) for Member States' competent authorities to upload, query and access data against Europol's analytical environment (Articles 40-41) to store, analyse and process data to fulfil its analytical tasks, the Police Shared Data Space (Articles 42-45), where Member States' competent authorities can open and perform joint operational analysis, in cooperation with Europol. It also sets out rules on the Secure Information Exchange Network Application (SIENA – Article 46) and of the information exchange mechanism aimed to facilitate communication with private parties (Article 47). Europol's role in the European Police Record Index System is also set out (Article 48) as well as the possibility for the Commission to adopt implementing acts to regulate additional functionalities or services and tools to be developed by Europol.

Section 3 sets out the rules required for the operation of Europol's services and tools. This includes rules on a cloud infrastructure (Article 50) to support the storage, processing, analysis and exchange of data, in an efficient and scalable fashion, for the purposes set out in this Regulation, as well as on the minimum requirements for police officers to access such data, by means of an EU Police Digital Identity (Article 51). It also includes requirements on

the reporting of statistical information for oversight and accountability purposes (Article 52) and sets out Europol's role in relation to the Universal message format (UMF – Article 53) and of an EU DNA matching application (Article 54).

Chapter IV – Technological capabilities and innovation

Chapter IV is structured along the innovation and capability development life cycle framework.

The objective is to avoid fragmented or isolated innovation activities by creating continuity between technological foresight, capability planning, research and innovation, development of advanced capabilities, operational testing, deployment, operational uptake, and specialised operational support.

Chapter IV is based on the recognition that the technological transformation of internal security increasingly requires capabilities, infrastructure, expertise, computing environments, data-processing capacities, and innovation ecosystems whose scale, complexity, and cost can no longer be efficiently developed at national level alone. Europol is uniquely positioned to support this role given its ability to identify common technological and operational needs, and its capacity to develop interoperable, scalable, and shared technological solutions capable of supporting law enforcement authorities across the EU. The objective is therefore to avoid technological fragmentation, duplication of investments, and diverging capability levels between Member States in areas where common EU-level technological capabilities provide clear operational and financial benefits.

Article 57 establishes the strategic foresight and capability planning layer under the establishment of a framework mechanism to identify operational capability gaps, emerging technologies, and future capability priorities at EU level. The provision is designed to support a more strategic and coordinated approach to technological capability development, including in areas such as interoperability, standardisation, capability sharing, and joint procurement.

Article 58 clarifies Europol's role in relation to Union funding programmes by enabling Europol to assist the Commission in the programming of the Union Framework Programme for Research and Innovation and participate in capability-development activities funded through the European Competitiveness Fund, while ensuring appropriate safeguards to prevent conflicts of interest.

Article 59 provides a legal basis for Europol to develop, host, operate, and provide shared advanced technological capabilities for law enforcement. This includes AI-enabled applications, secure information-processing environments, forensic capabilities, cloud-based collaborative environments, and capabilities supporting the processing and analysis of lawfully obtained encrypted data. It also introduces a mechanism enabling a number of Member States to request Europol to develop common EU-level capabilities where shared technological solutions provide operational benefits.

Article 60 establishes the research and innovation layer by providing Europol with a comprehensive legal basis to carry out and participate in research and innovation activities. This includes pilot projects, artificial intelligence-related activities, operational experimentation, and participation in regulatory sandboxes for artificial intelligence systems.

Article 61 establishes the legal and technical framework enabling Europol to develop, test and validate artificial intelligence systems and models in a secure environment, including through

the use of AI regulatory sandboxes[35] and dedicated safeguards ensuring compliance with Union law.

Articles 62 and 63 establish the operational capability development and deployment layer by strengthening Europol's role in supporting the operational testing, validation, deployment, scaling, and operational uptake of innovative technologies and capabilities. The objective is to ensure continuity between research activities and operational deployment across Member States.

Article 64 establishes the expertise and operational support layer ensuring that advanced technological capabilities are accompanied by specialised operational expertise and training. The provision significantly strengthens Europol's role in supporting Member States through specialised expertise, while reinforcing cooperation with the European Union Agency for Law Enforcement Training (CEPOL) in areas requiring coordinated EU-level support and specialised training.

Articles 65 to 67 establish the coordination and governance layer through the creation of a dedicated Capabilities and Innovation Service and a Capabilities and Innovation Advisory Group bringing together Member States, relevant EU bodies, and experts within a common EU innovation ecosystem for internal security.

Chapter V – Organisation of Europol

Chapter V aligns Europol's governance model with the common approach applicable to decentralised EU agencies. It updates the composition of the Management Board (Article 69) and reinforces its functions (Article 72) in order to boost its effectiveness and strengthen its strategic decision-making role.

Article 75 establishes an Executive Board to support the Management Board, in line with the two-layer governance model recommended for EU agencies. This aims to ensure more efficient oversight and preparation of decisions, while allowing the Management Board to focus on strategic matters. In the light of the significant expansion of Europol's responsibilities and the corresponding increase in resources, the Executive Board will also contribute to strengthened budgetary oversight.

Article 77 provides for the central role of the Executive Director in ensuring the overall functioning of the Agency, while reinforcing clear accountability for the effective implementation of Europol's mandate and strategic priorities.

Chapter VI – Relations with Union entities

Article 79 establishes common provisions governing Europol's cooperation with EU bodies, offices and agencies, including operational cooperation and information exchange. The provision introduces a framework for working arrangements, which requires the Commission's prior approval for working arrangements concluded with Union bodies, offices and agencies established within the framework of the TFEU.

Article 80 provides for indirect access to information held by Europol for relevant EU bodies, offices and agencies, on the basis of an automated hit/no-hit system and on the conditions of reciprocity. The provision creates a more coherent and future-proof framework for information cross-checking across EU bodies, offices and agencies, notably the anti-fraud

[35] Established pursuant to Regulation (EU) 2024/1689 (Artificial Intelligence Act).

actors, while maintaining the applicable access restrictions, data ownership principles, and data protection safeguards. It also provides for the adoption of implementing acts setting out the technical procedure, to also ensure coherent technical standards and interoperability across the broader EU anti-fraud architecture. The automation of the hit/no-hit system for data exchange substantially reduces manual follow-up, improving efficiency and operational responsiveness.

Articles 81 to 90 further structure and strengthen Europol's cooperation with key EU bodies, offices and agencies, including the EPPO, Eurojust, OLAF, AMLA, Frontex, eu-LISA, the EU Drugs Agency, the EU Agency for Fundamental Rights, the EU Customs Authority and ENISA.

Article 81 significantly strengthens Europol's relationship with the EPPO, reflecting the growing operational importance of cooperation in combating complex cross-border financial crime affecting the EU's financial interests. The provision reinforces Europol's obligations to support the EPPO investigations, including through dedicated analytical support. It also establishes a dedicated hit/no-hit mechanism enabling the EPPO to access data held by Europol related to offences falling within the EPPO's competence regardless of any restrictions on access to or use of information provided to Europol by Member States and Union institutions, bodies, offices or agencies. This dedicated mechanism reflects the particular role, status and competence of the EPPO within the Union's system for protecting the Union's financial interests and the obligations that Member States and Union institutions, bodies, offices and agencies have under Regulation (EU) 2017/1939. Therefore, a targeted derogation from the application of the restrictions indicated by providers of information to Europol is conceivable only as regards the EPPO.

Chapter VII – Relations with partners

Article 92 strengthens framework governing Europol's external engagement by ensuring that Europol's cooperation with non-EU countries and international organisations remains aligned with the EU's external policies and strategic priorities.

Article 93 establishes a specific framework for cooperation with countries associated with the implementation, application and development of the Schengen *acquis*, reflecting their particular role in the functioning and security of the Schengen area. Unlike other third countries, those countries participate in an area without controls at the internal borders and share responsibility for maintaining a high level of security throughout the Schengen area. In light of that close integration, the Article provides for the possibility of a higher degree of operational integration with Europol than is available under the general framework for cooperation with third countries. To that end, international agreements with those countries may provide, for direct access to specified Europol information exchange mechanisms, participation in certain governance structures, the posting of liaison officers and corresponding obligations relating to information sharing and financial contributions.

Article 96 updates and consolidates the framework governing Europol's cooperation with private parties. It clarifies the conditions under which Europol may receive and process personal data directly from private parties and reinforces Europol's role as a facilitator of cooperation between private parties and the competent authorities of the Member States. To ensure that information relevant for criminal investigations can be acted upon effectively, Europol is required to transmit relevant information received from private parties to the Member States concerned.

The Article provides for limitations on the transmission and transfer of personal data by Europol to private parties. Such exchanges remain subject to necessity and proportionality

requirements. Special conditions apply to transfers to private parties established outside the Union and outside countries benefiting from an adequacy decision.

The Article further clarifies the relationship between Europol's cooperation with private parties and the responsibilities of Financial Intelligence Units, ensuring that Europol's activities do not duplicate or interfere with the anti-money laundering framework established under Union law.

In addition, the Article, read together with Article 47, strengthens Europol's role as a trusted technical intermediary by allowing Member States and private parties to use Europol's infrastructure for the secure exchange of information in accordance with Union and national law. Where such exchanges concern crimes falling within Europol's competence, Europol is provided with a copy of the information exchanged in order to support its operational and analytical tasks. The Article also introduces enhanced transparency and accountability measures, including reporting obligations to the Management Board, the European Parliament, the Council, the Commission and national parliaments.

Chapter VIII – Data protection

Chapter VIII establishes the main data protection safeguards governing Europol's processing activities, while aligning the framework with Regulation (EU) 2018/1725. It provides for the framework governing sensitive data processing (Article 100), storage periods and erasure of data (Article 101), rights of data subjects including access, rectification and erasure (Articles 105 and 106) and responsibility for data protection compliance (Article 107). It further reinforces the institutional safeguards architecture through the roles for the Data Protection Officer and the Fundamental Rights Officer (Articles 109 and 110), mandatory fundamental rights training (Article 111), and enhanced supervision and cooperation mechanisms between the European Data Protection Supervisor (EDPS) and national supervisory authorities (Articles 112 and 113).

Article 102 establishes a dedicated framework governing the processing of personal data in the context of Europol's research and innovation projects. This includes activities involving artificial intelligence systems and models. The provision provides for specific safeguards relating to prior authorisation, isolated processing environments, restricted access, purpose limitation, and data protection impact assessments for certain projects, while clarifying that those requirements do not apply to the development or deployment of existing tools or capabilities where the nature, scope, and purpose of the processing remain unchanged.

On the prior consultation of the EDPS, Article 108 permits Europol, in duly justified cases of urgent operational necessity, to exceptionally begin certain processing activities without prior EDPS consultation. Such cases remain subject to prior notification of the EDPS; involvement of the Data Protection Officer; and subsequent submission of the required consultation to the EDPS.

Chapter IX – Remedies and Liability

Chapter IX establishes the framework governing remedies and liability, which is complementary to and aligned with that of Regulation (EU) 2018/1725. It sets out the procedure for the handling of complaints by the EDPS (Article 114) and general provisions on liability and the right to compensation (Article 115).

Chapter X - Joint Parliamentary Scrutiny Group

Chapter X sets out the arrangements for the joint parliamentary scrutiny of Europol by the European Parliament and national parliaments through the Joint Parliamentary Scrutiny Group. It defines the mechanisms for political oversight of Europol's activities, including

reporting obligations, access to information and the involvement of the European Data Protection Supervisor.

Chapter XI – Staff

Chapter XI sets out the rules governing Europol's staff. It provides for the application of the Staff Regulations and the Conditions of Employment of Other Servants to Europol staff and establishes the categories of staff employed by Europol. The Chapter also lays down specific provisions aimed at preserving and renewing operational expertise within Europol, including through posts reserved for personnel with experience in the competent authorities of the Member States and through the use of seconded national experts.

Chapter XII – Financial provisions

Chapter XII lays down the financial framework governing Europol's budgetary planning, financing, implementation and accountability. Article 120 establishes the principles applicable to Europol's budget and defines its sources of revenue, including the contribution from the Union budget, contributions from countries associated with the implementation, application and development of the Schengen *acquis* where provided for in the relevant international agreements, and voluntary financial contributions from Member States. It also sets out the main categories of expenditure and permits the use of multiannual budgetary commitments.

Article 121 governs the preparation, establishment and adoption of Europol's budget and establishment plan. In particular, it requires the draft statement of estimates to be prepared in a manner that ensures a clear differentiation of appropriations by sub-activity, consistent with the structure of the Single Programming Document, thereby strengthening the link between budgetary resources, operational priorities and expected outputs. The Article also defines the respective responsibilities of the Executive Director, the Management Board, the Commission, the Council and the European Parliament in the annual budgetary procedure. Article 122 entrusts the implementation of the budget to the Executive Director.

Article 123 sets out the arrangements relating to accounting, audit and discharge, including the preparation and presentation of accounts, the role of the Court of Auditors, the adoption of final accounts by the Management Board and the discharge procedure before the European Parliament, thereby ensuring compliance with the Union's financial accountability framework.

Article 124 establishes the framework governing Europol's financial rules, which are to be aligned with the Union's framework financial regulation for decentralised agencies unless operational requirements justify specific derogations approved by the Commission. In addition to providing for the award of grants, including without a call for proposals where this is justified by the nature of the beneficiaries and the operational objectives pursued, the Article enables Europol to support operational cooperation activities, including joint investigation teams, and, where necessary, to contribute to the financing of equipment and infrastructure required for law-enforcement cooperation.

Chapter XII – Miscellaneous provisions

Chapter XIII contains miscellaneous provisions governing the legal, administrative and accountability framework applicable to Europol. It lays down rules on privileges and immunities, language arrangements, transparency and public access to documents, the protection of sensitive non-classified and classified information, and the prevention and investigation of fraud affecting the Union's financial interests. The Chapter also provides for the periodic evaluation of Europol, inquiries by the European Ombudsman, and the arrangements relating to Europol's seat and headquarters.

Chapter XIV – Transitional provisions

Chapter XIV contains the transitional provisions necessary to ensure legal certainty and the uninterrupted functioning of Europol following the repeal of Regulation (EU) 2016/794. Article 133 establishes Europol as the legal successor to the agency established under Regulation (EU) 2016/79 in respect of all rights and obligations arising under national, Union and international law. It further provides that the replacement of the existing legal framework does not affect the validity of cooperation agreements and working arrangements concluded by Europol under the Europol Convention, Decision 2009/371/JHA or Regulation (EU) 2016/794. Those instruments remain in force and continue to apply until they expire or are replaced.

Article 134 sets out the arrangements governing the transition to the new Regulation. It ensures the continuity of ongoing operational activities, the continued processing of data lawfully held by Europol, and the validity of existing authorisations relating to transfers of personal data. It also preserves the legal effects of decisions, implementing measures, rules and arrangements adopted under Regulation (EU) 2016/794 pending their review, amendment, replacement or repeal under the new framework. In this context, the Management Board is required to assess the continued compatibility of existing acts with this Regulation and to take the necessary measures to adapt Europol's internal framework where appropriate.

Chapter XV –Amendments to other existing instruments

Chapter XV contains amendments to related Union instruments necessary to support the implementation of this Regulation. Article 135 provides for consequential amendment in order to strengthens the legal framework for cooperation between Europol and eu-LISA in areas of common technical and operational interest. Article 136 amends Regulation (EU) 2024/982 to enable Europol to make use of the Prüm II framework.

Chapter XVI - Final provisions

Chapter XVI lays down the arrangements governing the implementation of this Regulation. It establishes a phased approach for the operational deployment of key systems and capabilities, defines the procedures applicable to implementing and delegated acts, and provides for the repeal of Regulation (EU) 2016/794 and the continuity of references made thereto.

2026/0165 (COD)

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) 2018/1726 and Regulation (EU) 2024/982, and repealing Regulation (EU) 2016/794

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 87(2), point (a), and 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) Pursuant to Article 67(1) and (3) of the Treaty on the Functioning of the European Union (TFEU), the Union is to offer its citizens an area of freedom, security and justice in which a high level of security is ensured through measures to prevent and combat crime, racism and xenophobia, and through coordination and cooperation between police and judicial authorities and other competent authorities of the Member States.

(2) The existence of an area without internal border controls presupposes a common responsibility of the Union and the Member States to ensure a high level of internal security. Effective prevention and combating of serious crime, terrorism and other forms of crime affecting a common interest covered by a Union policy require effective cooperation, coordination and information exchange between the competent authorities of the Member States.

(3) Serious crime, terrorism and other forms of crime affecting a common interest covered by a Union policy increasingly have a cross-border dimension and are characterised by a high degree of complexity and adaptability. Such criminal activities frequently generate links that may not be apparent from a national perspective alone. To support the competent authorities of the Member States in addressing such threats effectively and to contribute to a coherent and effective response throughout the Union, enhanced support and coordination at Union level are necessary.

(4) Article 88 TFEU provides that Europol's mission is 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 affecting a common interest covered by a Union policy.

(5) Europol was initially established by the Europol Convention of 26 July 1995 and was subsequently integrated into the Union framework by Council Decision

2009/371/JHA[36]. Regulation (EU) 2016/794 of the European Parliament and of the Council[37] further strengthened Europol's role.

(6) In carrying out its mission, Europol should support the competent authorities of the Member States through information exchange, operational analysis and operational support, and other forms of assistance within the scope of its competence. Given the cross-border nature of the crimes falling within the scope of its competence and the diversity of actors involved in preventing and combating them, Europol should also facilitate the effective cooperation between the competent authorities of the Member States and, where appropriate, between those authorities and relevant Union institutions, bodies, offices and agencies, third countries, international organisations and private parties, in accordance with this Regulation.

(7) Effective support for the competent authorities of the Member States requires access to specialised expertise, capabilities and services that can be developed, maintained and made available more effectively and efficiently at Union level. Europol should therefore maintain and continuously develop such expertise, capabilities and services and make them available to the competent authorities of the Member States, thereby strengthening their ability to respond to increasingly complex, technologically sophisticated and cross-border criminal threats.

(8) The criminal threat landscape affecting the Union is continuously evolving. Certain forms of crime increasingly manifest themselves through online environments, creating new operational challenges for law enforcement authorities. Gender-based violence increasingly involves technology-facilitated forms of criminal conduct and spreads across borders. The use of information and communication technologies enables such conduct to be committed, facilitated, amplified or disseminated across jurisdictions, often involving victims, perpetrators, service providers, evidence and relevant information located in different Member States or third countries. Directive (EU) 2024/1385 of the European Parliament and of the Council[38] recognises violence against women and domestic violence as a distinct area requiring coordinated action across the Union. Such offences may therefore affect common interests covered by Union policies, including equality between women and men, the protection of victims of crime and the protection of fundamental rights. The recognition of gender-based violence as a distinct criminal phenomenon under Union law reflects the need to address those offences in a coherent manner across the Union. Effective action against gender-based violence may require the combination of information and expertise relating to different forms of criminal conduct, the identification of links between cases affecting several jurisdictions and enhanced cooperation between the competent authorities of the Member States. The list of forms of serious crime in respect of which Europol is competent should therefore include gender-based violence.

---

36 Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p. 37, ELI: http://data.europa.eu/eli/dec/2009/371/oj).

37 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, ELI: http://data.europa.eu/eli/reg/2016/794/oj).

38 Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence (OJ L, 2024/1385, 24.5.2024, ELI: http://data.europa.eu/eli/dir/2024/1385/oj).

(9) To address criminal offences related to the forms of crime falling within the scope of Europol's competence that form part of, contribute to or are linked to a threat with a hybrid dimension, Europol should make full use of the tasks, capabilities and tools provided for in this Regulation. The existence of a hybrid dimension in a crime falling within the scope of Europol's competence should not affect Europol's ability to support the competent authorities of the Member States through information exchange, operational analysis, operational cooperation and other forms of support within the scope of its competence.

(10) Europol should act in support of the competent authorities of the Member States and should not itself exercise coercive powers or carry out investigative measures. This Regulation should therefore establish clear rules concerning Europol's competence, tasks and functioning, while ensuring respect for fundamental rights, including the right to the protection of personal data.

(11) As Europol's operational support activities have expanded and diversified, it is necessary to ensure coherence, complementarity and operational continuity between the different forms of operational support provided by Europol. Europol's operational framework should therefore allow its operational tools, specialised expertise and support structures to function in an integrated and mutually reinforcing manner, while remaining sufficiently adaptable to evolving operational needs, technological developments and emerging security threats.

(12) The cross-border and interconnected nature of serious and organised crime and terrorism requires the identification of links, patterns and developments across jurisdictions and areas of criminal activity. Fragmented or incomplete criminal information may create operational blind spots that can be exploited by transnational criminal networks and terrorists. By bringing together information and criminal intelligence originating from multiple authorities and sources across the Union and beyond, Europol is uniquely placed to contribute to the development of a shared strategic analysis of criminal threats, operational developments and emerging security risks.

(13) To ensure that strategic analysis is translated into effective action, Europol's analytical products should support the identification of priorities, the allocation of resources and the planning of operational action at Union and national levels, including within the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT). They should also support the Commission and the Member States in carrying out risk assessments and verifying the implementation of the Schengen framework.

(14) The production of a common Union strategic analytical picture should be a shared responsibility of Europol, the Member States and the relevant Union institutions, bodies, missions, offices and agencies, which should provide the information necessary for the preparation of those analytical products in accordance with their respective mandates and applicable Union law. Europol should also support the development and use of common analytical methodologies and standards, in particular for Union-level threat assessments, to strengthen the comparability, consistency and interoperability of criminal intelligence analysis at Union level.

(15) Europol's strategic analyses and threat assessments should pay particular attention, where appropriate, to the Union's closest neighbourhood and, in particular, to the situation in countries that are candidate countries and potential candidates for accession to the Union. Such contributions may include assessments of those

partners' capacities to prevent and combat serious crime and terrorism. The strategic analyses and threat assessments should be further informed by contributions from EU candidate countries and potential candidates, whose own national serious and organised crime threat assessments are being developed with the support of Union-funded projects.

(16) By bringing together and analysing information and criminal intelligence originating from multiple sources, Europol may identify links that are not apparent from the perspective of a single Member State and that may require investigative action at national level. Since the responsibility for conducting criminal investigations rests with the competent authorities of the Member States, Europol should therefore be able, within the scope of its competence, to request those authorities to assess, without undue delay, the need to initiate, conduct or coordinate investigations in relation to forms of crime falling within the scope of Europol's competence. Europol should also be able to make such request where criminal activity primarily concerns a single Member State but may have implications for the Union's internal security. Criminal activities concentrated in a single Member State may nevertheless form part of wider criminal phenomena or generate risks and vulnerabilities extending beyond national borders and therefore require consideration from a broader Union perspective.

(17) Effective judicial follow up to requests made by Europol concerning the need to assess the initiation, conduct or coordination of criminal investigations may require judicial coordination and cooperation at Union level. The European Union Agency for Criminal Justice Cooperation ('Eurojust'), established by Regulation (EU) 2018/1727 of the European Parliament and of the Council[39], should therefore be informed without delay of such requests and of any follow-up decision taken by the competent authorities of the Member States. That should enable Eurojust to facilitate judicial follow-up, ensure coherence between law enforcement and prosecutorial action at Union level and exercise its tasks in accordance with that Regulation.

(18) Operational coherence across Europol's activities is essential for an integrated response to serious and organised crime, terrorism and other forms of crime falling within the scope of Europol's competence. Given the increasingly interconnected nature of criminal threats and the growing complexity of criminal activities, Europol should ensure the coordinated handling of information, criminal intelligence and operational support across its structures and areas of specialised expertise. Europol should therefore maintain a permanent Operational and Analysis Service to ensure coordination and coherence across its activities and to support Member States in delivering a multidisciplinary operational response at Union level.

(19) Several forms of crime falling within Europol's competence require dedicated expertise, operational capabilities and support that are most effectively organised and maintained at Union level. Europol should therefore maintain Union Centres of specialised expertise as part of its organisational structure in areas of particular relevance for the Union's internal security. The Centres should form an integral part of Europol's organisational structure, contributing to the performance of Europol's tasks in their respective areas of expertise. They should not have separate legal

[39] Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA (OJ L 295, 21.11.2018, p. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj).

personality. In order to ensure the continuity and stability of those core capabilities, the establishment of such Centres should be determined by this Regulation. The Management Board should be responsible for specifying the organisation, specialised functions, composition and operation of the Centres in light of operational needs and evolving security threats.

(20) Criminal activities involving a hybrid dimension may arise in relation to any form of crime falling within the scope of Europol's competence. All Centres should therefore contribute, within their respective fields of expertise, to the prevention and combating of such crimes, including where they form part of, contribute to or are linked to a threat with a hybrid dimension.

(21) As the operational landscape in which Europol operates is increasingly characterised by fluid criminal structures and the convergence of multiple crime areas, effective support for the competent authorities of the Member States requires close cooperation and coordination between the Centres and other organisational structures within Europol. The Centres should therefore work together and combine their respective expertise and capabilities where this is necessary to support multidisciplinary operational responses to cross-cutting threats. The allocation of tasks to a specific Centre under this Regulation should not preclude the involvement of other Centres or organisational structures in the performance of those tasks where operational needs so require.

(22) To address the increasingly severe threats posed by transnational serious and organised crime networks, Europol should provide, in particular through its European Serious and Organised Crime Centre, Member States with operational, analytical, technical and forensic support to combat forms of serious and organised crime such as drug trafficking, trafficking in firearms and explosives, environmental crime and property crime and in complex cross-border investigations.

(23) The terrorist threat affecting the Union continues to evolve in terms of actors, methods and means, including through the exploitation of online environments and emerging technologies. An effective counter-terrorism response requires Europol, through its European Counter Terrorism Centre, to provide Member States with operational, analytical, technical and forensic support to counter terrorist activities such as terrorist financing, online radicalisation, the dissemination of terrorist content online or physical attack prevention. Europol should also support the coordination of crisis response mechanisms at Union level.

(24) Financial and economic crime undermines the integrity of the Union's economy, financial system, and legal order and constitutes a key enabler of serious and organised crime and terrorism. The use of complex financial schemes, crypto-assets and digital financial technologies makes the detection, investigation and tracing of criminal assets increasingly challenging. It requires permanent specialised expertise and capabilities at Union level. Europol, in particular through its European Financial and Economic Crime Centre, should therefore provide Member States and relevant Union bodies, offices and agencies, such as the European Public Prosecutor's Office (EPPO), established by Council Regulation (EU) 2017/1939[40], with specialised support for financial investigations, asset tracing and recovery, crypto-assets and

[40] 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, ELI: http://data.europa.eu/eli/reg/2017/1939/oj).

digital financial technologies, and the identification and analysis of criminal financial schemes and transactions.

(25) To enable Europol to provide effective support to national asset recovery offices in assets tracing and recovery, Member States should ensure that Europol has effective access to the information necessary for the tracing and identification of property. Where, on the basis of its analytical activities, Europol identifies an imminent risk of disappearance of traced and identified property, it should be able to request the competent authorities of the Member State concerned to take immediate action.

(26) Cybercrime and cyber-enabled criminal activities constitute a central component of the threat landscape affecting the Union's internal security. The growing availability of cybercrime-as-a-service facilitates the use of sophisticated tools and services by a broad range of criminal and terrorist actors, thereby increasing the scale and impact of cyber-enabled criminal activities. Europol, in particular through its European Cybercrime Centre, should therefore support Member States in preventing and combating cybercrime, responding to cyberattacks, and addressing the growing digital dimension of criminal activities across all crime areas falling within the scope of its competence. Europol should also contribute to the development and deployment of specialised technical capabilities, in particular in the areas of digital forensics, lawful access, and the processing and analysis of encrypted data. Such capabilities require a level of expertise and resources that can be provided more effectively at Union level.

(27) Cyber incidents of suspected criminal origin, notably ransomware incidents, often require both a cybersecurity and a law enforcement response. The European Cybercrime Centre should therefore cooperate closely with the European Union Agency for Cybersecurity (ENISA), established by Regulation (EU) 2019/881 of the European Parliament and of the Council[41], in relation to cybersecurity, cyber threats and cyber incidents of suspected criminal origin, with a particular focus on ransomware incidents, including through ENISA's ransomware helpdesk. Such cooperation should support effective coordination, the exchange of information and expertise, and the development of synergies between the cybersecurity and law enforcement communities.

(28) Migrant smuggling and trafficking in human beings constitute major cross-border criminal activities that endanger human life, undermine the Union's migration and border management policies and generate significant profits for organised criminal networks. The European Centre Against Migrant Smuggling established within Europol should ensure permanent specialised expertise and capabilities at Union level to support the fight against migrant smuggling and trafficking in human beings. Europol, in particular through that Centre, should support Member States in dismantling migrant smuggling routes and criminal facilitation networks. Europol should also support the identification of victims of trafficking and other vulnerable persons, ensuring cooperation with the EU anti-trafficking coordinator referred to in Directive 2011/36/EU of the European Parliament and of the Council[42].

---

[41] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[42] Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA (OJ L 101, 15.4.2011, p. 1, ELI: http://data.europa.eu/eli/dir/2011/36/oj).

(29) Evolving crime threats and operational needs may, in exceptional circumstances, require the establishment of additional Centres dedicated to areas requiring specialised expertise or coordinated action at Union level. The Executive Director should continuously assess operational developments, capability requirements and emerging crime areas and, where appropriate, identify the need for the establishment of additional Centres. Additional Centres should only be established where a sustained operational need exists that cannot be adequately addressed through Europol's existing organisational structures. It should also be possible to adapt, merge or discontinue such additional Centres where this is necessary to reflect changing operational requirements. In order to ensure a coherent framework for the establishment of Centres, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of the establishment, adaptation, merger or discontinuation of additional Centres. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[43]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(30) In carrying out their activities, the Centres should cooperate closely with similar specialised structures established at Union level, including Eurojust's Centres of Expertise in criminal matters and the future EU Centre for the Protection of Children from Child Sexual Abuse, within their respective competences. Such cooperation should contribute to ensuring complementarity, avoiding duplication of efforts and maximising the operational value of specialised expertise and capabilities.

(31) The investigation of high-risk criminal networks and complex cross-border criminal phenomena requires structured yet flexible forms of operational cooperation between the competent authorities of the Member States. Operational task forces provide a framework for concentrating investigative efforts, operational expertise and criminal intelligence on priority targets, supported by Europol. Europol should therefore participate in operational task forces, enabling operational coordination, facilitating the exchange and analysis of information and contributing with its specialised operational, technical, analytical and forensic support. Where appropriate, operational task forces should be integrated within EMPACT activities. Where operational findings indicate the need for judicial coordination, Europol should ensure timely transmission of relevant information to Eurojust to support the effective exercise of its mandate in accordance with Regulation (EU) 2018/1727.

(32) Joint investigation teams provide a structured framework for coordinated investigations, shared operational planning and the use of evidence within a common investigative setting. Europol should therefore be able to support joint investigation teams for crimes falling within the scope of its competence by contributing criminal intelligence, analytical input and specialised operational capabilities, and by facilitating operational coordination where this strengthens joint investigative action. Where operational findings indicate the need for judicial coordination, Europol

[43] OJ L 123, 12.05.2016, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

should ensure timely transmission of relevant information to Eurojust to support the effective exercise of its mandate in accordance with Regulation (EU) 2018/1727.

(33) To provide effective operational support to the competent authorities of the Member States and, where relevant, third countries, Europol needs to make its expertise, capabilities and support available where operational activities are carried out. Europol should therefore be able to deploy staff in order to provide analytical, operational, technical and forensic support directly to the competent authorities concerned. Such deployments should notably support large-scale and complex investigations, operational coordination activities and major international events. They should also contribute to ensuring coherence between law enforcement activities and activities carried out at the Union's external borders, with each authority acting within the limits of its competence. In particular, Europol deployments should assist screening authorities in carrying out checks in accordance with Regulation (EU) 2024/1356 of the European Parliament and of the Council[44], support Frontex established by Regulation (EU) 2019/1896 of the European Parliament and of the Council[45] and migration management activities under Regulation (EU) 2019/1896, and support border management authorities in performing security checks against Europol information at the Union's external borders. The effectiveness of Europol deployments is contingent on timely and active support from the Member States. Member States should therefore ensure that staff deployed by Europol has, where relevant and appropriate, secure access to operational sites, information and technical equipment, and should facilitate coordination and integration with national operational teams.

(34) In certain situations, Europol may require the secondment of highly specialised expertise to respond to specific operational needs. Maintaining specialised operational and technical pools composed of experts designated by the Member States contributes to ensuring the availability of such expertise when needed. At the same time, the specialised knowledge and experience of those experts remain essential for the performance of the tasks of the competent authorities of the Member States. A balanced approach is therefore necessary to enable Europol to draw on that expertise for specific operational needs while preserving national operational capacities. Secondments from those pools provide an effective mechanism to achieve that objective.

(35) The value of Europol's operational support depends on its close integration with the activities of the competent authorities of the Member States. Such integration requires robust national coordination structures capable of acting as a genuine interface between Europol and competent authorities of the Member States. Europol national units play a central role in ensuring cooperation between Europol and those authorities and in facilitating the exchange of information. They should also contribute to the identification of national operational priorities and capability needs to be supported by Europol, facilitate national contributions to Europol's analytical and strategic assessments, and help ensure the effective coordination of Europol's support at national level. Liaison officers attached to Europol should play an important role in facilitating direct cooperation and coordination with the competent

---

[44] Regulation (EU) 2024/1356 of the European Parliament and of the Council of 14 May 2024 introducing the screening of third-country nationals at the external borders and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817 (OJ L, 2024/1356, 22.05.2024, ELI: http://data.europa.eu/eli/reg/2024/1356/oj).

[45] OJ L 123, 12.05.2016, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

authorities of the Member States, including through the rapid exchange of information and the identification of cross-border operational links.

(36) Europol national units should also assume a reinforced role in ensuring that EMPACT delivers its full operational potential, addressing existing coordination gaps that prevent effective linkage between Union-level priorities and national needs. To that end, Europol national units should evolve into central operational platforms hosting their national EMPACT support team, responsible for facilitating operational participation and aligning national contributions with EMPACT priorities.

(37) To effectively use Europol's operational, analytical, technical and forensic support in national investigations, that support needs to be tailored to national needs and procedures. To ensure that Europol support can be mobilised rapidly and aligned with operational needs and procedural requirements at national level, Europol support offices should be established within the Europol national unit in each Member State. These offices should facilitate the integration of criminal intelligence, analytical tools, digital and forensic technologies and operational expertise directly into ongoing national investigations. The support offices should also help ensure that operational outputs provided by Europol can be used effectively by the competent authorities of the Member States in preventing and combating serious crime and terrorism.

(38) The Europol support offices should be staffed by Europol staff that has completed a structured career pathway combining experience in the competent authorities of a Member State and subsequent service within Europol, before being seconded back to the national structure. That rotation model is essential to ensure that the expertise acquired at Europol is effectively reinvested into the national system and that the integration of Europol support is carried out by Europol staff with operational understanding of the specific legal, operational and organisational framework within which the competent authorities of the respective Member State operate. Such Europol staff should act under a dual reporting line to Europol and the Member State where the Europol support office is established. The establishment of the Europol support offices should not affect the responsibilities and powers of the competent authorities of the Member States under national law. To ensure the effectiveness of the rotation-based staffing model underpinning Europol support offices, Member States should take the necessary measures to facilitate the reintegration of staff into their national administrations upon completion of their assignment within that office. That requires the removal of administrative, organisational and career-related barriers that could hinder mobility between national authorities and Europol, thereby ensuring that such mobility is recognised as an integral part of their professional career development.

(39) To serve as the Union's criminal information hub, Europol should be able to process information that it has received from the sources or that it has directly retrieved from publicly available sources, subject to the conditions and safeguards laid down in this Regulation. The effective gathering of information from publicly available sources for Europol includes notably the use of online search engines, including the input of personal data, which should not be regarded as a transmission or transfer of personal

data to private parties under this Regulation or Regulation (EU) 2018/1725 of the European Parliament and of the Council[46].

(40) Member States should ensure the timely provision of the information necessary for Europol to fulfil its tasks, including through structured, secure and automated exchange mechanisms. In that context, Member States should establish and maintain appropriate national data loaders enabling the structured feeding of relevant information into Europol services and tools, ensuring data quality, completeness and timeliness.

(41) Europol's operational model remains firmly anchored in the data ownership principle, under which Member States, Union institutions, bodies, missions, offices and agencies, third countries and international organisations providing information to Europol retain control over the purpose and conditions of its processing. That principle is a cornerstone of mutual trust in the exchange of information with Europol and ensures that the use of data remains strictly aligned with the intent defined by the provider.

(42) In so far as is necessary for the fulfilment of its tasks, Europol should be able to process personal data, provided that such processing is carried out only for the purposes laid down in this Regulation. Regulation (EU) 2018/1725 lays down the rules on the protection of natural persons with regard to the processing of personal data by Union institutions, bodies, offices and agencies. Regulation (EU) 2018/1725 should apply to the processing of personal data by Europol, complemented by the specific rules of this Regulation.

(43) Europol operates in an information environment characterised by high volumes of heterogeneous data, which often originate from multiple sources and operational contexts. A substantial share of that information is received in an unstructured form, making categorisation with predefined data subject categories difficult or at times even impossible. That reflects the reality of modern law enforcement where the extraction of information from large and unstructured datasets constitutes a core operational task of law enforcement authorities. In that context, the data subject categorisation rules applicable to Europol should be aligned with Regulation (EU) 2018/1725. Europol should therefore make a clear distinction between personal data relating to the different categories of data subjects listed in Annex II only where applicable and as far as possible, ensuring that operational effectiveness is ensured while fully respecting data protection safeguards and principles, such as data minimisation and purpose limitation.

(44) The categorisation of personal data is a dynamic process that may change as new leads and information become available. Personal data that are initially not considered relevant for inclusion under a data subject category of Annex II may, upon further processing, acquire operational significance or reveal connections to ongoing investigations. Where it is not possible to clearly distinguish between the personal data that relate to the different categories of data subjects listed in Annex II, or where Europol has to process personal data outside of the categories of data subjects listed in Annex II, Europol should inform its Data Protection Officer. Such

[46] 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

personal data should be immediately deleted once the purpose of processing is fulfilled.

(45) The effective carrying out of Europol's tasks and the processing of information require the development and use of services and tools, which should be established and managed in a manner that ensures their effectiveness, efficiency and compliance with applicable data protection and security standards.

(46) For the purpose of processing information for cross-checking against existing data already stored and categorised by Europol in cooperation with the Member States, the establishment of a Europol cross-checking service is necessary to support Europol's objectives and tasks and to facilitate the exchange of information between Member States and other Union bodies, offices and agencies. For the effective and efficient functioning of that service, the case management systems of the competent authorities of the Member States should be interoperable and technically connected with such service. To maximise technical efficiency and ensure consistency with existing Union information systems, the Europol cross-checking service should, where technically feasible, re-use and adapt existing technologies and components developed by eu-LISA, including the technology underpinning the Shared Biometric Matching Service (sBMS), for its biometric matching functionalities. The re-use and adaptation of such technology should serve solely technical, operational and cost-efficiency objectives, including economies of scale and the avoidance of duplication of investments, and should not affect existing governance arrangements, access rights, data ownership, interoperability architectures, the allocation of responsibilities between Union bodies, offices and agencies, or the legal conditions governing access to information under Union law.

(47) The processing of personal data in the Europol cross-checking service requires the definition of a precise and exhaustive list of categories of data to ensure that the processing remains necessary and proportionate for the fulfilment of Europol's tasks and that the rights of individuals are protected in accordance with the applicable data protection rules. The data formats of such categories of data, including identifiable objects or multimedia data used for the querying of the service, should be laid out by means of an implementing act.

(48) The systematic and timely uploading of relevant data to the Europol cross-checking service by Member States and Europol is essential to ensure the effectiveness of the service and to support cross-border cooperation in the prevention and combating of serious and organised crime, while also providing for necessary safeguards to protect the essential interests of the security of the Member States and the rights of individuals. By systematically cross-checking any newly uploaded data against already stored data to identify links and connections between cases, the service enables Europol to support Member States in cross-border investigations.

(49) Systematic querying of the Europol cross-checking service by competent authorities of the Member States is necessary to ensure the effective use of the service by all relevant law enforcement actors across the Union, and thereby enhance the prevention and combating of serious crime and terrorism, while also ensuring that access to the data remains subject to strict conditions and safeguards to protect the rights of individuals and respect the data ownership principle.

(50) For Europol to effectively support cross-border investigations and operational activities, it is necessary to establish a Europol Analytical Environment as a secure technical and operational platform for the storage, processing, analysis and

visualisation of data. The Europol Analytical Environment should support the fulfilment of Europol's tasks by facilitating the operational analysis of data received by Member States, third countries, international organisations, private parties or other sources in accordance with this Regulation.

(51) To ensure that the rights of individuals are protected, the querying of and access to Europol Analytical Environment data, including data stored as part of analysis projects, should be subject to strict access conditions and data protection safeguards, while also enabling authorised entities to effectively query and have indirect access to the data to contribute to the prevention and combating of serious crime and terrorism.

(52) To support Member States in carrying out joint operational analysis, the Police Shared Data Space should leverage the capabilities of the Europol Analytical Environment. This includes, where appropriate, advanced analytical tools and modules, such as those enabling the processing and comparison of biometric data, and functionalities supporting the collection and analysis of data from publicly available sources. The availability of such capabilities within the Police Shared Data Space should enhance the detection of links between cases and facilitate coordinated operational responses.

(53) In order to facilitate real-time operational cooperation between competent authorities of different Member States and Europol, the Police Shared Data Space should enable the establishment of Joint Operational Analysis Cases (JOAC). A JOAC should constitute a secure collaborative environment in which participating authorities and Europol can jointly process, analyse, enrich and exchange information relating to a specific criminal investigation, threat, criminal network or operational objective. The creation of JOACs should be subject to clear criteria and procedures, including the designation of participating authorities and the conditions governing access to and use of the information processed therein.

(54) To enhance the effectiveness of joint operational analysis, Europol should be able to propose the establishment of a JOAC to Member States, based on its analysis of available information and data, while respecting the discretion of Member States to decide on the opening of a JOAC.

(55) To enable participants to a JOAC to effectively collaborate and analyse data, exchange information and conduct joint activities, while granting the possibility to use Europol relevant capabilities, a set of advanced features, including secure communication tools such as chat and video conferencing, and collaborative document editing and visualisation capabilities, should be provided within the Police Shared Data Space as means to facilitate effective and efficient cooperation and analysis among participants and to support the exchange of information and expertise in a secure and controlled environment.

(56) Given the increasingly transnational nature of crime, it should be possible, in duly justified cases, for the Member State opening a JOAC to propose the participation of third country. Such participation should remain limited to third countries having an agreement enabling the exchange of personal data with Europol and to situations where Europol considers that the involvement of the third country concerned is relevant for achieving the objectives of the JOAC. Participation by a third country should not lead to generalised access to Europol services and tools, but should be limited only to the specific JOAC and the information made available therein in accordance with this Regulation.

(57) To facilitate the seamless exchange of information between the single points of contact and competent authorities of Member States, Europol and other authorised entities, Europol should provide a secure and reliable tool, such as the Secure Information Exchange Network Application (SIENA), with web interfaces, mobile applications and dedicated programming interfaces.

(58) To streamline the cooperation between private parties, Member States and Europol in preventing and responding to online crisis situations, cybersecurity threats, and other criminal activities exploiting digital services, Europol should establish a dedicated mechanism within the Europol Analytical Environment. That mechanism should, in particular, support compliance with Union reporting and notification obligations under Regulations (EU) 2021/784[47] and (EU) 2022/2065[48] of the European Parliament and of the Council by both private parties, such as hosting service providers, and competent law enforcement or judicial authorities of the Member States and enable rapid coordination during online crisis situations. It should be designed to facilitate the determination of the Member State to be notified and ensure interoperability with national systems while maintaining robust security and data protection safeguards. Europol should ensure that the development and maintenance of the mechanism is supported by the necessary resources.

(59) To support the objectives of Regulation (EU) 2024/982 of the European Parliament and of the Council[49], Europol should perform the tasks conferred on it in relation to the European Police Record Index System (EPRIS), providing a centralised platform for the indexing and sharing of police records, and enabling law enforcement authorities to access and exchange information efficiently and effectively.

(60) To support the effective achievement of its objectives and to enhance the cooperation between Europol, competent authorities of the Member States and other authorised entities, Europol should establish a secure, scalable and sovereign Europol cloud infrastructure, hosting the Police Shared Data Space and enabling the storage, processing, analysis and exchange of data, while ensuring strict access control, data compartmentalisation and full compliance with Union law, and allowing for the development, operation and maintenance of a range of digital services and operational data-processing capabilities.

(61) To facilitate secure, efficient and trusted access to the Police Shared Data Space for a wide range of investigators across the Union, an EU Police Digital Identity should be established, enabling representatives of competent authorities of the Member States, Europol and other authorised entities to access the Europol infrastructure and connected national systems in a harmonised and secure manner, while ensuring accountability and oversight through logging and auditing mechanisms, and allowing for differentiated access rights based on specific needs and requirements.

---

47 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (OJ L 172, 17.5.2021, p. 79, http://data.europa.eu/eli/reg/2021/784/oj).

48 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj).

49 Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation) (OJ L, 2024/982, 05.04.2024, ELI: http://data.europa.eu/eli/reg/2024/982/oj).

(62) To ensure effective monitoring, evaluation and oversight of Europol's services and tools, Europol should develop and maintain statistics and reporting tools capable of generating statistical information, indicators and analytical reports concerning their use, performance, operational effectiveness and interoperability. Those tools should support the preparation of strategic and operational analyses, threat assessments, trend reports and situational briefings, and contribute to the annual reporting obligations of Europol and to the Commission's evaluation reports, in particular regarding the operational impact of this Regulation. They should also facilitate the availability of reliable information for evaluation, monitoring and reporting purposes and, where appropriate, support the Commission in carrying out its responsibilities under Union law, including the monitoring, implementation and evaluation of legislation relevant to Europol's mandate. They should also facilitate the provision of information to the Joint Parliamentary Scrutiny Group (JPSG). The statistics and reporting tools should enable the analysis of trends, operational needs and information exchange activities, while ensuring that statistical information is processed in compliance with Union law on data protection, cybersecurity and confidentiality. Such information should be subject to appropriate safeguards and access control measures. To ensure that the report to be submitted each year by the Commission pursuant to Article 325(5) TFEU includes a comprehensive overview of the measures taken to counter fraud affecting the Union's financial interests, Europol should contribute to the preparation of that report. That contribution should cover the results achieved and the activities carried out to that end by Europol.

(63) To facilitate the efficient and interoperable exchange of information between Member States, Union bodies, offices or agencies and other relevant entities, Europol should support the development, implementation and operational use of the universal message format established Regulation (EU) 2019/818 of the European Parliament and of the Council[50] by providing the secretariat and steering technical and operational discussions. To that end, Europol should cooperate closely with the Commission to support the consistent application of the UMF across relevant information systems and communication channels, thereby enhancing interoperability and the effectiveness of information sharing.

(64) The comparison of DNA profiles requires specialised matching tools that are distinct from the information systems through which DNA data are exchanged. Europol should therefore be able to provide a common DNA matching application serving as a technical and forensic component for the automated comparison of DNA profiles. The application should function as a shared technical capability that can be deployed within Europol services and tools or by Member States. It should support the implementation of information exchange frameworks, including Regulation (EU) 2024/982, while respecting the ownership of data by the authorities providing them and the safeguards governing their processing and exchange. The availability of a common EU DNA matching tool is also important to strengthen Europe's technological sovereignty in a critical area of law enforcement and forensic cooperation, reduce dependency on external technologies and providers, and ensure that the development, operation and evolution of DNA matching functionalities remain subject to Union standards, governance and security requirements.

[50] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj).

(65) To ensure that Europol remains equipped to effectively respond to evolving operational, technical and analytical needs, and to support the effective achievement of its objectives, Europol should be able to design, develop and manage additional services and tools, while ensuring that such systems and tools comply with the applicable data protection rules and safeguards and are subject to appropriate procedural and technical requirements. The Commission should be empowered to adopt implementing acts laying out such procedural and technical requirements.

(66) To ensure the effective development and implementation of Europol's information systems and ICT infrastructure, an ICT and Information Management Steering Group should be established as a sub-structure of the Management Board to provide strategic guidance, expertise and oversight on ICT and information management activities and to support the Management Board in taking informed decisions on those matters, while ensuring consistency with Member States' operational needs and Union-wide interoperability objectives.

(67) To provide specialised technical expertise and advice to support the development and implementation of Europol's information systems and ICT infrastructure, an ICT and Information Management Advisory Group should be established to assist the Steering Group and Europol in designing, developing and operating information systems, communication infrastructure and information exchange mechanisms, and to promote common technical components, standards and best practices, while ensuring close coordination and cooperation between Europol, eu-LISA, Member States and the Commission on technical and implementation-related matters.

(68) To achieve a more coordinated approach to anticipating and addressing operational and technological needs of law enforcement authorities across the Union, Europol should establish a Foresight and Common Capability Development Framework ('the Framework') aimed at developing a common understanding of short-, medium- and long-term capability priorities. The Framework should contribute to the more efficient pooling, sharing and use of resources, promote interoperability and standardisation and help avoid duplication of investments.

(69) To ensure continuity between the identification of capability priorities under the Framework, the development of innovative solutions for advanced capabilities and their deployment in operational law enforcement environments, Europol should be able to assist the Commission in the programming of the Union Framework programme for Research and Innovation, and participate in capability-development activities supported under Union funding programmes, notably the European Competitiveness Fund, where necessary for the fulfilment of its tasks. As Europol may perform different functions in relation to Union funding programmes, the Commission and Europol should ensure that Europol's participation in activities supported under Union funding programmes does not confer any undue advantage resulting from its involvement in the programming of those programmes.

(70) Certain technological, analytical and forensic capabilities are increasingly complex and resource-intensive, making it inefficient for Member States to develop and maintain such capabilities separately at national level. Europol should therefore be able to develop, operate, host and provide shared advanced capabilities in support of its tasks and of the competent authorities of the Member States. As law enforcement authorities increasingly rely on electronic evidence and face growing challenges in accessing data that is lawfully available to them, Europol should support the development and provision of capabilities for the decryption of such data. To avoid

duplication and inefficient use of resources at Union level, Europol should, before developing new capabilities, assess the availability of equivalent solutions on the market or within Member States, Union institutions, bodies, offices and agencies and, where available, prioritise their reuse, adaptation or acquisition. Europol should also take into account risks arising from strategic dependencies and reliance on suppliers outside the Union. In the context of investigations and operational activities supported by Europol, where necessary, it should be possible to make available those capabilities to participating third countries, notably where this contributes to the effective conduct of the operational activity and supports the operational objectives pursued by the participating Member States.

(71) To support the development of innovative solutions for advanced capabilities relevant to the performance of its tasks, Europol should be able to carry out and participate in research and innovation activities, including pilot projects and preparatory actions. Europol should ensure synergies and avoid duplications with activities supported by other Union institutions, bodies, agencies and offices and under relevant Union funding programmes.

(72) To enable the development, testing and validation of algorithmic tools and AI systems and models, in a controlled and secure environment providing for adequate safeguards, Europol should use dedicated testing environments. It should participate in regulatory sandboxes established pursuant to Regulation (EU) 2024/1689[51] of the European Parliament and of the Council and, where appropriate, make such environments available to private parties participating in collaborative research and innovation activities.

(73) To assess the effectiveness, suitability and added value for law enforcement use of innovative solutions, Europol should be able to support early deployment, operational testing and validation activities. Where commercial solutions are concerned, such activities should be based on transparent procedures and objective technical and operational criteria.

(74) To facilitate the transition of tested and validated innovative solutions into advanced capabilities for operational use and maximise the operational impact across the Union, Europol should support their uptake, deployment, scaling and integration into operational activities and investigations of the competent authorities of the Member States. Innovative solutions and advanced capabilities can only deliver their full operational benefit where they are accompanied by the necessary skills, expertise and know-how. Europol should therefore support Member States in strengthening specialised expertise and operational capabilities through specialised training activities, in close cooperation with European Union Agency for Law Enforcement Training (CEPOL) established by Regulation (EU) 2015/2219 of the European Parliament and of the Council[52], which coordinates centres of excellence.

(75) To promote coherence, coordination and continuity across foresight, capability planning, research, innovation and capability-development activities carried out under this Regulation, Europol should maintain a dedicated Capabilities and

---

[51] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj).

[52] Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA (OJ L 319, 4.12.2015, p. 1, ELI: http://data.europa.eu/eli/reg/2015/2219/oj).

Innovation Service acting as a central coordination hub within Europol to support the implementation of the Framework and ensure coherence across Europol's Centres and other organisational structures.

(76) Effective capability development increasingly requires cooperation between law enforcement authorities, Union institutions, bodies, offices and agencies, research organisations, academia, technology providers, industry and other innovation actors. Europol should therefore support cooperation and coordination on capability-development and innovation activities at Union level, such as those of the EU Innovation Hub for Internal Security and the Commission's Security Research and Innovation Campus. Europol should also be able to facilitate joint projects, testing activities and other forms of cooperation, including with private parties and, where appropriate, through joint development and procurement activities carried out in accordance with applicable Union law.

(77) Europol should be supported by a Capabilities and Innovation Advisory Group providing expertise on capability-development, research and innovation activities, supporting the preparation and updating of the Framework and facilitating exchanges with other relevant partners, notably research organisations and private parties.

(78) To fulfil its tasks effectively, Europol should be equipped with a governance structure that ensures effective strategic direction, accountability, transparency and sound financial and administrative management. The governance of the Agency needs to be aligned with the Joint Statement of the European Parliament, the Council of the EU and the European Commission of 2012 on decentralised agencies ('Joint Statement and Common Approach') and Commission Delegated Regulation (EU) 2019/715[53].

(79) In order to streamline the decision-making process within Europol, an efficient and effective governance structure should be introduced. To that end, the Member States and the Commission should be represented on a Management Board vested with the necessary powers, including the power to approve the single programming document. In order to ensure effective political oversight, the Management Board should also include a member designated by the European Parliament. The Management Board should be the principal body responsible for the strategic direction and oversight of Europol. It should establish Europol's priorities and objectives, oversee their implementation and exercise the powers conferred upon it under this Regulation in relation to programming, budgetary matters, organisational structure, governance and accountability.

(80) In order to ensure an efficient and effective governance, the Management Board should be assisted by an Executive Board responsible for supporting the preparation and follow-up of strategic, administrative and budgetary decisions. Such arrangements should facilitate effective decision-making while preserving the respective responsibilities of the Management Board and the Executive Director.

(81) To fulfil its tasks, Europol requires strong executive management capable of ensuring the implementation of strategic priorities, the efficient allocation of resources and the effective performance of operational, administrative and organisational tasks. The Executive Director should therefore be entrusted with the

[53] Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (OJ L 122, 10.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg_del/2019/715/oj).

day-to-day management of Europol and should perform those duties independently. Where necessary, the Executive Director should be assisted by one or more Deputy Executive Directors.

(82) To ensure that Europol's activities remain aligned with its strategic objectives and operational priorities, Europol should operate on the basis of a coherent programming and performance-management framework linking multiannual planning, annual activities, resource allocation and performance assessment. Such framework should be driven by the principles of sound financial management, effective use of Union resources and accountability for results.

(83) With regard to the prevention and management of conflicts of interest, it is essential that the Agency acts impartially, demonstrates integrity and establishes high professional standards. To that end, members of Europol's administrative and management structure should act in the public interest and be subject to appropriate rules on transparency, declarations of interests and the prevention and management of conflicts of interest.

(84) To strengthen the Union security architecture, Europol should be able to develop close relations with relevant Union bodies, offices and agencies. Europol should also be able to develop close relations with Union institutions and missions. To frame and facilitate such relations, Europol should conclude working arrangements with them. To ensure consistency with Union policies, the conclusion of working arrangements with Union bodies, offices and agencies established within the framework of the TFEU should be subject to the prior approval of the Commission. Such working arrangements should be updated on a regular basis to remain effective, operationally relevant and aligned with the Union priorities on the fight against evolving criminal threats.

(85) Europol should be able to receive from and transmit or transfer to Union institutions, bodies, missions, offices and agencies both personal and non-personal data in accordance with this Regulation and applicable Union law.

(86) To achieve efficient information exchange while ensuring appropriate safeguards, Europol should ensure that Union bodies, offices and agencies have, in accordance with this Regulation, indirect access to information held by Europol on the basis of an automated hit/no-hit system, under conditions of reciprocity and without affecting any restriction indicated by the provider of the information pursuant to this Regulation. Such access should be limited to information strictly falling within the respective competences of those Union bodies, offices and agencies, such as the EPPO, Eurojust, OLAF and the Authority for Anti-Money Laundering and Countering the Financing of Terrorism ('AMLA'), established by Regulation (EU) 2024/1620 of the European Parliament and of the Council[54].

(87) To ensure that crimes affecting the financial interests of the Union are effectively prosecuted by the EPPO and that information received by Europol from the EPPO strengthens Europol's criminal intelligence on forms of crime falling within the scope of Europol's competence, Europol should develop a structured cooperation with the EPPO. To support the investigations of the EPPO, Europol should, upon request by the EPPO, provide the EPPO with relevant information and operational

[54] Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (OJ L, 2024/1620, 19.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1620/oj).

and analytical support. To that end, Europol should ensure that appropriate organisational arrangements are in place, including the allocation of dedicated human resources, for instance through the establishment of a dedicated support unit. That would allow the EPPO to benefit from Europol's analytical support, ensuring an efficient use of Union resources in the investigation and prosecution of crimes affecting the financial interests of the Union. Considering the competences attributed to the EPPO under Union law, information exchange between the EPPO and Europol on the basis of the automated hit/no-hit system should not be affected by any restriction indicated by the Member State or the Union institution, body, office or agency that provided the information to Europol. Providing the EPPO with such information, independently from any restriction, would reduce delays and avoid taking additional procedural steps following a hit in respect of information that the EPPO could otherwise obtain in accordance with Union law. Given that timely access to information is essential for the effective conduct of investigations by the EPPO, that mechanism would maximise the efficiency gains and added value of Europol as a centralised information hub. In addition, Europol should report to the EPPO on criminal conduct in respect of which the EPPO could exercise its competence, regardless of any restriction indicated by a Member State or a Union institution, body, office or agency. In both instances, Europol should inform the provider of the information.

(88) To ensure synergies at Union level between law enforcement cooperation, through Europol, and judicial cooperation, through Eurojust, Europol should develop a structured cooperation with Eurojust. Where the need for effective judicial follow-up is identified, Europol should initiate the procedure for sharing the relevant information with Eurojust, in compliance with the rules set out in this Regulation.

(89) To reinforce the fight against financial crime at Union level, Europol should develop close relations with the AMLA including through the exchange of operational, strategic and other non-operational information and through the posting of liaison officers at each other's premises. Where Europol, pursuant to Directive (EU) 2019/1153, is invited to support Financial Intelligence Units ('FIUs') in the context of joint analyses and these are carried out with the assistance of the AMLA, Europol should cooperate with the AMLA to more effectively support those FIUs in that context.

(90) Serious and organised crime increasingly exploits international trade flows, supply chains and cross-border movements of goods. Cooperation between Europol and the European Union Customs Authority (EUCA) established by Regulation […] can therefore provide valuable insights for the prevention and combating of serious and organised crime and terrorism. Europol should develop close relations with the European Union Customs Authority, notably to enable reciprocal exchange of relevant data and information, in accordance with Regulation […] and subject to the applicable safeguards and conditions laid down therein.

(91) To contribute to effective protection of the Union's financial interests, Europol should cooperate with the other anti-fraud actors involved in the protection of the Union's financial interests, such as the EPPO, Eurojust, OLAF, AMLA and the EU Customs Authority, to address matters relevant to the coordination of anti-fraud activities, such as facilitating the exchange of information, the undertaking of coordinated or joint actions, exchanging on emerging criminal trends in activities affecting the financial interests of the Union, the sharing of best practices including matters relating to information technology security and development, establishing

criteria for common reporting or coordinating training activities or general developments concerning the anti-fraud architecture of the Union. Being a relevant actor in the protection of the Union financial interests, Europol should participate actively in such joint cooperation activities.

(92) To enhance the Union's overall operational response to cross-border crime such as migrant smuggling trafficking in human beings, Europol and Frontex should be able to leverage their complementary capabilities. They should closely cooperate in particular within the framework of the European Integrated Border Management, as defined in Regulation (EU) 2019/1896 and the European Integrated Border Management multiannual strategic policy cycle, ensuring coherence of action and avoiding operational gaps.

(93) To enhance efficiency, avoid duplication of investments, benefit from economies of scale and promote interoperability, Europol and eu-LISA should cooperate in the development, procurement and use of technical information management components, including, where appropriate, solutions related to biometric data processing and other shared services, in full compliance with their respective mandates and applicable data protection rules.

(94) The prevention and combating of the forms of crime falling within Europol's competence increasingly require cooperation beyond the Union. Europol should, where necessary for the performance of its tasks, establish and maintain cooperative relations with third countries, international organisations and private parties, in accordance with Union law and subject to appropriate safeguards. This cooperation should be conducted in a manner that is consistent with the Union's external policies and priorities. To ensure coherence and consistency, Europol's external engagement should be coordinated, where appropriate, with the relevant Union institutions, bodies, offices and agencies.

(95) Europol's engagement with third countries should focus on operational cooperation, including exchange of information, operational coordination and support to investigations. Concentrating Europol's external activities on operational objectives ensures that its expertise and resources are directed towards activities that provide the greatest operational added value for the competent authorities of the Member States, while remaining complementary to the role of the CEPOL in the area of capacity building in third countries.

(96) The functioning of the Schengen area without controls at the internal borders creates a high degree of mutual dependence between the participating States in the prevention and combating of cross-border crime. Countries associated with the implementation, application and development of the Schengen *acquis* are closely integrated into that common security framework and contribute directly to the security of the Schengen area. Effective protection of the Union internal security therefore requires particularly close cooperation between Europol and those countries. To that end, specific arrangements reflecting the special relationship between those countries and the Union will be key. Given the reciprocal benefits arising from such cooperation, it is also important that those arrangements could be based on mutual rights and obligations, including obligations to share relevant information and provisions on financial contributions.

(97) Countries that are candidates for accession to the Union, as well as potential candidates, are key partners for strengthening European internal security. Owing to their geographical proximity to the Union, their position along major criminal routes

and the cross-regional nature of organised crime, terrorism and criminal offences related to a crime falling within the scope of Europol's competence where such offences involve a hybrid dimension, close operational cooperation with those countries is an important element for the effective prevention and combating of such crimes and threats.

(98) In order to support operational cooperation with third countries and international organisations, it is necessary to provide clear conditions under which personal data may be transferred while ensuring a high level of protection of fundamental rights and freedoms, in particular the right to the protection of personal data. Any such transfers should take place only in accordance with Regulation (EU) 2018/1725 and the specific provisions of this Regulation and be subject to the conditions and safeguards laid down therein. Transfers of personal data to third countries and international organisations may require swift decisions. In order to ensure both operational responsiveness and a clear allocation of responsibility, decisions authorising such transfers under the conditions and safeguards laid down in Regulation (EU) 2018/1725 should be taken by the Executive Director.

(99) Information necessary for the prevention and combating of crimes increasingly originates from private parties, including providers of electronic communications services, online platforms, financial institutions, transport operators and other private entities. Europol should, within its competence, receive, process and exchange information and personal data involving private parties where necessary and proportionate for the performance of its tasks, while respecting the responsibilities of the Member States.

(100) The prevention of serious threats to public security, including those arising from the dissemination of terrorist content and from online crisis situations, increasingly relies on effective cooperation between public authorities and private parties. The effective implementation of certain measures and obligations provided for under Union law, including Regulation (EU) 2021/784 and Regulation (EU) 2022/2065, may require timely exchanges of information between Europol and relevant private parties. To reconcile operational effectiveness with a high level of protection of fundamental rights, in particular the right to the protection of personal data, it is therefore necessary to set out the conditions for such exchanges.

(101) Information voluntarily provided by natural persons may contribute to the prevention and combating of the forms of crime falling within Europol's competence. Appropriate conditions are necessary to ensure that such information can be used where operationally relevant, while preserving Europol's role as a law-enforcement support agency and ensuring the protection of the rights and freedoms of the persons concerned.

(102) Regulation (EU) 2018/1725 of the European Parliament and of the Council applies to the processing of personal data by Europol. This Regulation should therefore be understood as laying down only those data protection rules that are necessary to supplement, clarify or specify the application of Regulation (EU) 2018/1725 in view of the specific tasks and operational activities of Europol. Accordingly, the provisions of this Regulation concerning the processing of personal data by Europol constitute *lex specialis* in relation to Regulation (EU) 2018/1725 and should prevail only to the extent that they provide more specific rules.

(103) The effectiveness of criminal intelligence and law enforcement cooperation depends on the quality of the information processed by Europol. Therefore, wherever

possible, the reliability of the source of the information and the accuracy of the information received, retrieved or analysed by Europol should be assessed based on a common evaluation methodology. Where information is received by Europol, the responsibility for that assessment should remain with the provider of the information. Where Europol considers that an assessment should be revised, it should seek agreement with the provider concerned.

(104) Personal data concerning victims of criminal offences, witnesses and other persons who may provide information relevant to criminal offences require particular protection, in line with the provisions of the Directive 2012/29/EU on establishing minimum standards on the rights, support and protection of victims of crime. Europol should therefore process such data only where it is strictly necessary and proportionate for the performance of its tasks and subject to appropriate safeguards. In order to better contribute to the fight against the criminal exploitation of young perpetrators and in the best interest of the child, Europol should be able to process the data of persons under the age of 18 where it is necessary and proportionate for preventing or combating crime which falls within the scope of Europol's competence.

(105) Sensitive personal data in accordance with Article 4(13), (14) and (15) and Article 9 and recitals (51) to (56) of Regulation (EU) 2016/679 should be processed by Europol only where strictly necessary and proportionate for the performance of its tasks and subject to appropriate safeguards and oversight mechanisms.

(106) Biometric data may be processed for different purposes and do not in all circumstances present the same risks to the rights and freedoms of data subjects. The specific safeguards laid down in this Regulation for special categories of personal data should therefore apply to biometric data only where they are processed for the purpose of uniquely identifying a natural person, in accordance with Regulation (EU) 2018/1725. Processing of biometric data for the purpose of uniquely identifying a natural person by Europol in the Europol Analytical Environment and where otherwise required under Union law should be considered strictly necessary for preventing or combating crimes falling within the scope of Europol's competence.

(107) Europol should be able to process personal data for research and innovation purposes subject to appropriate safeguards, including prior authorisation by the Executive Director and oversight by the Management Board. Where Europol considers that a new type of project poses a significant risk to the rights and freedoms of data subjects, Europol should also carry out a data protection impact assessment and inform the European Data Protection Supervisor before launching the project.

(108) Data subjects should be able to exercise the right of access referred to in Regulation (EU) 2018/1725 by making a request either to Europol or through the national authority appointed for that purpose in any Member State. Given that personal data processed by Europol frequently originate from providers, decisions on data subject access requests should be taken in close cooperation with the Member States and the data providers concerned in order to ensure both the effective protection of data subject rights and the safeguarding of ongoing investigations. In order to ensure that the time limit for answering data subject access requests can always be respected, the Member States and the providers consulted should reply to Europol without delay.

(109) In order to ensure a high level of data quality and accuracy, personal data processed by Europol should be rectified, erased or subject to restriction of processing where they are inaccurate, unlawfully processed or no longer required in accordance with

this Regulation and Regulation (EU) 2018/1725. Given that personal data processed by Europol may originate from a variety of sources, Europol and the provider of the data concerned should cooperate closely when taking measures affecting the accuracy, storage or use of such data.

(110) The prior consultation mechanism with the European Data Protection Supervisor (EDPS) under Regulation (EU) 2018/1725 is a key safeguard. It applies only to high-risk processing operations, where the potential risks to data subjects are particularly significant. At the same time, prior consultation should not be required for the adjustment, modification or deployment of existing capabilities, including in a defined operational context, provided that such activities do not alter the nature, scope, or purpose of the processing in a manner that would increase the risk to the rights and freedoms of data subjects. To preserve Europol's operational effectiveness, the period within which the EDPS is able to provide written advice pursuant to Regulation (EU) 2018/1725 should be of eight weeks and should not be suspended or extended. In particularly urgent cases of substantial significance for the performance of Europol's tasks, Europol should be able to exceptionally begin processing where this is necessary to prevent and combat an immediate criminal threat or to protect vital interests of the data subject or another person. In such cases, Europol should inform the EDPS prior to the start of the processing operations and should provide all the information required for the purpose of the prior consultation within four weeks following the start of the processing operations.

(111) Regulation (EEC, Euratom) No 1182/71 of the Council[55] should be applicable to any time period provided for the EDPS under this Regulation.

(112) To ensure robust compliance with the rules on the protection of personal data, the Management Board of Europol should appoint a Data Protection Officer. The Data Protection Officer should be able to perform his or her duties in accordance with Regulation (EU) 2018/1725. Where the Data Protection Officer identifies a case of non-compliance with the rules on the protection of personal data, he or she should be able to require the Executive Director to take corrective action within a specified timeframe. Should the Executive Director fail to act, the Data Protection Officer should be empowered to escalate the matter to the Management Board and, where necessary, ultimately to the EDPS.

(113) To support Europol in respecting, promoting and fulfilling fundamental rights throughout its action, the Management Board should designate a Fundamental Rights Officer.

(114) Ensuring respect for fundamental rights requires specialist knowledge by Europol staff. Europol staff should therefore receive appropriate training on fundamental rights and freedoms. Europol staff involved in operational activities should receive dedicated training on data protection and the practical application of the safeguards laid down in this Regulation and Regulation (EU) 2018/1725. To ensure a high and consistent standard of training, Europol should cooperate with the European Union Agency for Fundamental Rights established by Council Regulation (EC) No 168/2007[56]and CEPOL in the development of such training.

---

[55] Regulation (EEC, Euratom) No 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits (OJ L 124, 8.6.1971, p. 1, ELI: http://data.europa.eu/eli/reg/1971/1182/oj).

[56] Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights (OJ L 53, 22.2.2007, p. 1, ELI: http://data.europa.eu/eli/reg/2007/168/oj).

(115) National authorities competent for the supervision of the processing of personal data should monitor the lawfulness of any provision of personal data to Europol by Member States. The EDPS should monitor the lawfulness of data processing carried out by Europol, exercising his or her functions in accordance with Regulation (EU) 2018/1725. To ensure effective supervision of Europol, the EDPS and national supervisory authorities should closely cooperate with each other on specific issues requiring national involvement.

(116) Pursuant to Article 88 of the TFEU, Europol's activities are to be subject to scrutiny by the European Parliament together with national parliaments. Effective parliamentary scrutiny contributes to the democratic accountability, transparency and legitimacy of Europol's activities while respecting its operational independence and the responsibilities of the competent authorities of the Member States. Effective scrutiny requires regular dialogue with Europol and access to the information necessary for the performance of that task, while respecting the requirements of confidentiality and the protection of ongoing investigations and operational activities. The protection of fundamental rights, in particular the right to the protection of personal data, is of particular importance in the exercise of Europol's tasks. Parliamentary scrutiny should therefore be supported by appropriate exchanges with the European Data Protection Supervisor and by access to independent expertise on fundamental rights matters.

(117) Europol's operational effectiveness depends on maintaining specialised expertise and practical experience in law enforcement matters. In order to preserve a close connection with the operational realities and needs of the competent authorities of the Member States, certain posts should be occupied by personnel possessing relevant experience acquired within those authorities. This contributes to ensuring that Europol's activities remain closely aligned with operational developments, investigative practices and emerging security threats across the Union.

(118) The exchange of expertise and operational experience between Europol and the competent authorities of the Member States contributes to effective law-enforcement cooperation within the Union. The use of seconded national experts strengthens mutual understanding, facilitates the sharing of specialised knowledge and best practices and supports the effective performance of Europol's tasks.

(119) The performance of Europol's tasks requires budgetary resources that are commensurate with its operational responsibilities and capable of supporting long-term planning, operational support and the development of common capabilities for the benefit of the Member States. To carry out its tasks, Europol should be properly resourced and granted an autonomous budget. It should be mainly financed by a contribution from the general budget of the Union. The Union budgetary procedure should be applicable to the Union contribution and to any other subsidies chargeable to the general budget of the Union. The auditing of accounts should be undertaken by the European Court of Auditors.

(120) Financial contributions through grants are an important element of Europol's operational support to Member States to prevent and combat the forms of crime falling within Europol's competence. Moreover, given the transnational nature of serious crime and terrorism, effective operational support might also require financial contributions to third countries or international organisations involved in operational activities with Member States. In that respect, certain activities necessary for the fulfilment of Europol's tasks are intrinsically linked to the actors involved in a in a

particular operational activity. Moreover, the effectiveness of Europol's financial support may depend on timely implementation, confidentiality and continuity of cooperation among the actors involved. In such cases, a competitive call for proposals would not be capable of identifying an alternative beneficiary Therefore, it should be possible for Europol, in duly justified cases, to award grants without a call for proposals for activities falling within the scope of its tasks.

(121) The necessary provisions regarding accommodation for Europol in the Netherlands, where it has its seat, and the specific rules applicable to Europol staff and members of their families should be laid down in a Headquarters Agreement between Europol and the Kingdom of the Netherlands. The host Member State should provide the best possible conditions to ensure the effective functioning of Europol.

(122) Europol established by this Regulation should succeed Europol established by Regulation (EU) 2016/794 in respect of all its rights and obligations. In order to ensure legal certainty, operational continuity and the stability of Europol's external relations, cooperation agreements and working arrangements concluded by Europol under the Europol Convention, Decision 2009/371/JHA or Regulation (EU) 2016/794 should remain in force and be applied until they expire or are replaced.

(123) Appropriate transitional arrangements are necessary to ensure the uninterrupted functioning of Europol and the continuity of its activities. Decisions, implementing measures, rules and arrangements adopted pursuant to Regulation (EU) 2016/794 should therefore remain in force until repealed or replaced. In order to ensure consistency with the legal framework established by this Regulation, the Management Board should review those measures without undue delay and determine whether they remain appropriate and compatible with this Regulation or should be amended or repealed. In order to strengthen continuity and strategic leadership within Europol and to enhance the long-term planning and implementation of its operational priorities, it is appropriate also to adapt the duration of the on-going respective mandates of the Executive Director and the Deputy Executive Directors. Ensuring continuity in Europol's current executive management is necessary to safeguard institutional stability and operational effectiveness of the Agency. Therefore, the duration of the term of office for the members of Europol's executive management who are serving their first term of office at the time of entry into force of this Regulation, should allow for a maximum total term of office of ten years. The duration of the term of office for the members of Europol's executive management who are serving their second term of office at the time of entry into force of this Regulation, should allow for a maximum total term of office of nine years.

(124) The increasing digitalisation of law enforcement cooperation and the development of advanced information systems, cloud infrastructures and secure communication services require closer cooperation between Europol and eu-LISA. Given eu-LISA's expertise in the development and operation of large-scale information systems and related communication infrastructures in the area of freedom, security and justice, and Europol's role in supporting operational law enforcement cooperation, it is appropriate to provide rules for the cooperation between the two agencies. Such cooperation should enable synergies, avoid duplication of efforts, promote interoperability and cost-efficiency, and facilitate the re-use of technical components, services and expertise, while fully respecting the respective mandates, governance structures and responsibilities of the two agencies. Therefore, Regulation (EU)

2018/1726 of the European Parliament and of the Council[57] should be amended accordingly.

(125) eu-LISA already operates a public key infrastructure and provides certification services supporting the secure operation of Union information systems in the area of freedom, security and justice. In order to ensure a high level of security, trust and interoperability across Europol services and tools, Europol should be able to make use of those existing services. To that end, eu-LISA should be able to provide public key infrastructure certificates to Europol and, where appropriate, to the competent authorities of the Member States connected to Europol services and tools. That should enable Europol to benefit from existing capabilities and expertise available at Union level in a cost-efficient manner, contributing to secure authentication, encrypted communications and trusted electronic interactions.

(126) In order to strengthen Europol's capacity to support Member States in the prevention and combating of serious crime and terrorism, and to make more effective use of existing Union information exchange frameworks, Europol should be able, under clearly defined conditions, to conduct searches in national databases connected under the Prüm II framework on behalf of Member States. It is important that Europol provides operational, analytical, technical and forensic support in situations where its expertise, resources or cross-border perspective can provide added value, while fully preserving Member States' ownership of data, investigative autonomy and the decentralised architecture underpinning the Union information exchange systems. Regulation (EU) 2024/982 currently enables Europol to conduct searches in Member States' Prüm databases using data received from third countries. In order to remove any operational limitation that may prevent the identification of relevant cross-border links, Europol should also be able to conduct such searches using data originating from Member States, where authorised by the data-owning Member State. This should apply in particular to searches involving DNA profiles, dactyloscopic data and facial images, while ensuring that Member States will be able to decide on the conditions under which their data may be used. Therefore, Regulation (EU) 2024/982should be amended accordingly.

(127) To enhance the effectiveness of Europol's access to data stored in Member States' databases, while ensuring the protection of personal data and the respect of national law, Europol should have access to data stored in national databases and police record indexes, subject to specific conditions and limitations, including the use of designated routers and systems, such as EPRIS, EUCARIS and the router for biometric data and the requirement for human oversight and decision-making in the return of core data, and should only use data originating from Member States where authorised by the data-owning Member State, and should handle such data in accordance with Regulation (EU) 2018/1725 and this Regulation as well as the consent of the relevant Member State.

(128) Where Europol conducts searches using biometric data originating from Member States, it should act solely as a technical and forensic service provider on behalf of the authorising Member State. Europol should therefore carry out such searches only within the scope of the authorisation granted by the Member State concerned, whether on a case-by-case basis or through standing authorisations subject to conditions defined by that Member State. Europol should fully respect any

[57] Regulation (EU) 2018/1726 of the European Parliament and of the Council …(OJ…, ELI: ..).

restrictions imposed by the authorising Member State regarding access to, use, transmission, retention, deletion or destruction of the information concerned.

(129) Since the objectives of this Regulation, namely to support and strengthen the action of 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 affecting a common interest covered by a Union policy, cannot be sufficiently achieved by the Member States acting alone but can rather, by reason of the scale, transnational nature and effects of those threats, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(130) [In accordance with Article 3 and Article 4a(1) 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 (TEU) and to the TFEU, Ireland has notified [*, by letter of ...,*] its wish to take part in the adoption and application of this Regulation] OR [In accordance with Articles 1, 2 and Article 4a(1) 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 (TEU) and to the TFEU, and without prejudice to Article 4 of that Protocol, Ireland is not taking part in the adoption of this [*act*] and is not bound by it or subject to its application.]

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

(132) The EDPS was consulted in accordance with Article 42 of Regulation (EU) 2018/1725 and delivered an opinion on [date].

(133) This Regulation fully respects the fundamental rights and freedoms 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 respectively, as well as by Article 16 TFEU, the right to an effective remedy and to a fair trial under Article 47 of the Charter, the presumption of innocence under Article 48 of the Charter, and the rights of victims of crime.

(134) This Regulation aims to amend and expand the provisions of Regulation (EU) 2016/794. Since the amendments to be made are substantial in number and nature, that legal act should, for the sake of clarity, be repealed,

HAVE ADOPTED THIS REGULATION:

Chapter I
General provisions

Article 1

Subject matter

1. This Regulation establishes a European Union Agency for Law Enforcement Cooperation (Europol) to support and strengthen action by the competent authorities of the Member States and their mutual cooperation with the aim to prevent and combat cross-border serious crime, terrorism and forms of crime which affect a common interest covered by a Union policy.

2. Europol, as established by this Regulation, shall replace and succeed the agency established by Regulation (EU) 2016/794.

Article 2

Legal status

1. Europol shall be an agency of the Union and shall have legal personality.

2. In each of the Member States, Europol shall enjoy the most extensive legal capacity accorded to legal persons under national law. It may, in particular, acquire and dispose of movable and immovable property and be party to legal proceedings.

3. Europol shall be represented by an Executive Director.

Article 3

Seat

The seat of Europol shall be in The Hague, the Netherlands.

Article 4

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'competent authorities of the Member States' means all police authorities and other law enforcement services existing in the Member States which are responsible under national law for preventing and combating criminal offences and other public authorities existing in the Member States which are responsible under national law for preventing and combating criminal offences in respect of which Europol is competent;

(2) 'strategic analysis' means all methods and techniques by which information is collected, stored, processed and assessed with the aim of supporting and developing a criminal policy that contributes to the efficient and effective prevention and combating of crime;

(3) 'operational analysis' means all methods and techniques by which information is collected, stored, processed and assessed with the aim of supporting criminal investigations and criminal intelligence activities;

(4) 'private parties' means entities and bodies established under the law of a Member State or third country, including companies and firms, business associations, non-profit organisations and other legal persons that are not covered by point 5;

(5) 'recipient' means a natural or legal person, public authority, agency or any other body to which data are disclosed, whether a third party or not;

(6) 'administrative personal data' means personal data processed by Europol other than operational personal data

(7) ‘terrorist content’ means terrorist content as defined in Article 2, point (7), of Regulation (EU) 2021/784;

(8) ‘online child sexual abuse’ means the online dissemination of child sexual abuse material and the solicitation of children;

(9) ‘online crisis situation’ means the dissemination of online content stemming from an ongoing or recent real world event which depicts harm to life or to physical integrity, or calls for imminent harm to life or to physical integrity;

(10) ‘immigration liaison officer’ means an immigration liaison officer as defined in Article 2, point (1), of Regulation (EU) 2019/1240 of the European Parliament and of the Council[58];

(11) 'single point of contact' means the central entity responsible for coordinating and facilitating the exchange of information in accordance with Article 14 of Directive (EU) 2023/977 of the European Parliament and of the Council[59];

(12) ‘advanced capabilities’ means technological, analytical or operational capabilities providing enhanced or novel functionalities supporting the prevention and combating of the forms of crime falling within the scope of Europol’s competence and cooperation between the competent authorities of the Member States.

Article 5

Competence

1. Europol shall 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, as listed in Annex I.

2. Europol’s competence shall also cover criminal offences related to the forms of crime listed in Annex I, in particular offences committed for the purpose of preparing, facilitating, supporting or concealing such forms of crime, offences committed in connection therewith, or offences committed to ensure the impunity of persons involved in such forms of crime, including where such offences involve a hybrid dimension.

Article 6

Tasks

1. Europol shall perform the following tasks:

   (a) collect, store, process, analyse and exchange information, including criminal intelligence;

   (b) provide operational support to the competent authorities of the Member States, including the coordination, organisation and implementation of investigative

[58] Regulation (EU) 2019/1240 of the European Parliament and of the Council of 20 June 2019 on the creation of a European network of immigration liaison officers (OJ L 198, 25.7.2019, p. 88, ELI: http://data.europa.eu/eli/reg/2019/1240/oj).

[59] Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA (OJ L 134, 22.5.2023, p. 1, ELI: http://data.europa.eu/eli/dir/2023/977/oj).

and operational actions, analytical support through operational analysis, and technical and forensic support;

(c) provide support of a strategic and thematic nature to the competent authorities of the Member States and Union institutions through strategic analysis and by preparing analytical products, including threat assessments, strategic analyses, trend reports and situational briefings;

(d) cooperate with Union institutions, bodies, missions, offices and agencies, where relevant through the exchange of information and provision of analytical support in areas that fall within their respective mandates;

(e) cooperate with third countries and other relevant partners, in particular through the exchange of information;

(f) carry out research and innovation activities under the Union Framework Programme for Research and Innovation, and develop advanced capabilities;

(g) develop and maintain information management and ICT services, tools and components enabling it to perform the tasks referred in points (a) to (e);

(h) provide financial support for operational activities carried out in the context of investigative or operational actions.

2. In addition to the tasks set out in paragraph 1, Europol shall carry out the following supportive tasks:

(a) provide information and operational support to Member States in connection with major international events;

(b) provide information and operational support to Union crisis management structures and missions established on the basis of the TEU, within the scope of Europol's competence;

(c) provide administrative, financial and technical support to Union-funded operational projects and European law enforcement networks falling within the scope of Europol's competence, to enhance coordination, continuity and coherence of action;

(d) act as the Central Office for combating euro counterfeiting in accordance with Council Decision 2005/511/JHA[60], including by encouraging the coordination of measures carried out to fight euro counterfeiting by the competent authorities of the Member States or in the context of joint investigation teams, where appropriate in liaison with Union bodies, offices and agencies and the authorities of third countries;

(e) support the Member States in the screening, as regards the expected implications for security, of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council[61] that concern undertakings that provide technologies, including

[60] Council Decision 2005/511/JHA of 12 July 2005 on protecting the euro against counterfeiting, by designating Europol as the Central Office for combating euro counterfeiting (OJ L 185, 16.7.2005, p. 35, ELI: http://data.europa.eu/eli/dec/2005/511/oj).

[61] 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, ELI: http://data.europa.eu/eli/reg/2019/452/oj).

software, used by Europol for the prevention and combating of crimes falling within the scope of Europol's competence

(f) contribute to the implementation of the Schengen Evaluation and Monitoring Mechanism to verify the application of the Schengen acquis under Council Regulation (EU) 2022/922[62], Regulation (EU) 2022/922, within the scope of Europol's competence, through the participation in Schengen evaluation missions and other on-site visits, provision of expertise and analyses, where requested by the Commission.

(g) cooperate in a structured way and on a regular basis, including by concluding bilateral or multilateral working arrangements governing the modalities of such cooperation, with the anti-fraud actors involved in the protection of the Union's financial interests, such as the EPPO, Eurojust, OLAF, AMLA and the EU Customs Authority.

3. Europol shall not apply coercive measures in carrying out any of its tasks.

During the execution of investigative measures by the national competent authorities of the Member States, Europol may support those competent authorities, at their request and in accordance with their national law, in particular by facilitating cross-border information exchange and other forms of data processing and by providing operational support remotely or by being present during the execution of those measures. Europol shall not have the power to execute investigative measures.

Article 7

Europol's strategic support

1. Europol shall contribute to the development of a common Union strategic analytical framework relating to serious crime and terrorism.

For that purpose, Europol shall prepare, on a regular basis, analytical products on internal security, including strategic analyses, threat assessments, trend reports and situational briefings, and shall make them available in accordance with Article 129.

2. Europol shall support the development and use of common analytical methodologies and standards, in particular for Union-level threat assessments, to ensure comparability, interoperability and consistency of analytical products.

3. Member States shall provide Europol with all necessary information for the preparation of the analytical products referred to in paragraph 1.

Member States may refuse to supply information based on one or more of the following grounds:

(a) the supply of information is contrary to the essential interests of the security of the Member State concerned;

(b) the supply of information jeopardises the success of an ongoing investigation or the safety of an individual;

(c) the supply of information would disclose information relating to organisations or specific intelligence activities in the field of national security.

---

62 Council Regulation (EU) 2022/922 of 9 June 2022 on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen *acquis*, and repealing Regulation (EU) No 1053/2013 (OJ L 160, 15.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/922/oj).

Member States shall supply information as soon as the grounds referred to in points (a), (b) or (c), cease to exist.

4. Union institutions, bodies, offices and agencies shall, within their competence and in accordance with applicable Union law, provide Europol with information relevant for the preparation of the analytical products referred to in paragraph 1.

5. Europol may use open-source information and contributions from relevant partners as complementary sources for the preparation of the analytical products referred to in paragraph 1.

6. The analytical products referred to in paragraph 1 shall be made available to the Council and the Commission for the identification, development and implementation of strategic, policy and operational priorities of the Union for fighting crime and in the implementation thereof.

7. Europol shall use the analytical products referred to in paragraph 1 to support the planning and implementation of operational activities under this Chapter and shall take those products into account in the preparation and regular updating of the Framework referred to in Article 57.

8. Member States shall take the analytical products referred to in paragraph 1 into account when determining their participation in operational activities supported by Europol, allocating operational resources and implementing Union strategic and operational priorities at the national level.

9. The analytical products referred to in paragraph 1 may be used for the purposes of analyses carried out by the Commission and the Member States and for Schengen evaluations and monitoring activities carried out in accordance with Regulation (EU) 2022/922 in the policy areas falling within the scope of Europol's competence.

Chapter II
Operational cooperation

SECTION 1
OPERATIONAL SUPPORT AND COORDINATION

Article 8

Europol's operational support

1. Europol shall provide operational support to the competent authorities of the Member States to contribute to the prevention and combating of the forms of crime falling within Europol's competence.

2. Europol shall establish and maintain the capabilities necessary to provide continuous and effective operational support to the competent authorities of the Member States.

3. Europol shall support, in particular:

   (a) investigations and operational activities requiring coordinated action at Union level;

   (b) the identification, targeting and disruption of high-risk criminal networks and their supporting criminal infrastructure;

(c) operational activities requiring specialised analytical, technical, digital, forensic or multidisciplinary capabilities;

(d) the detection, analysis and coordination of action against large-scale, emerging, rapidly evolving security threats, including criminal offences related to the forms of crime listed in Annex I where such offences involve a hybrid dimension and the coordination of law enforcement responses to them;

(e) the implementation of Union strategic and operational priorities relating to internal security.

4. Operational support provided by Europol may, as appropriate and in accordance with operational needs, be provided through, among others:

(a) Union Centres of specialised expertise ('Centres'), as referred to in Articles 13 to 19;

(b) operational task forces in accordance with Article 20;

(c) joint investigation teams in accordance with Article 21, including in cooperation with Eurojust;

(d) Europol deployments in accordance with Article 22;

(e) support to strategic and operational activities carried out within the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT) in accordance with Article 23.

5. Europol shall ensure the coordination, coherence and complementarity of the operational support, structures and cooperation instruments referred to in this Chapter, including where several forms of operational support are deployed simultaneously.

6. Member States shall seek to make effective use of the forms of operational support referred to in paragraph 4, notably where coordinated Union-level action is necessary to ensure an effective response to serious and organised crime and terrorism.

7. Where the Operational and Analysis Service or the Centres identify operational links or coordination needs relating to cross-border criminal activities, Europol shall request the competent authorities of the Member States concerned to provide relevant information, criminal intelligence or contribute to coordination measures.

The competent authorities of the Member States concerned shall respond without undue delay and, where they decide not to provide the requested contribution or participate in the proposed coordination measures, they shall provide Europol with a reasoned justification.

Article 9

Operational support to financial investigations and asset recovery

1. Europol shall cooperate with asset recovery offices established pursuant to Article 5 of Directive (EU) 2024/1260.

2. Member States shall ensure that Europol has direct and immediate access to the information referred to in Article 6(2) of Directive (EU) 2024/1260 under the conditions set out therein and to the extent necessary for the performance of the tasks referred to in Article 16 of this Regulation.

Member States shall also ensure that Europol can swiftly obtain the information listed in Article 6(3) of Directive (EU) 2024/1260 upon request to the relevant access recovery office and in situations described in Article 6(4) of that Directive, to the extent necessary for the performance of the tasks referred to in Article 16 of this Regulation.

Access to information referred to in this paragraph shall be compliant with Article 6(5) and (6) of Directive (EU) 2024/1260.

3. Where Europol considers that there is an imminent risk of disappearance of property traced and identified as a result of the activities referred to in Article 16 of this Regulation, it shall submit a request to the competent authorities of the Member States concerned to take immediate action in accordance with Article 11(2) of Directive (EU) 2024/1260.

The competent authority of the Member State concerned shall decide on the request without delay and, where possible, within 24 hours.

Where the competent authority of the Member State concerned decides not to take immediate action, it shall inform Europol and provide the reasons for its decision. Those reasons may be withheld in the following cases:

(a) the disclosure of the reasons is contrary to the essential interests of the security of the Member State concerned;

(b) the disclosure of the reasons jeopardises the success of an ongoing investigation or the safety of an individual.

4. Europol shall cooperate, in accordance with Article 12 of Directive (EU) 2019/1153 of the European Parliament and of the Council[63], with Financial Intelligence Units (FIUs) established pursuant to Directive (EU) 2015/849 of the European Parliament and of the Council[64], through the relevant Europol national unit or, where allowed by the relevant Member State, by direct contact, in particular through the exchange of information and the provision of analyses to Member States to support cross-border investigations falling within the scope of Europol's competence.

5. Each Member State shall ensure that its FIU, within the limits of its mandate and competence and subject to national procedural safeguards, is entitled to reply to duly justified requests that are made by Europol in accordance with Article 12 of Directive (EU) 2019/1153 regarding financial information and financial analyses, either via its Europol national unit or, where allowed by that Member State, by direct contact between the FIUs and Europol.

Article 10

Financial support for operational activities

---

63 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, ELI: http://data.europa.eu/eli/dir/2019/1153/oj).

64 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, ELI: http://data.europa.eu/eli/dir/2015/849/oj).

1. Upon receipt of a duly justified written request from a Member State, Europol may provide targeted financial support for operational activities carried out in the context of a priority investigation or operational action supported by Europol and falling within the scope of its competence.

2. The financial support referred to in paragraph 1 shall be limited to what is necessary and proportionate for the purposes of the relevant priority investigation or operational action and may cover the operational, technical, logistical and other necessary expenditures required for its effective implementation.

3. Europol may, where appropriate and in accordance with operational priorities, prioritise financial support for coordinated cross-border operational activities.

4. Decisions to grant the financial support referred to in paragraph 1 shall be taken by Europol on a case-by-case basis, in accordance with implementing rules adopted by the Management Board on a proposal from the Executive Director and after consultation of the Commission.

   Those implementing rules shall provide for the conditions and procedures for granting, managing and monitoring such support, including requirements ensuring accountability, traceability, auditability and compliance with applicable Union financial rules.

Article 11

Request to initiate a criminal investigation

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

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

3. Paragraphs 1 and 2 do not apply with regard to criminal offences affecting the Union's financial interests that fall within the scope of the competence of the EPPO.

4. The competent authorities of the Member States concerned shall examine any request made pursuant to paragraphs 1 and 2 as a matter of priority and shall take a reasoned decision without undue delay.

   Europol national units shall inform Europol, with regard to any request made pursuant to paragraphs 1 or 2, of the decision of the competent authorities of the Member States, without undue delay.

5. Where the competent authorities of a Member State decide not to accede to a request made pursuant to paragraphs 1 and 2, they shall inform Europol of the reasons for the decision without undue delay, and in any event within one month of receipt of the request. The reasons may be withheld in the following cases:

   (a) the disclosure of the reasons is contrary to the essential interests of the security of the Member State concerned;

(b) the disclosure of the reasons jeopardises the success of an ongoing investigation or the safety of an individual.

6. Europol shall immediately inform Eurojust of any request made under paragraphs 1 and 2, and of any decision of a competent authority of a Member State taken pursuant to paragraphs 4 and 5 to enable Eurojust to ensure timely judicial follow-up at national level and to exercise its competence, including, where appropriate, the capacity to act on its own initiative in accordance with the applicable provisions of Regulation (EU) 2018/1727.

7. Europol shall immediately inform the EPPO of requests made under paragraphs 1 and 2 concerning criminal offences falling within the EPPO's competence, and of any related decision of a competent authority of a Member State pursuant to paragraph 4 and 5.

SECTION 2
OPERATIONAL SPECIALISED CAPABILITIES

Article 12

Operational and Analysis Service

1. Europol shall maintain, through the Operational and Analysis Service, a continuous 24/7 operational and analytical capability to support the coordination, organisation and implementation of investigative and operational action carried out jointly with the Member States pursuant to this Regulation.

2. The Operational and Analysis Service shall ensure:

(a) the operational and strategic analysis of information and criminal intelligence, including in support of the activities carried out by the Centres;

(b) the support and coordination of analysis projects;

(c) the provision of cross-cutting services in the areas of interoperability, biometrics, open-source intelligence (OSINT), travel intelligence and satellite imagery;

(d) the identification of operational links, and the coordination of cross-border operational and investigative responses, including, where appropriate, by proposing the establishment of a Joint Operational Analysis Case (JOAC);

(e) the coordination and coherence of operational support provided pursuant to this Regulation, including in the framework of operational task forces, joint investigation teams, Europol deployments and EMPACT activities;

(f) the preparation of the analytical products referred to in Article 7.

3. The Operational and Analysis Service shall ensure coordination, cooperation and operational coherence between the Union Centres of specialised expertise, in particular where operational activities, criminal intelligence or investigations concern multiple forms of crime, or criminal offences related to the forms of crime listed in Annex I where such offences involve a hybrid dimension, or otherwise require a multidisciplinary response.

Article 13

Union Centres of specialised expertise

1. The European Cybercrime Centre, the European Counter Terrorism Centre, the European Financial and Economic Crime Centre, the European Serious and Organised Crime Centre and the European Centre Against Migrant Smuggling are hereby established as Union Centres of specialised expertise ('Centres').

2. The Centres shall form part of Europol's organisational structure and shall not have separate legal personality. They shall serve as Europol's primary specialised capability and expertise structures in their respective areas and shall support the prevention and combating of the forms of crimes, including criminal offences related to the forms of crime listed in Annex I where such offences involve a hybrid dimension, falling within the scope of Europol's competence.

3. The Centres shall, in particular:

   (a) provide specialised operational support to the competent authorities of the Member States;

   (b) provide operational support within the framework of operational task forces, joint investigation teams and EMPACT;

   (c) facilitate coordination and cooperation between Member States, and, where appropriate, with other Union institutions, bodies, offices and agencies and relevant partners, including the identification of operational links;

   (d) support integrated operational action, under the coordination of the Operational and Analysis Service, involving multiple forms of crime falling within the scope of Europol's competence, or criminal offences related to the forms of crime listed in Annex I where such offences involve a hybrid dimension, including through the mobilisation and coordination of specialised expertise and capabilities across several operational areas;

   (e) identify capability needs and contribute to the development, deployment and integration of advanced capabilities into the activities of Europol and of the competent authorities of the Member States, including through specialised training, in coordination with the Foresight and Capability Service and in close cooperation with the Europol support offices;

   (f) contribute to the preparation of analytical products referred to in Article 7.

4. Europol shall ensure that the activities of the Centres are consistent with Union strategic and operational priorities on internal security, including those established within the EMPACT framework.

5. The Centres may include liaison officers and representatives of other Union bodies, offices and agencies in accordance with the implementing rules referred to in paragraph 6.

   Europol may also invite partners with relevant expertise to contribute to the activities referred to in paragraph 3, points (e) and (f), in accordance with the implementing rules referred to in paragraph 6.

6. Upon a proposal from the Executive Director, the Management Board shall adopt implementing rules on the organisation, specific functions, composition and operation of the Centres and shall regularly review and, where necessary, adapt these rules in light of operational needs and evolving security threats.

Article 14

European Serious and Organised Crime Centre

In accordance with Article 6(1), point (b), the support provided by Europol, notably through the European Serious and Organised Crime Centre shall, in particular, consist of:

(a) supporting the identification, prioritisation, targeting and disruption of high-value targets and high-risk criminal networks;

(b) supporting and coordinating cross-border investigations and operational activities relating to drug trafficking, trafficking in firearms and explosives, environmental crime, property crime and other forms of serious and organised crime;

(c) providing specialised expertise in support of complex, multi-jurisdictional investigations and operational activities, including in the framework of Operational Task Forces, joint investigation teams and EMPACT activities;

(d) supporting the identification, monitoring and disruption of the recruitment and exploitation of children and young persons by criminal networks, including through online services and platforms, for the purposes of committing, facilitating or concealing criminal activities.

Article 15

European Cybercrime Centre

In accordance with Article 6(1), point (b), the support provided by Europol, notably through the European Cybercrime Centre shall, in particular, consist of:

(a) supporting Member States, and where relevant private parties, in preventing and responding to cyberattacks of suspected criminal origin and large-scale malicious online activities, including in cooperation with the European Union Agency for Cybersecurity (ENISA), including with respect to ransomware incidents, and by accessing the infrastructure used to conduct the attack;

(b) supporting Members States, and where relevant private parties, in addressing online crisis situations, in particular by providing private parties with the information necessary to identify relevant online content, services, accounts, infrastructures or digital activities, including by means of referrals of online content to online service providers;

(c) supporting Member States in preventing and combating child sexual abuse, the dissemination of online child sexual abuse material and the solicitation of children;

(d) contributing to the identification of victims and offenders of cybercrime and cyber-enabled criminal activities, including online child sexual abuse;

(e) maintaining and deploying specialised digital forensic, technical, analytical and investigative expertise and capabilities, including to support the processing and analysis of digital data and lawfully obtained encrypted data;

(f) hosting and supporting operational coordination platforms and specialised operational cooperation frameworks in the area of cybercrime and cross-border access to electronic evidence, including the Joint Cybercrime Action Taskforce.

Article 16

European Financial and Economic Crime Centre

In accordance with Article 6(1), point (b), the support provided by Europol, notably through the European Financial and Economic Crime Centre, shall, in particular, consist of:

(a) supporting the asset recovery offices of Member States in the tracing and identification of instrumentalities, proceeds, and properties, which are, or might become, the object of a freezing or confiscation order, in accordance with Article 9;

(b) supporting the detection, analysis and monitoring of criminal financial flows, illicit financial networks and criminal business models linked to organised crime and terrorism financing;

(c) providing operational and analytical support to the EPPO in relation to crimes falling within the competence of Europol and the EPPO in accordance with Article 81;

(d) supporting Member States in tackling large-scale digital fraud, including by facilitating reporting of fraud and cooperating with financial institutions, online platforms, and international partners.

Article 17

European Centre Against Migrant Smuggling

In accordance with Article 6(1), point (b), the support provided by Europol, notably through the European Centre Against Migrant Smuggling, shall, in particular, consist of:

(a) supporting the identification, monitoring and analysis of criminal networks involved in migrant smuggling and trafficking in human beings, including their business models, *modi operandi* and criminal infrastructure;

(b) supporting the detection and analysis of the digital dimension of migrant smuggling and trafficking in human beings, including through open-source analysis, cooperation with online service providers and specialised practitioner networks;

(c) supporting the detection, analysis and disruption of illicit financial flows, criminal assets and financial infrastructure used by migrant smuggling and trafficking in human beings networks, in close cooperation with the European Financial and Economic Crime Centre;

(d) supporting cooperation and operational coordination with Member States, Frontex, Eurojust, other relevant Union bodies, offices and agencies, third countries and international partners in matters relating to migrant smuggling and trafficking in human beings.

Article 18

European Counter Terrorism Centre

In accordance with Article 6(1), point (d), the support provided by Europol, notably through the European Counter Terrorism Centre shall, in particular, consist of:

(a) addressing the dissemination of terrorist and violent extremist content online including by cooperating with the competent authorities of the Member States with regard to removal orders, in accordance with Article 14 of Regulation (EU) 2021/784, and by making referrals of online content to online service providers;

(b) supporting investigations, including through the detection and analysis of terrorist financing flows and networks, threats related to chemical, biological, radiological and nuclear substances and explosives, online radicalisation and the misuse of online platforms for terrorist and new technologies for terrorist purposes;

(c) supporting crisis response and operational coordination, including in online crisis situations, through dedicated capabilities, tools, joint coordination structures and support mechanisms, including through the information exchange mechanism referred to in Article 47;

(d) supporting the prevention of radicalisation that leads to terrorism by facilitating the exchange of information, criminal intelligence and analytical products, between the competent authorities of the Member States and, where appropriate, with relevant Union bodies, offices and agencies and private parties.

Article 19

Establishment and governance of additional Union Centres of specialised expertise

1. Additional Union Centres of specialised expertise may be established within Europol, in particular where the Executive Director identifies a need for permanent specialised capabilities or coordinated action at Union level in order to fulfil Europol's tasks.

2. The establishment, adaptation and, where appropriate, merger and discontinuation of the additional Centres shall be decided by means of delegated acts adopted in accordance with Article 139 taking into account, in particular:

   (a) the scale, complexity or cross-border dimension of the relevant criminal or security threats and of criminal offences related to the forms of crime listed in Annex I where such offences involve a hybrid dimension;

   (b) the operational needs of the Member States and the need for permanent specialised capabilities at Union level;

   (c) the need to ensure coherence, and complementarity with existing Centres and other Union operational frameworks;

   (d) the availability of resources within Europol.

3. Article 13(2) to (6) shall apply to the Centres established under this Article.

SECTION 3
OPERATIONAL COOPERATION INSTRUMENTS

Article 20

Operational task forces

1. Operational task forces may be established by the competent authorities of the Member States, with the support of Europol, for the purpose of addressing specific cross-border criminal threats falling within the scope of Europol's competence.

   An operational task force may be established where the criminal threat concerned involves two or more Member States and, by reason of its scale, complexity or cross-border dimension, requires coordinated operational and investigative action at Union level.

2. The Member States participating in an operational task force and Europol shall ensure coherence and, where possible, integration with the framework of EMPACT.

3. The Member States setting up an operational task force may decide to invite other Member States, and third countries referred to in Chapter VII to participate in or support the operational task force.

4. Europol shall, in agreement with the Member States participating in an operational task force, support the planning, coordination and implementation of the operational and criminal intelligence activities carried out in the framework of that task force.

   Europol shall make available the relevant operational and financial support.

5. Member States participating in an operational task force shall, in accordance with national law:

   (a) ensure the continuous and structured exchange of all relevant information with Europol and the other participating Member States in a timely manner, through the Secure Information Exchange Network Application (SIENA), and, where appropriate, ensure that such information is made available for direct access in accordance with Articles 39, 40 and 41;

   (b) make effective use of the operational and financial support provided by Europol;

   (c) undertake, where necessary and in accordance with national law, coordinated criminal intelligence activities and investigations to address the criminal threats concerned;

   (d) initiate parallel financial investigations to identify, freeze and seize criminal assets;

   (e) mobilise, where relevant, liaison officers deployed in third countries where criminal activities are investigated in the context of the operational task force to enhance cooperation and information sharing and provide Europol with the information obtained.

6. The Executive Director shall propose to the competent authorities of the Member States concerned via the Europol national unit the establishment of an operational task force where, on the basis of objective criteria, such a task force would provide added value in addressing a specific cross-border criminal threat falling within the scope of Europol's competence and respond to identified operational needs.

7. The Management Board shall adopt implementing rules for the setting up and implementation of operational task forces, including the necessary safeguards for the participation of third countries.

8. Europol shall, together with the Member States participating in an operational task force, assess at all stages of the operational activities whether the establishment of a

joint investigation team in accordance with Article 21 is necessary to support coordinated and sustained action at Union level.

Article 21

Participation in joint investigation teams

1. Europol may participate in the activities of joint investigation teams, including those established in accordance with Council Framework Decision 2002/465/JHA[65] and the Convention established by the Council in accordance with Article 34 of the TEU, on Mutual Assistance in Criminal Matters between the Member States of the European Union[66], dealing with forms of crime falling within the scope of Europol's competence. The agreement setting up a joint investigation team shall determine the conditions relating to the participation of Europol in the team and shall include information on the rules on liability.

2. Europol may, within the limits of the laws of the Member States in which a joint investigation team is operating, assist in all activities and exchanges of information with all members of the joint investigation team.

3. When participating in a joint investigation team, Europol may, in accordance with this Regulation, provide all members of the team with necessary information processed by Europol for the purposes set out in Article 32(2). Europol shall at the same time inform the Europol national units of the Member States represented in the team, and those of the Member States which provided the information.

4. Europol may process, for the purposes set out in Article 32(2), information obtained while participating in a joint investigation team with the consent of the Member State which provided the information, under the conditions laid down in this Regulation.

5. Where Europol has reason to believe that setting up a joint investigation team would add value to an investigation, it may propose that to the Member States concerned and take measures to assist them in setting up the joint investigation team.

6. Upon a request made the competent authority of a Member States made following the advice of Eurojust pursuant to Article 27(1) of Regulation (EU) …/… *[proposal for Eurojust Regulation]*, Europol shall, within the limits of its competence, participate in the joint investigation team concerned, unless it provides duly justified reasons for not doing so.

Article 22

Europol deployments

1. A Member State may request, in accordance with its national law, Europol deployments on its territory to make use of the operational support provided by Europol.

2. Europol deployments for operational support shall take place, in particular, in the context of complex or large-scale investigations or criminal intelligence activities requiring coordinated support at Union level. Europol deployments may include participation in joint investigation teams established in accordance with Article 21, in

---

65 Council Framework Decision of 13 June 2002 on joint investigation teams (OJ L 162, 20.6.2002, p. 1, ELI: http://data.europa.eu/eli/dec_framw/2002/465/oj).

66 OJ C 197, 12.7.2000, p. 3.

operational task forces established in accordance with Article 20, or in other coordinated operational activities.

Europol deployments may also take place to support checks against relevant databases, including in the context of strengthening controls at the Union's external borders or supporting migration management activities in accordance with Regulation (EU) 2019/1896, or to support Member States in major international events.

Europol deployments shall also take place, in particular, to ensure the effective use, integration and deployment of Europol's services, tools and advanced capabilities in the operational environments of the Member States.

3. Europol shall assess any request made by a Member State pursuant to paragraph 1 and may authorise a Europol deployment, taking into account Europol's available resources.

4. Following authorisation of a Europol deployment pursuant to paragraph 3, Europol and the Member State concerned shall agree on the modalities of the Europol deployment.

5. Europol staff and seconded national experts deployed in the territory of the Member State concerned shall act in accordance with this Regulation and with the national law of the Member State in whose territory the deployment takes place.

6. The Member State in whose territory the deployment takes place shall, in accordance with the modalities agreed pursuant to paragraph 4:

   (a) provide Europol with all relevant information without undue delay and, where possible, enable direct access to such information for Europol deployments, in accordance with national law;

   (b) allow Europol deployments to be present during the execution of investigative measures, in accordance with national law;

   (c) facilitate the mobilisation of specialised expertise, including analytical, digital forensic, IT and system-integration expertise;

   (d) take the necessary measures, in accordance with national law, to ensure that the outputs produced through the operational support provided by Europol deployments may be used as evidence in national investigative and judicial proceedings, including by ensuring such outputs are generated, documented and transmitted in a manner compatible with the requirements of national law.

7. The Executive Director may propose to the competent authorities of a Member State, via the Europol support office, a Europol deployment where he or she considers that such deployment would provide added value in preventing or combating forms of crime falling within the scope of Europol's competence.

8. Where a third country, with whom Europol has established cooperative relations pursuant to this Regulation or Regulation (EU) 2018/1725, requests Europol deployments on its territory pursuant to this Article, the requirements and the procedure set out in paragraphs 2, 3 and 4 of this Article shall apply, in accordance with the implementing rules referred to in paragraph 9 of this Article.

9. Upon a proposal from the Executive Director, the Management Board shall adopt implementing rules on the preparation and implementation of Europol deployments.

Article 23

Europol support to EMPACT

1. For the purpose of supporting Member States in further strengthening the EMPACT as a coherent framework to prevent and combat the threats posed by criminal networks at Union level, Europol shall provide administrative, logistical, financial and operational support to operational and strategic activities carried out by Member States and third countries, including related exchange of information, as well as to third countries participating in such activities.

   In that regard, Europol shall complement the coordination functions carried out at national level by Europol national units.

2. For the purposes of paragraph 1, Europol, through the EMPACT Support Team, shall, in particular:

   (a) support the development and implementation of biennial operational action plans, including by assisting in the definition of operational priorities, targets and deliverables;

   (b) facilitate the meetings of the National EMPACT Coordinators;

   (c) support the preparation and management of operational action plans;

   (d) support the involvement of third countries in EMPACT, notably EU candidate countries and potential candidates.

3. In carrying out the support referred to in paragraph 2, Europol shall, through the EMPACT Support Team, cooperate closely with Europol national units, the National EMPACT Coordinators, and with other relevant Union bodies, offices and agencies involved in EMPACT, and, where appropriate, with third countries and other partners in accordance with this Regulation.

Article 24

Use of operational and technical pools

1. Europol shall establish and maintain specialised operational and technical pools composed of experts designated by the Member States in order to ensure the availability of highly specialised expertise necessary for the fulfilment of Europol's tasks and to support Member States.

2. Member States shall designate experts for inclusion in the specialised operational and technical pools referred to in paragraph 1, in accordance with the profiles and participation requirements determined by the Management Board, in order to ensure the availability of specialised expertise. The designation of an expert to a pool shall not affect the employment relationship between that expert and the competent authority of the Member State concerned.

3. Experts participating in the pools may, with the agreement of the competent authority of the Member State concerned, be seconded to Europol.

4. Europol may provide financial support to Member States in connection with the training and secondment of experts participating in the pools.

5. Upon a proposal from the Executive Director, the Management Board shall adopt implementing rules on the operation of the pools, including the modalities for the

secondment of experts, the organisation of training, and the provision of financial support referred to in paragraph 4.

SECTION 4
NATIONAL STRUCTURES FOR OPERATIONAL COOPERATION

Article 25

Europol national units

1. The Member States and Europol shall cooperate with each other in the fulfilment of their respective tasks set out in this Regulation.

2. Each Member State shall establish or designate a Europol national unit.

   The Europol national unit shall be the liaison body and central coordination point between Europol and the competent authorities of the Member State. Each Member State shall ensure its Europol national unit is able to fulfil the tasks assigned to it under this Regulation and, in particular, that it has access to national law enforcement data and other relevant data necessary for cooperation with Europol.

3. Europol national units shall ensure the strategic coordination at national level of the competent authorities of the Member States whose activities fall within the scope of Europol's competence, for the purposes of cooperation with Europol.

   For that purpose, the Europol national units shall, in particular:

   (a) identify, consolidate and communicate to Europol the operational priorities and capability needs of the competent authorities of the Member State, including in the context of the Framework referred to in Article 57;

   (b) coordinate national contributions to Europol's strategic and analytical activities;

   (c) support the alignment of national priorities with Union priorities for preventing and combating the forms of crime falling within the scope of Europol's competence.

4. The heads of the Europol national units shall meet on a regular basis to coordinate strategic priorities for cooperation with Europol and to identify common operational priorities and capability needs.

5. Europol national units shall facilitate the information exchange between Europol and the competent authorities of their Member States. For that purpose, Europol national units shall:

   (a) receive from Europol any information exchanged in the course of direct contacts between Europol and the competent authorities of their Member States, unless the Europol national unit indicates that it does not need to receive such information;

   (b) have access to national law enforcement data and other relevant data necessary for cooperation with Europol;

   (c) contribute to the fulfilment of tasks assigned to the competent authorities of the Member States in relation to their obligations on information exchange with Europol, in accordance with Chapter III.

6. The Europol national unit shall ensure the appropriate uptake by Member States of Europol's operational support, including by facilitating the integration of Europol support and tools in national investigations and the participation of the competent authorities of the Member State in operational activities coordinated, organised or supported by Europol, including operational task forces and Europol deployments.

For the purposes referred to in the first subparagraph, the Europol national unit shall include a Europol support office, established in accordance with Article 26.

7. Europol national units shall ensure the coordination at national level of activities carried out in the framework of the EMPACT, including by supporting the EMPACT National Coordinator in the planning and implementation of EMPACT activities and facilitating the involvement of competent authorities of the Member State.

For the purposes referred to in the first subparagraph, the Europol national unit shall include an EMPACT support team.

Each Member State setting up or participating in an EMPACT operational action supported by Europol shall, whenever feasible, use SIENA to provide all relevant information without delay to Europol and to other Member States.

8. The costs incurred by Europol national units in communications with Europol shall be borne by the Member States and, with the exception of the costs of connection, shall not be charged to Europol.

Europol shall support the functioning and capacity of Europol national units, including their support functions.

Such support shall include financial contributions to Europol national units, provided for in accordance with the rules adopted pursuant to Article 124.

Article 26

Europol support offices

1. Member States shall establish a Europol support office within the Europol national unit to ensure appropriate uptake by Member States of Europol's support.

2. Europol support offices shall, as appropriate:

(a) facilitate the use and integration of Europol's operational support, analytical products and expertise by the competent authorities of the Member State;

(b) support the preparation, conduct and follow-up of operational activities supported by Europol, including operational task forces and Europol deployments;

(c) facilitate the mobilisation of specialised capabilities for investigations at national level.

3. Europol support offices shall be composed of seconded Europol staff with prior experience in the competent authorities of the Member State in which the Europol support office is established. That staff shall operate under the responsibility of Europol and the Member State where the Europol support office is established, in accordance with the implementing rules referred to in paragraph 4.

4. Upon a proposal from the Executive Director, the Management Board shall adopt implementing rules governing the establishment, organisation and functioning of Europol support offices, including the minimum requirements to be fulfilled by

Europol staff seconded to such offices, the arrangements governing their secondment and the allocation of responsibilities between Europol and the Member State in which the Europol support office is established.

Article 27

Liaison officers

1. Each Europol national unit shall designate at least one liaison officer to be attached to Europol.

   Except as otherwise laid down in this Regulation, the liaison officers shall be subject to the national law of the designating Member State.

2. Liaison officers shall constitute the national liaison bureaux at Europol and shall be instructed by their Europol national units to represent the interests of the Member State they represent within Europol in accordance with the national law of the designating Member State and the provisions applicable to the administration of Europol.

3. Liaison officers shall support the effective integration of Europol's support into national operational activities.

   For that purpose, liaison officers shall, in coordination with Europol, contribute to the delivery of support tailored to the operational needs and requirements of their Member State.

4. Liaison officers shall assist in the exchange of information between Europol and the Member States.

5. Liaison officers shall, in accordance with the national law, assist in the exchange of information between Member States and the liaison officers of other Member States, third countries and international organisations.

   Europol's infrastructure may be used, in accordance with national law, for such bilateral exchanges also to cover forms of crime falling outside the scope of Europol's competence. All such exchanges of information shall be in accordance with applicable Union and national law.

6. Through the exchange of information referred to in paragraph 5, liaison officers shall support the identification of operational links and the coordination of cross-border operational and investigative responses, in close cooperation with the Operational and Analysis Service.

7. The Management Board shall determine the rights and obligations of liaison officers in relation to Europol. Liaison officers shall enjoy the privileges and immunities necessary for the performance of their tasks in accordance with Article 125(2).

8. Europol shall ensure that liaison officers are fully informed of and associated with all of its activities, in so far as necessary for the performance of their tasks.

9. Europol shall cover the costs of providing Member States with the necessary premises within the Europol's headquarters and adequate support for liaison officers to perform their duties. All other costs that arise in connection with the designation of liaison officers shall be borne by the designating Member State, including the costs of equipment for liaison officers.

Chapter III
Information management

SECTION 1
HORIZONTAL RULES ON DATA PROCESSING

Article 28

Sources of information

1. Europol shall only process information that has been provided to it:
   (a) by Member States in accordance with their national law and Article 29;
   (b) by Union institutions, bodies, missions, offices and agencies, third countries and international organisations;
   (c) by private parties and natural persons.
2. Europol may directly retrieve and process information, including personal data, from publicly available sources, including the internet and public data.
3. In so far as Europol is entitled under Union, international or national legal instruments to gain access to data from Union, international or national information systems, it may retrieve and process information, including personal data, by such means if and to the extent that is necessary for the performance of its tasks. The applicable provisions of such Union, international or national legal instruments shall govern access to, and the use of, that information by Europol, in so far as they provide for stricter rules on access and use than those laid down by this Regulation. Access to such information systems shall be granted only to duly authorised staff and only in so far as this is necessary and proportionate for the performance of their tasks.

Article 29

Provision of information by Member States

1. Member States shall provide Europol in a timely manner with the information necessary for it to carry out its tasks.
2. Member States shall ensure the effective participation of the competent authorities of the Member States in the information exchange and operational data management frameworks established under this Regulation and shall, where appropriate, enable the structured, automated and interoperable provision of information to Europol in accordance with applicable Union and national law.
3. Immigration liaison officers designated by competent authorities of the Member States shall provide Europol with relevant information through the information exchange frameworks established under this Regulation, using SIENA. Where this is not possible due to legal, organisational or technical reasons, Member States shall ensure that the relevant information is transmitted to Europol through other secure channels by the competent authorities of the Member States concerned.
4. In accordance with Article 107, the Europol national unit and the competent authorities of the Member State concerned shall be responsible for ensuring

compliance with national law when providing information to Europol, and for ensuring, to the extent possible, the completeness, accuracy and timeliness of such information.

5. Without affecting the discharge by Member States of their responsibilities with regard to the maintenance of law and order and the safeguarding of internal security, Member States may refuse to supply information based on one or more of the following grounds:

   (a) the supply of information is contrary to the essential interests of the security of the Member State concerned;

   (b) the supply of information jeopardises the success of an ongoing investigation or the safety of an individual;

   (c) the supply of information would disclose information relating to organisations or specific intelligence activities in the field of national security.

   Member States shall supply information as soon as the grounds referred to in the first subparagraph, points (a), (b) or (c), cease to exist.

6. Europol shall produce an annual assessment of the information provided by Member States under this Article on the basis of quantitative and qualitative criteria defined by the Management Board. The assessment shall be transmitted to the European Parliament, the Council, the Commission and national parliaments.

Article 30

Europol's role in relation to the Schengen Information System

1. Europol shall, through the SIRENE Office, ensure the exchange and availability of supplementary information, in accordance with Regulations (EU) 2018/1860[67], (EU) 2018/1861[68] and (EU) 2018/1862[69] of the European Parliament and the Council.

2. Europol shall support Member States, upon request of the alert issuing Member State, by facilitating the crosschecking and analysis of alert data and supplementary information against information stored at Europol, in particular to locate the persons subject to an alert.

3. Europol shall, upon request, forward to Member States information it receives in accordance with Article 35(8) of Regulation (EU) 2018/1861 and in accordance with Article 48(8) of Regulation (EU) 2018/1862 by the exchange of supplementary

---

67 Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals (OJ L 312, 7.12.2018, p. 1, ELI: http://data.europa.eu/eli/reg/2018/1860/oj).

68 Regulation (EU) 2018/1861 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 border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14, ELI: http://data.europa.eu/eli/reg/2018/1861/oj).

69 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, ELI: http://data.europa.eu/eli/reg/2018/1862/oj).

information, subject to restrictions for processing the information as indicated by the alert issuing Member State.

4. Europol shall support Member States in processing data provided by third countries or international organisations to Europol on persons involved in terrorism or in serious crime.

For such data, Europol shall propose to Member States that information alerts on third-country nationals in the interest of the Union ('information alerts') be entered into the Schengen Information System (SIS), in accordance with Article 37a Regulation (EU) 2018/1862.

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

Europol may transmit to the Member States concerned information relating to hits for the purposes of operational coordination, cross-checking and investigative support, in accordance with Chapter III of this Regulation.

Article 31

Europol's role in relation to the Visa information system and the European travel information and authorisation system

1. Europol shall take all appropriate measures to enable the VIS designated authorities, for the purposes of Regulation (EC) No 767/2008 of the European Parliament and of the Council[70], to have indirect access on the basis of a hit/no-hit system to data provided for the purposes of Article 32(2), point (a) of this Regulation, without affecting any restriction indicated by the provider of the information in accordance with Article 33(2).

2. In the case of a hit pursuant to paragraph 1, Europol shall initiate the procedure by which the information that generated the hit may be shared, in accordance with the decision of the provider of the information to Europol, and only to the extent that the data generating the hit are necessary for the performance of the VIS designated authorities' tasks related to the Visa Information System.

3. Europol shall manage the ETIAS watchlist in accordance with Articles 34 and 35 of Regulation (EU) 2018/1240 of the European Parliament and of the Council[71].

4. Europol may enter data into the ETIAS watchlist related to terrorist offences or other serious criminal offences obtained by Europol, without prejudice to the conditions regulating Europol's international cooperation.

5. Europol shall provide a reasoned opinion following a consultation request referred to in:

---

[70] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60, ELI: http://data.europa.eu/eli/reg/2008/767/oj).

[71] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60, ELI: http://data.europa.eu/eli/reg/2008/767/oj).

(a) Article 29 of Regulation (EU) 2018/1240;

(b) Article 9e(4) of Regulation (EC) No 767/2008;

(c) Article 9g(4) of Regulation (EC) No 767/2008;

(d) Article 22b(14) and (16) of Regulation (EC) No 767/2008.

For the purposes of point (a), Europol may issue a reasoned positive or negative opinion. Europol shall transmit, via SIENA, a report supporting that opinion to the Europol national unit of the Member State responsible for the ETIAS application file. The Europol National Unit shall make that report available to the ETIAS National Unit concerned for the purposes of its assessment and decision-making under Regulation (EU) 2018/1240.

6. For the purpose of carrying out the task referred to in paragraph 3, Europol's Management Board shall, after consulting the European Data Protection Supervisor, adopt the procedures referred to in Article 35 of Regulation (EU) 2018/1240.

7. Europol shall take all appropriate measures to enable the European Border and Coast Guard Agency, within its mandate and for the purposes of Regulation (EU) 2018/1240, to have indirect access on the basis of a hit/no-hit system to data provided for the purposes of Article 32(2), point (a) of this Regulation, without affecting any restriction indicated by the provider of the information in question in accordance with Article 33(2) of this Regulation.

8. In the case of a hit, Europol shall initiate the procedure by which the information that generated the hit may be shared, in accordance with the decision of the provider of the information to Europol, and only to the extent that the data generating the hit are necessary for the performance of the European Border and Coast Guard Agency's tasks related to ETIAS. Paragraphs 2 to 6 of this Article shall apply accordingly.

Article 32

Purposes of information processing activities

1. In so far as is necessary for fulfilling its tasks, Europol may process information, including personal data.

2. Personal data may be processed only for the purposes of:

(a) cross-checking aimed at identifying connections or other relevant links with information related to a criminal offence in respect of which Europol is competent;

(b) analyses of a strategic or thematic nature;

(c) operational analyses;

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

(e) relevant research and innovation projects carried out under the Union Framework Programme for Research and Innovation;

(f) supporting Member States, upon their request, in informing the public about suspects or convicted individuals who are wanted on the basis of a national judicial decision relating to a crime that falls within the scope of Europol's

competence, and facilitating the provision by the public of information on those individuals to the Member States and Europol;

(g) distinguishing between the operational data that relate to the different categories of data subjects listed in Annex II of this Regulation, in accordance with Article 73 of Regulation (EU) 2018/1725.

3. Processing for the purpose of operational analyses as referred to in paragraph 2, point (c), shall be performed by means of operational analysis projects, in respect of which the following specific data protection safeguards shall apply:

(a) for every operational analysis project, the Executive Director shall define the specific purpose, categories of personal data and categories of data subjects, participants, duration of storage and conditions for access, transmission or transfer and use of the data concerned, and shall inform the Management Board and the European Data Protection Supervisor (EDPS) thereof;

(b) personal data may only be collected and processed for the purpose of the specified operational analysis project and stored in the Europol Analytical Environment referred to in Article 40, whereas it becomes apparent that personal data may be relevant for another operational analysis project, further processing of that personal data shall only be permitted insofar as such further processing is necessary and proportionate and the personal data are compatible with the conditions set out in point (a) of this paragraph that apply to the other analysis project;

(c) only authorised staff may access and process the data of the relevant project.

4. Where necessary to achieve the objectives of the research and innovation projects carried out by Europol, the processing of personal data for that purpose shall be in accordance with Article 102.

5. The processing referred to in paragraphs 2 and 3 shall be carried out in compliance with the data protection safeguards provided for in Regulation (EU) 2018/1725 and in this Regulation. Europol shall duly document those processing operations. The documentation shall be made available, upon request, to the Data Protection Officer and to the EDPS for the purpose of verifying the lawfulness of the processing operations.

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

7. Europol may only process personal data outside of the categories of data subjects listed in Annex II where such processing is relevant and necessary for the purposes set out in paragraph 2. Such personal data shall be immediately deleted once the purpose of processing is fulfilled.

8. Where it is not possible to clearly distinguish between the personal data that relate to the different categories of data subjects listed in Annex II, or where Europol has to process personal data outside of the categories of data subjects listed in Annex II, Europol shall inform its Data Protection Officer.

9. Personal data that do not relate to the categories of data subjects listed in Annex II shall be kept functionally separate from other data where applicable and as far as possible, and shall in any case only be processed where necessary and proportionate for the purposes of paragraphs 2.

10. Europol may temporarily process data for the purpose of determining whether the processing of such data is relevant and necessary for Europol to fulfil to its tasks. The time limit for the processing of such data shall not exceed six months from the receipt of those data.

11. The Management Board, after consulting the EDPS, shall, as appropriate, adopt guidelines further specifying procedures for the processing of information for the purposes listed in paragraph 2 of this Article in accordance with Article 72(2), point (t).

Article 33

Determination of the purpose of, and restrictions on, the processing of information by Europol

1. A Member State, a Union institution, body, mission, office or agency, a third country or an international organisation that provides information to Europol shall determine the purpose or purposes for which that information is to be processed, in accordance with Article 32.

   Where a provider of information referred to in the first subparagraph has not complied with that subparagraph, Europol, in agreement with the provider of the information concerned, shall process the information to determine the relevance of such information and the purpose or purposes for which it is to be further processed.

   Europol shall process information for a purpose different from that for which information has been provided only where authorised to do so by the provider of the information.

   Information provided for the purposes referred to in Article 32(2), points (a) to (d), may also be processed by Europol, in accordance with Article 102, for the purpose of Article 32(2), point (e).

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

3. In duly justified cases Europol may assign access restrictions by Member States, Union institutions, bodies, missions, offices and agencies, third countries and international organisations of information retrieved from publicly available sources.

Article 34

Duty to notify Member States

1. Europol shall notify a Member State without delay of any information concerning it. If such information is subject to access restrictions pursuant to Article 33(2) that would prohibit its being shared, Europol shall consult with the provider of the information stipulating the access restriction and seek its authorisation for sharing.

   In such a case, the information shall not be shared without an explicit authorisation by the provider.

2. Irrespective of any access restrictions, Europol shall notify a Member State of any information concerning it where that is necessary in the interest of preventing an imminent threat to life.

In such a case, Europol shall at the same time notify the provider of the information about the sharing of the information and justify its analysis of the situation.

SECTION 2
EUROPOL SERVICES AND TOOLS

Article 35

Europol data environment

1. Europol shall develop and maintain the necessary services and tools enabling it to perform its tasks under this Regulation, and in particular to process information in accordance with Section 1 of this Chapter.

2. Europol services and tools shall consist of interoperable technical components, infrastructures and functionalities enabling Europol to perform its tasks under this Regulation.

3. Europol shall develop, in particular:

   (a) a cross-checking service, for the purposes of Article 32(2), point (a);

   (b) an IT environment for the purposes of Article 32(2);

   (c) SIENA, as the secure information exchange tool for the purposes of Article 32(2), point (d);

   (d) a shared data space for joint operational analysis as referred to in Article 42;

   (e) a platform to facilitate cooperation and exchange of information with private parties as referred to in Article 47.

Article 36

Europol cross-checking service

1. Europol's cross-checking service shall be composed of:

   (a) an infrastructure for the storage of information;

   (b) a search interface, enabling to query and retrieve any relevant information;

   (c) an interface, enabling to upload, update or delete information;

   (d) a secure communication infrastructure between the cross-checking service and Member States, and the Union bodies, offices and agencies that are entitled to use the service;

   (e) a secure communication infrastructure between the cross-checking service and the European Search Portal established by Article 6(2), point (c), of Regulation (EU) 2019/818.

   (f) Europol shall ensure the operational management, security, availability and integrity of the cross-checking service.

2. Member States shall ensure that the case management systems of their single points of contact, of their Europol national units and of the competent authorities of the

Member State are technically connected and interoperable with the Europol cross-checking service.

3. The Commission shall adopt implementing acts laying down the procedures for defining the technical connection between national case management systems and the cross-checking service and the technical connection between that service and other Europol services and tools. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 138(2).

4. Europol shall, when developing and operating the Europol cross-checking service and where appropriate, make use of existing technological components and infrastructures developed and managed by the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA).

Europol shall seek synergies in the design and technical architecture of the cross-checking service, including through the re-use of shared services, communication infrastructures and software components, where that is technically feasible and does not affect the specific purpose, governance or data protection requirements of the cross-checking service as set out in this Regulation and in Regulation (EU) 2018/1726.

For the purposes of biometric matching, Europol shall, where technically feasible, re-use and adapt the technology underpinning the Shared Biometric Matching Service (sBMS), established in Article 12 of Regulation (EU) 2019/818, developed by eu-LISA.

Article 37

Content of the Europol cross-checking service data

1. The Europol cross-checking service shall only contain data relating to:

(a) persons who, in accordance with the national law of the Member State concerned, are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent or who have been convicted of such an offence;

(b) persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences in respect of which Europol is competent;

(c) identifiable objects used in or linked to criminal offences, including documents, vehicles, weapons and other relevant items.

2. Data relating to the persons or objects referred to in paragraph 1 may include:

(a) identity data, including biographical data and biometric data;

(b) criminal intelligence data;

(c) operational data, including data on criminal activities, investigations and connections between cases;

(d) reference data, including national case identifiers and police records references;

(e) data relating to objects used in or linked to criminal offences, including documents, vehicles, weapons and other relevant items.

3. In accordance with this Regulation, the Europol cross-checking service may contain data uploaded by the following entities:

(a) Europol national units established or designated pursuant to Article 25(2);

(b) the competent authorities of the Member States;

(c) Europol, including data provided by third countries, Union institutions, bodies, offices and agencies, private parties and international organisations.

4. The Commission shall adopt implementing acts laying down the technical procedures for the storage of data, including data formats, data quality requirements and rules for cross-checking.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 138(2).

Article 38

Uploading data to Europol cross-checking service

1. Member States shall ensure that their Europol national units and the competent authorities of the Member State, systematically and without undue delay, upload into the Europol cross-checking service any data that:

(a) relates to forms of crime falling within the scope of Europol's competence;

(b) is relevant for cross-border cooperation or where there are factual indications of a possible link to other Member States or third countries.

2. By way of derogation from paragraph 1, competent authorities of the Member States may refrain from uploading data into the Europol cross-checking service on the grounds referred to in Article 29(5).

3. Member States shall ensure that Europol national units and competent authorities of the Member States are equipped with automated technical means ('data loaders') enabling to systematically upload data from their national case management systems to the Europol cross-checking service in accordance with paragraph 1.

4. Europol shall upload, systematically and without undue delay, data to the Europol cross-checking service that fulfil the conditions set out in paragraph 1.

5. Member States and Europol shall ensure that data uploaded into Europol cross-checking service is accurate, up to date and complete, and shall update or delete it where necessary.

6. The Europol cross-checking service shall automatically cross-check any newly uploaded data against data already stored in the service, to identify links between:

(a) persons;

(b) objects;

(c) criminal activities;

(d) investigations conducted in one or more Member States or with third countries.

7. Upon obtaining a positive result from the cross-checking referred to in paragraph 6, the Europol cross-checking service shall generate an alert and notify the relevant entity in accordance with Article 34.

8. The Commission shall adopt implementing acts laying down the technical procedures for the upload of data, including on data formats, and the automated uploading and cross-checking procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 138(2).

Article 39

Querying of and access to Europol cross-checking service data

1. Member States shall be able to query and have access to all information stored in the Europol cross-checking service, in accordance with this Regulation.

2. The Europol cross-checking service shall enable the querying by the Europol national units and the competent authorities of the Member States of the information stored by means of:

   (a) alphanumeric data;

   (b) biometric data;

   (c) multimedia data.

3. Competent authorities of the Member States shall systematically query the Europol cross-checking service with the relevant information:

   (a) when conducting investigations into forms of crime falling within the scope of Europol's competence;

   (b) where there are reasonable grounds to consider that the case has a cross-border or international dimension.

4. Europol shall not have access to the content of the query carried out by the competent authorities of the Member States nor to the results of the query.

5. Europol shall query the Europol cross-checking service to carry out its tasks set out in this Regulation.

6. The Europol cross-checking service may be queried where provided for by other legislative acts of the Union.

7. The result of the query shall include any relevant data stored in the Europol cross-checking service to which the querying entity pursuant to paragraphs 2 and 4 of this Article has access in accordance with any restriction indicated pursuant to Article 33(2).

8. The Commission shall adopt implementing acts laying down the technical procedures for the querying of data, including on data formats. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 138(2).

Article 40

The Europol Analytical Environment

1. Europol shall develop and maintain the technical and operational environment for the storage, processing, cross-checking, visualisation and analysis of data, including in support of criminal investigations and operational coordination (Europol Analytical Environment).

2. Europol Analytical Environment shall comprise analytical workspaces, case management functionalities, collaborative tools, data processing services and other capabilities necessary to support Europol's analytical activities and cooperation with Member States and other authorised partners and to respond to operational, technical or analytical needs identified in the context of its activities.

3. The Europol Analytical Environment shall provide for logically separated analysis projects for storing and processing data for distinct analytical purposes, as referred to in Article 32(3).

4. Europol shall ensure the operational management, security, availability and integrity of the Europol Analytical Environment.

Article 41

Query of and access to Europol Analytical Environment data

1. The Europol Analytical Environment shall enable the querying by the Europol national units and the competent authorities of the Member States of the data stored to find connections with existing cases by means of:

   (a) alphanumeric data;

   (b) biometric data;

   (c) multimedia data.

2. Europol shall query the Europol Analytical Environment to carry out its tasks, including biometric data for the purpose of uniquely identifying a natural person.

3. Europol national units and competent authorities of the Member States, including in the context of a JOAC, querying the Europol Analytical Environment shall only have indirect access to the results of such query, on a hit / no-hit basis. In the case of a hit, Europol shall initiate the procedure by which the information that generated the hit may be shared with the querying entity, in accordance with Article 34.

4. Union information systems may also query the Europol Analytical Environment where provided for by other legislative act of the Union.

   (a) alphanumeric data;

   (b) biometric data;

   (c) multimedia data.

5. Europol shall query the Europol Analytical Environment to carry out its tasks, including biometric data for the purpose of uniquely identifying a natural person.

6. Europol national units and competent authorities of the Member States, including in the context of a JOAC, querying the Europol Analytical Environment shall only have indirect access to the results of such query, on a hit / no-hit basis. In the case of a hit, Europol shall initiate the procedure by which the information that generated the hit may be shared with the querying entity, in accordance with Article 34.

7. Any restriction on access to, use or storage of data in the Europol Analytical Environment shall comply with this Regulation, in particular Articles 33 and 101.

Article 42

Police Shared Data Space establishment

1. Europol shall develop and maintain a service which enables Europol national units and competent authorities of the Member States to open JOACs ('Police Shared Data Space').

2. The Police Shared Data Space shall be based on the Europol cloud infrastructure referred to in Article 50.

3. The Police Shared Data Space shall, to the extent technically possible, share and re-use the hardware and software components of the Europol Analytical Environment referred to in Article 40.

4. The Police Shared Data Space shall make available the tools, functionalities and modules of that environment, including analytical, data processing and data integration functionalities, to the extent necessary for the conduct of joint operational analysis within JOACs.

5. The Commission shall adopt implementing acts laying down the procedures for defining the necessary functionalities of the Police Shared Data Space and the modalities for ensuring interoperability and availability of the tools and those functionalities. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 138(2).

Article 43

Creation of a Joint Operational Analysis Case

1. Europol national units and competent authorities of the Member States may decide to open a JOAC for carrying out joint operational analysis.

2. The Member State opening the JOAC shall indicate:

   (a) the Member State(s) invited to participate to the JOAC and have access to the relevant data uploaded in the JOAC;

   (b) the third country that may participate to the JOAC and have access to the relevant data uploaded in the JOAC;

   (c) the reasons for involving Centre(s), Member States or third countries into the JOAC.

3. Europol shall have access to the JOAC and, where appropriate, provide analytical support and expertise to the Member States concerned in relation to the JOAC.

4. The participating Member States shall designate representatives of the respective competent authorities of the Member States which will participate to the JOAC and have access to the data processed therein.

5. When the Member State(s) opening the JOAC proposes that a third country should be part of the JOAC, Europol shall be responsible to enable the participation and to give access to the relevant data stored in the Police Shared Data Space to the third country, where the following conditions are met:

   (a) Europol considers it relevant for the third country to participate in the JOAC, including based on the information provided by the Member States opening a JOAC pursuant to point (c) of paragraph 2;

   (b) an agreement enabling the third country to exchange personal data with Europol is in force.

6. The third country authorised to participate to the JOAC shall appoint its participating representatives.

7. Europol shall appoint one or more of its representatives to participate in a JOAC and have access to the information uploaded therein.

Article 44

Europol proposal for the establishment of a Joint Operational Analysis Case

1. Based on the analysis of information and data available to it, Europol may propose to one or more Member States the opening of a JOAC, where it considers that coordinated operational analysis could provide added value in the joint operational analysis of a crime falling within the scope of Europol's competence.

2. Any proposal made pursuant to paragraph 1 shall be non-binding and shall not affect the discretion of the Member States concerned to decide whether to open a JOAC in accordance with Article 43.

3. For the purposes of paragraph 1, Europol may identify and flag relevant information within the Europol Analytical Environment that should be uploaded in the JOAC.

Article 45

Use of a Joint Operational Analysis Case

1. The participants to a JOAC may carry out the following activities within the Police Shared Data Space:

   (a) process information uploaded by the entities opening the JOAC or by any other participating entity;

   (b) upload new data which is deemed relevant for analysis as part of the JOAC, in accordance with Article 33;

   (c) securely communicate and exchange information within the JOAC with other participants, either by chat, video or with other relevant tools supported by the Europol Analytical Environment;

   (d) jointly visualise or edit any documents or reports relevant for the JOAC.

2. Europol and the participating Member States shall ensure that the personal data uploaded in a JOAC, when processed outside of the Police Shared Data Space, is protected through technical and organisational measures in accordance with, Regulation (EU) 2018/1725, with this Regulation and with Directive (EU) 2016/680 of the European Parliament and of the Council[72].

Article 46

Secure Information Exchange Network Application

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

1. SIENA is established for the purpose of facilitating the exchange of information between Member States, Europol, Union institutions, bodies, offices and agencies, third countries and international organisations.

2. SIENA shall be composed of:

   (a) a central infrastructure for the storage and processing of data;

   (b) web interface(s) to exchange information;

   (c) mobile application(s) to exchange information;

   (d) dedicated programming interface(s) for Member States and, where appropriate, Union institutions, bodies, offices or agencies supporting the interoperability with their systems, including their case management systems;

   (e) a secure communication infrastructure between SIENA and Member States, and, where appropriate, the Union institutions, bodies, offices or agencies, third countries and international organisations that are entitled to use SIENA.

3. In accordance with Article 13 of Directive (EU) 2023/977, SIENA shall be the secure communication channel used by the single points of contact and by the competent authorities of the Member States to send requests for information, to provide information pursuant to such requests or to provide information on its or their own initiative including, where applicable, to send a copy of such request or information to Europol. For that purpose, single points of contact and competent authorities of the Member States shall be connected to SIENA, including, where appropriate, through mobile devices.

4. When exchanging information between themselves, SIENA shall provide for the possibility for the single points of contact or competent authorities of the Member States to indicate that a JOAC should be opened in accordance with Article 43.

5. SIENA shall be the default channel of communication to be used by the competent authorities of the Member States to exchange information with Europol.

6. Europol or competent authorities of the Member States may use SIENA to exchange information with third countries whose authorities have been connected to SIENA by Europol, pursuant to working arrangements or international agreements concluded with the Union.

7. The authorities of third countries referred to in paragraph 6 may also use SIENA to exchange information with the authorities of other third countries with whom a working arrangement or international agreement has been concluded.

8. Europol shall ensure the operational management, security, availability and integrity of SIENA.

9. The Commission shall adopt implementing acts laying down the procedures for defining the necessary functionalities of the secure infrastructure referred to in paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 138(2).

Article 47

Information exchange mechanism for cooperation with private parties

1. The Europol Analytical Environment shall include an information exchange mechanism to facilitate cooperation and exchange of information between private parties, Europol and the Member States.

2. The information exchange mechanism shall have, in particular, the following functions:

   (a) facilitate communication between Europol, the Member States and private parties offering services in the Union, including by facilitating reporting or notification obligations under Regulations (EU) 2021/784 and 2022/2065;

   (b) act as a crisis response platform in online crisis situations, in accordance with Article 96 by facilitating communication between Europol, the Member States, private parties and where applicable third countries and by enabling Europol to provide private parties with the information necessary to identify relevant online content, services, accounts, infrastructures or digital activities.

3. The information exchange mechanism shall as a minimum be composed of:

   (a) a central infrastructure for the storage and processing of data;

   (b) web interface(s);

   (c) dedicated programming interface(s) for Member States supporting the interoperability with their national systems, including their case management systems;

   (d) a secure communication infrastructure between Europol, the Member States and private parties.

4. Europol shall establish the procedure and conditions for granting or withdrawing secure access of private parties to the information exchange mechanism.

Article 48

European Police Record Index System

In relation to the European Police Record Index System (EPRIS), Europol shall perform the tasks conferred on it by Regulation (EU) 2024/982.

Article 49

Development of other services and tools

The Commission may adopt implementing acts laying down additional functionalities of existing services and tools or the necessary functionalities of additional services and tools. Those additional functionalities or additional services and tools shall comply with the applicable rules on processing of personal data set out in Regulation (EU) 2018/1725 and this Regulation. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 138(2) of this Regulation.

SECTION 3
TECHNICAL COMPONENTS AND STANDARDISATION

Article 50

Europol cloud infrastructure

1. The Europol cloud infrastructure is established. The Europol cloud infrastructure is a secure and scalable platform of cloud computing services enabling Europol and competent authorities of the Member States to access Europol's tools, collaborative environments and other operational and analytical capabilities in accordance with this Regulation. The Europol cloud infrastructure may also be used by other Union institutions, bodies, offices or agencies, and third countries to access Europol's tools, collaborative environments and other operational and analytical capabilities in accordance with this Regulation.

2. The Europol cloud infrastructure shall support the achievement of the purposes set out in this Regulation in the context of criminal investigations and operational support, including by supporting the storage, processing, analysis and exchange of data, while ensuring strict access control, data compartmentalisation and full compliance with Union law.

3. Europol shall establish, operate and maintain the Europol cloud infrastructure. In establishing, operating and maintaining the Europol cloud infrastructure, Europol shall, where appropriate and technically feasible, make use of existing technical solutions, services and infrastructure components developed or operated by Union institutions, bodies, offices and agencies, including eu-LISA, with a view to ensuring efficiency, interoperability and the optimal use of Union resources.

4. Europol shall ensure that the procurement of cloud computing services complies with applicable Union law, including requirements on the EU cloud sovereignty framework, data security, data protection, cybersecurity and digital sovereignty.

5. Europol systems and tools processing operational data shall be made available to authorities of the Member States from the Europol cloud infrastructure.

6. Europol shall prioritise the development of new systems and tools on the Europol cloud infrastructure.

7. Access to and use of the Europol cloud infrastructure shall be limited to authorised users from competent authorities of the Member States, from third countries, where appropriate, and Europol, in accordance with their respective access rights under this Regulation and subject to appropriate authentication mechanisms, including high-assurance digital identity solutions in accordance with Article 51.

8. Europol shall assess the technical, operational and financial implications of making existing systems and tools available on the Europol cloud infrastructure and submit a reasoned report to the Commission by … [6 months after start date of application of this Regulation].

9. The Commission shall adopt implementing acts defining the requirements relating to security, interoperability, performance and the architecture of the Europol cloud infrastructure. On the basis of the report referred to in paragraph 8, those implementing acts shall also indicate the systems and tools that shall be migrated to the Europol cloud infrastructure. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 138(2).

Article 51

EU Police Digital Identity

1. The EU Police Digital Identity shall constitute the set of rules for the common identification and access management means for each authorised representatives of competent authorities of the Member States or of Union institutions, bodies, offices and agencies to securely access, use and interact with the Europol cloud infrastructure and to national systems connected to the Europol cloud infrastructure. Member States, Europol, Union institutions, bodies, offices and agencies as well as third countries shall ensure that access to the Europol cloud infrastructure and to national systems connected to the Europol cloud infrastructure is granted to their respective representatives in a secure, harmonised and trusted manner, by means of an EU Police Digital Identity.

2. In establishing the EU Police Digital Identity, Europol and the Member States shall, where appropriate and technically feasible, make use of existing Union digital identity solutions and standards, including those established under Regulation (EU) No 910/2014 of the European Parliament and of the Council[73], provided that they meet the operational, security and data protection requirements laid down in this Regulation.

3. Europol shall ensure that any operation carried out in the Europol cloud infrastructure is logged and available for oversight purposes.

4. Member States, Europol, Union institutions, bodies, offices and agencies and third countries shall grant differentiated access rights to services or tools hosted in the Europol cloud infrastructure, commensurate with the roles, responsibilities and access authorisations of the users concerned, in full respect of this Regulation.

5. The Commission shall adopt implementing acts defining the procedures for the establishment of an EU Police Digital Identity referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 138(2).

Article 52

Statistics and reporting tools

1. Europol shall develop, implement and maintain statistics and reporting tools for evaluation, monitoring, analysing and reporting. Those tools shall not allow for the identification of individuals. Those tolls shall allow the entities referred to in paragraph 2, point (a), to obtain customisable reports and statistics.

2. The statistics and reporting tools concerning the use, performance, operational effectiveness and interoperability of the services and tools shall collect, generate and provide aggregated statistical information, indicators, technical logs, usage metrics and analytical reports relating in particular to:

   (a) the use of Europol services and tools by Member States, Europol, Union institutions, bodies, offices or agencies, third countries and international organisations in accordance with this Regulation;

[73] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(b) the exchange, querying, upload, cross-checking and processing of data;

(c) information exchange activities;

(d) the performance, availability and security of the technical infrastructures;

(e) trends, patterns and operational needs relevant for the implementation of this Regulation.

3. Europol, Member States and the Commission shall have access to statistical information and reports generated pursuant to paragraph 2, solely for the purposes of reporting and statistics. Access to that data repository shall be granted by means of secured access through TESTA with control of access and specific user profiles solely for the purpose of reporting and statistics.

4. The statistics and reporting tools shall not be used to take decisions affecting individuals solely on the basis of automated processing and shall not be used for operational analysis concerning identifiable persons.

5. Europol shall ensure that the generation and sharing of statistics pursuant to this Article complies with Union law on data protection, cybersecurity and confidentiality. Statistical information shall, where appropriate, be anonymised or aggregated.

6. The Commission shall adopt implementing acts laying down detailed rules concerning the technical functionalities, access rights, categories of statistics, reporting arrangements and data protection safeguards applicable to the statistics and reporting tools referred to in paragraph 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 138(2).

Article 53

Universal message format

1. Europol shall support the development, implementation and operational use of the universal message format (UMF) standard established under Article 38 of Regulation (EU) 2019/818 for the exchange of information between Member States, eu-LISA and other Union bodies, offices and agencies.

2. Europol shall ensure the provision of the secretariat for the governance of the UMF and shall facilitate and steer discussions of a technical and operational nature with Member States, eu-LISA and other relevant Union agencies.

3. In carrying out its tasks under paragraph 2, Europol shall:

(a) support the further development and updating of the UMF, including data models, semantics and technical specifications;

(b) promote the consistent and interoperable use of the UMF across information systems and communication channels in the area of freedom, security and justice;

(c) assist Member States and Union bodies, offices and agencies in the implementation and practical application of the UMF;

(d) ensure coherence with the relevant requirements of the large-scale IT systems in the area of freedom, security and justice for which eu-LISA is responsible

for the preparation, development or operational management pursuant to Union law.

Article 54

EU DNA matching application

1. Europol shall develop, implement and maintain an EU DNA matching application for the purpose of enabling the secure and reliable comparison of DNA profiles in support of Member States' investigations of criminal offences.
2. The EU DNA matching application shall provide a technical capability allowing for the automated comparison of DNA profiles in accordance with scientifically established matching rules. The application shall replicate the core functionalities of existing DNA matching systems used by Member States and shall support their adaptation to Union legal and technical requirements, including those stemming from Regulation (EU) 2024/982.
3. The use of the EU DNA matching application shall not affect the ownership or control of DNA data.
4. The EU DNA matching application shall be used by the competent authorities of the Member States, Europol and any other Union bodies, offices or agencies on a voluntary basis. Europol shall act solely in a supporting and technical capacity.
5. Europol shall support Member States in the transition from existing DNA matching systems to the EU DNA matching application, including by providing technical guidance, tools and assistance to ensure continuity of operations.
6. Europol shall ensure that appropriate technical and organisational measures are in place to guarantee a high level of security, integrity and confidentiality.

Article 55

Information and Communication Technology and Information Management Steering Group

1. An Information and Communication Technology and Information Management Steering Group (the 'ICT/IM Steering Group') is established.
2. The ICT/IM Steering Group shall be composed of one member representing each Member State, one for the Commission, one for Europol and one for eu-LISA. The Management Board shall appoint the members of the ICT/IM Steering Group. The ICT/IM Steering Group shall include the chair of the ICT/IM Advisory Group established pursuant to Article 56.
3. The Management Board shall adopt the rules of procedure of the ICT/IM Steering Group.
4. The ICT/IM Steering Group shall be chaired by a representative of a Member State appointed by the Management Board.
5. The ICT/IM Steering Group shall support the Management Board for decisions related to Europol ICT and information management activities, in particular with regard to the following:

(a) analytical capabilities;

(b) central systems;

(c) information exchange and communication tools;

(d) technical infrastructure and platforms;

(e) cybersecurity;

(f) interoperability with EU information systems and national systems and databases.

6. The ICT/IM Steering Group shall support and monitor the strategic direction, design, development and implementation of Europol's information management and ICT services, tools and components, including the financial aspects related to information systems and information exchange mechanisms.

7. In particular, the ICT/IM Steering Group shall:

(a) contribute to the definition of Europol strategic multiannual programming of Europol ICT and information management activities including the objectives, the expected results over time, the performance indicators and the multiannual resource planning per information management and ICT services, tools and components;

(b) provide an opinion to the Management Board on Europol ICT and Information Management annual work programmes in accordance with Article 73;

(c) provide an opinion to the Management Board on internal evaluations related to Europol ICT and Information Management activities;

(d) ensure consistency with Member States' operational needs and Union-wide interoperability objectives;

(e) monitor the implementation of major ICT and information management initiatives;

(f) provide opinions and recommendations to the Executive Director and, where appropriate, to the Management Board.

8. The ICT/IM Steering Group shall meet regularly. It shall have no decision-making power and shall not represent the Management Board.

9. Europol shall provide the ICT/IM Steering Group with a secretariat and administrative support.

10. The ICT/IM Advisory Group established pursuant to Article 56 shall provide technical expertise to support the tasks of the ICT/IM Steering Group and shall report regularly to it.

Article 56

ICT and Information Management Advisory Group

1. An Information and Communication Technology and Information Management Advisory Group (the 'ICT/IM Advisory Group') is hereby established.

2. The ICT/IM Advisory Group shall be composed of one expert designated by each Member State, the Commission and eu-LISA for a four-year term, which may be renewed.

3. Representatives of other relevant Union institutions, bodies, offices and agencies may be invited to participate, where appropriate.

4. The ICT/IM Advisory Group shall be chaired by Europol.

5. The ICT/IM Advisory Group shall assist Europol and the ICT/IM Steering Group established pursuant to Article 55 by providing technical expertise on the design, development, implementation and operation of information systems and related communication infrastructure and information exchange mechanisms.

6. In particular, the ICT/IM Advisory Group shall:

   (a) provide technical advice on ICT architecture, data management and interoperability;

   (b) support the preparation and implementation of technical solutions for information exchange;

   (c) contribute to the identification and promotion of common technical components, standards and best practices;

   (d) support coordination between Europol, the Member States and the Commission on technical and implementation-related matters;

   (e) follow and assess the state of preparation and implementation by the Member States, where relevant;

   (f) report regularly to the Information Management Steering Group and provide it with the technical input necessary for the performance of its tasks.

7. The ICT/IM Advisory Group shall meet regularly. It shall have no decision-making power and shall not represent the Steering Group or the Management Board.

8. Europol shall provide the ICT/IM Advisory Group with a secretariat and administrative support.

9. The ICT/IM Advisory Group shall adopt its rules of procedure.

Chapter IV
Technological capabilities and innovation

SECTION 1
CAPABILITY PLANNING, RESEARCH, INNOVATION AND DEVELOPMENT

Article 57

Foresight and Common Capability Development Framework

1. On the basis of strategic analyses, threat assessments, trend reports and situational briefings referred to in Article 7, Europol shall establish a Foresight and Common Capability Development Framework ('the Framework').

2. The Framework shall support the identification of immediate, emerging and longer-term capability needs at Union level for preventing and combating the forms of crime falling within the scope of Europol's competence.

   The Framework shall identify:

   (a) common capability gaps, challenges and critical dependencies;

(b) key research themes and priorities for research, innovation and capability development activities in which Europol participates or could participate;

(c) emerging developments and technologies relevant to the identified priority capabilities;

(d) needs and opportunities for interoperability, standardisation and common capability development at Union level.

3. On the basis of the Framework, Europol shall support Member States and the Commission, in particular by:

(a) contributing to research, innovation, and capability development activities;

(b) supporting interoperability and standardisation processes, in cooperation with ENISA where appropriate, including the development and promotion of common standards, interoperability requirements, and operational and technical specifications relevant for law enforcement cooperation;

(c) providing, where relevant in cooperation with Union institutions, bodies, offices and agencies advice and capability development support;

(d) facilitating the pooling, sharing and joint procurement of capabilities, including technical resources and equipment, knowledge and expertise between Member States, including in cooperation with relevant Union institutions, bodies, offices and agencies and through the specialised training referred to in Article 64.

4. For the purposes of establishing and updating the Framework referred to in paragraph 1, Member States shall provide Europol, on an annual basis, with information on national research and innovation activities, including relevant investments, and on their participation in Union-funded and nationally funded research and innovation projects, relevant to Europol's competence.

5. The Framework shall form part of Europol's multiannual programming referred to in Article 73 and shall be adopted by the Management Board on the basis of a proposal from Europol after consultation of the Commission.

The Framework shall be regularly reviewed and, where necessary, updated. Europol shall report, in the annual work programmes referred to in Article 73 on the implementation of the Framework, including on the follow-up given to the capability needs identified therein.

Europol shall consult the Capabilities and Innovation Advisory Group established pursuant to Article 65 in the preparation and regularly reviewing and updating of the Framework.

Article 58

Europol's role in Union funding programmes supporting research, innovation and capability development

1. Europol may assist the Commission in the programming of Union funding programmes supporting research, innovation and capability development relevant to Europol's competences.

2. Europol may participate in activities supported under relevant Union funding programmes for the development, uptake, deployment, scaling and integration of

innovative solutions and advanced capabilities, where such participation is necessary for Europol to fulfil its tasks.

3. In accordance with the applicable rules, the Commission and Europol shall take all necessary measures to avoid conflicts of interest and ensure a clear separation between Europol's roles referred to in paragraphs 1 and 2.

Article 59

Advanced capabilities

1. Europol shall develop, operate, host and provide advanced capabilities, including systems, services, analytical environments, infrastructure, tools, technical components and platforms necessary for the performance of its tasks.

2. Europol may undertake such activities on its own initiative or at the request of at least three Member States pursuant to paragraph 3.

3. Before developing a new advanced capability pursuant to paragraph 1, Europol shall assess:

   (a) whether equivalent capabilities are already available on the market or have been developed or acquired by Union institutions, bodies, offices and agencies or Member States;

   (b) whether reliance on suppliers outside the Union would create risks to the Union's security interests or technological resilience;

   (c) the availability of resources, taking into account the capability development priorities identified in the Framework referred to in Article 57.

   Where Europol concludes that equivalent advanced capabilities are already available, it shall, where appropriate, prioritise the reuse, adaptation, interoperability, scaling or acquisition of such capabilities.

   Where Europol concludes that the development of the advanced capabilities requested by at least three Member States is necessary and feasible, it shall develop, operate and host such capabilities.

4. The development, operation, hosting or provision of the advanced capabilities referred to in paragraph 1 shall not affect the responsibility of the requesting Member States for compliance with their obligations under Union and national law, including obligations related to data protection and cybersecurity.

5. Europol shall support Member States in the development, deployment, integration and interoperability of shared advanced capabilities, including by making available shared infrastructure, technical services and secure technological environments.

6. The advanced capabilities referred to in paragraph 1 and the shared infrastructure, technical services and secure technological environments referred to in paragraph 4 shall, where technically feasible, be integrated into the Police Shared Data Space referred to in Article 42.

7. In the context of an investigation or operational activity supported by Europol, Europol may make the advanced capabilities referred to in paragraph 1 available to a participating third country where such use is necessary for the effective conduct of that investigation or activity.

Article 60

Research and innovation

Europol may carry out and participate in research and innovation activities, including pilot projects and preparatory actions, where necessary for the performance of its tasks under this Regulation, in particular for the development of innovative solutions for advanced capabilities intended for use by the competent authorities of the Member States.

Article 61

Testing environments and regulatory sandboxes

1. Europol may make use of the separate, isolated and protected processing environment referred to in Article 102(2), point (c)(i), for the development, substantial modification, testing and validation of algorithmic tools, AI systems and models and other advanced technologies and, where relevant, for the training of such systems.

2. Where AI systems or AI models developed or substantially modified in the context of Europol's research and innovation activities constitute high-risk AI systems within the meaning of Regulation (EU) 2024/1689, Europol shall ensure that the environment referred to in paragraph 1 complies, as applicable with the requirements governing AI regulatory sandboxes laid down in Article 57 of that Regulation.

3. Europol may make the environment referred to in paragraph 1 available to private parties participating in research and innovation activities carried out by Europol or in which Europol participates, subject to appropriate technical, organisational, security and data protection safeguards.

4. Europol may also participate in regulatory sandboxes for AI systems and models established in accordance with Article 57 of Regulation (EU) 2024/1689 including regulatory sandboxes established by the European Data Protection Supervisor.

Article 62

Early deployment, operational testing and validation of innovative solutions

1. Europol may support the early deployment, operational testing and validation of innovative solutions for advanced capabilities, including commercial solutions, taking into account the Framework referred to in Article 57.

2. Where Europol participates in research and innovation activities pursuant to Article 60, it shall assess the potential operational use of resulting innovative solutions and, where appropriate, support their early deployment, operational testing and validation for use by the competent authorities of the Member States.

   Where Europol concludes that such support is necessary and feasible, taking into account available resources and the Framework referred to in Article 57, it shall provide such support in accordance with this Article.

Article 63

Uptake, deployment, scaling and integration of advanced capabilities

1. Europol shall support the uptake, deployment, scaling and integration of advanced capabilities, in particular those resulting from the research and innovation activities

referred to in Article 60, into operational activities and investigations of competent authorities of the Member States, in accordance with applicable Union and national law.

2. For the purpose of paragraph 1, Europol shall cooperate closely with Member States to facilitate the effective use and integration of advanced capabilities in national operational environments, in particular through the Centres, Europol deployments and Europol support offices, as appropriate.

Article 64

Specialised training

1. Europol shall support Member States in strengthening specialised expertise and ensuring the effective deployment and use of the shared advanced capabilities developed, hosted, operated or provided under this Regulation, including through specialised training activities on:

   (a) advanced operational, analytical, technical and forensic methods relevant to criminal investigations;

   (b) capabilities relating to emerging technologies, including artificial intelligence, digital investigations, open-source intelligence and the decryption and processing of data;

   (c) operational methodologies relevant for cross-border law enforcement cooperation, including crime prevention methods and investigative procedures.

2. Europol shall also provide specialised expertise and training where common operational or capability needs identified under the Framework require coordinated support at Union level.

3. Europol shall carry out the activities referred to in paragraphs 1 and 2 in close cooperation with the European Union Agency for Law Enforcement Training (CEPOL) including in relation to the specialised training activities carried out through centres of excellence coordinated by CEPOL.

SECTION 2
COOPERATION AND COLLABORATION ON CAPABILITIES AND INNOVATION

Article 65

Capabilities and Innovation Service

1. Europol shall maintain a Capabilities and Innovation Service to coordinate Europol's activities in the fields of foresight, research, innovation and capability development.

2. The Capabilities and Innovation Service shall, in particular:

   (a) coordinate the preparation, implementation, review and updating of the Framework referred to in Article 57;

   (b) coordinate and carry out research, innovation and capability development activities carried out by Europol, including within the Centres, and steer the development and evolution of Europol's services, tools and technical capabilities established under this Regulation;

(c) support Member States in the development, testing, validation, uptake, deployment, scaling and integration of advanced capabilities, including by facilitating interoperability, standardisation and their consistent use across Member States;

(d) contribute to Union-level cooperation and coordination between Member States, Union institutions, bodies, offices and agencies and, where appropriate, other relevant stakeholders in the fields of research, innovation and capability development relevant to Europol's competence.

(e) disseminate, in accordance with Article 129, the results of research, innovation and capability development activities carried out pursuant to this Regulation.

Article 66

Collaborative arrangements for innovation and capability development

1. Europol may establish and participate in collaborative arrangements, cooperation networks and other innovation initiatives with Union institutions, bodies, offices and agencies, and competent authorities of the Member States.

   For the purpose of the collaborative arrangements referred to in the first subparagraph, Europol may establish and participate in innovation partnerships, pre-commercial procurements and other innovation and capability development activities with relevant private parties, including research organisations, academia, technology providers, industry, small and medium-sized enterprises, start-ups and innovation actors, subject to appropriate data protection and security safeguards and without prejudice to applicable Union law.

2. Europol shall regularly inform and consult the Capability and Innovation Advisory Group established pursuant to Article 67 regarding the activities carried out under this Article.

Article 67

Capabilities and Innovation Advisory Group

1. A Capabilities and Innovation Advisory Group (the 'Innovation Advisory Group') is hereby established.

2. The Innovation Advisory Group shall be composed of one expert designated by each Member States and one expert designated by the Commission.

   ENISA, ECCC, Frontex, eu-LISA and Eurojust may each appoint a representative to the Innovation Advisory Group.

3. Europol may invite representatives of other relevant Union bodies, agencies and offices and private parties to participate, where appropriate.

4. The Advisory Group shall assist Europol by providing technical expertise on research, innovation and capability development activities, in particular in relation to the preparation, review and regular updating of the Framework referred to in Article 57.

   For that purpose, the Innovation Advisory Group shall:

(a) enable participants to exchange on ongoing and planned capability development and innovation activities carried out at Union and national level that may have a relevance for the Framework;

(b) support consistency, complementarity and coordination between research, innovation and capability development activities carried out pursuant to this Regulation and related national and Union-level initiatives;

(c) support structured engagement with private parties for capability development, testing and innovation relevant to Europol's competence.

5. The Innovation Advisory Group shall meet regularly. It shall have no decision-making power and shall not represent the Management Board.

6. Europol shall provide secretariat and administrative support.

7. The Innovation Advisory Group shall adopt its rules of procedure.

Chapter V
Organisation of Europol

Article 68

Administrative and management structure of Europol

1. The administrative and management structure of Europol shall comprise:

(a) a Management Board;

(b) an Executive Board;

(c) an Executive Director;

(d) Deputy Executive Directors, where such positions are established;

(e) an ICT/IM Steering Group;

(f) an ICT/IM Advisory Group;

(g) an Innovation Advisory Group;

(h) where appropriate, other advisory bodies established by the Management Board in accordance with Article 72;

(i) the Centres.

2. The members of Europol's administrative and management structure shall not have any financial or other interests that could affect their impartiality. They shall act in the public interest and carry out their activities in an independent, impartial and transparent manner. They shall make annual declarations of interests in accordance with the internal rules adopted by the Management Board. Europol shall make those declarations public on an annual basis.

SECTION 1
MANAGEMENT BOARD

Article 69

Composition of the Management Board

1. The Management Board shall be composed of one representative from each Member State and two representatives of the Commission, all with a voting right.

2. The Management Board shall also include:

   (a) one member designated by the European Parliament, without the right to vote.

   (b) one member appointed by each of the countries associated with the implementation, application and development of the Schengen acquis, where provided for and in accordance with the relevant international agreement referred to in Article 93.

3. Each member of the Management Board shall have an alternate. The alternate shall represent the member in his or her absence.

4. The members of the Management Board and their alternates shall be appointed in light of their knowledge of law enforcement cooperation relevant to the Europol's competence, taking into account their managerial, administrative and budgetary skills and expertise. All parties represented in the Management Board shall make efforts to limit the turnover of their representatives to ensure continuity in the work of the Management Board. All parties shall aim to achieve a balanced representation between men and women on the Management Board.

5. The term of office for members and their alternates shall be four years. The terms of office shall be extendable.

Article 70

Chairperson of the Management Board

1. The Management Board shall elect a Chairperson and a Deputy Chairperson from within the group of three Member States that have jointly prepared the Council's 18-month programme. They shall serve for the 18-month period corresponding to that Council programme. Where, however, the Chairperson's or the Deputy Chairperson's membership of the Management Board ends at any time during their term of office as Chairperson or Deputy Chairperson, their term of office shall automatically expire at the same time.

2. The Chairperson and the Deputy Chairperson shall be elected by a majority of two-thirds of the members with the right to vote of the Management Board.

3. The Deputy Chairperson shall automatically replace the Chairperson if he or she is prevented from attending to his or her duties.

Article 71

Meetings of the Management Board

1. The Chairperson shall convene the meetings of the Management Board.

   Meetings of the Management Board shall, in principle, be held at Europol's headquarters.

2. The Executive Director shall take part in the deliberations, without the right to vote.

3. The Management Board shall hold at least two ordinary meetings a year. In addition, it shall meet on the initiative of its Chairperson, at the request of the Commission, or at the request of at least one-third of its members.

4. Where necessary, the Management Board may hold joint meetings with the management boards of Eurojust, Frontex and CEPOL.

5. The Management Board may invite any person whose opinion may be of interest to attend its meeting as an observer.

6. Two representatives of the JPSG shall be invited to attend two ordinary meetings of the Management Board per year as non-voting observers to discuss the following matters of political interest:

   (a) the consolidated annual activity report referred to in Article 72(2), point (m), for the previous year;

   (b) the single programming document referred to in Article 73 for the following year and the annual budget;

   (c) JPSG written questions and answers;

   (d) external relations and partnership matters.

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

7. The members of the Management Board and their alternates may, subject to its rules of procedure, be assisted at the meetings by advisers or experts.

8. Europol shall provide the secretariat for the Management Board.

Article 72

Functions of the Management Board

1. The Management Board shall be responsible for taking the strategic decisions of Europol and give the general orientations for Europol's activities.

2. The Management Board shall:

   (a) adopt, by a majority of two-thirds of its members with voting rights, the annual budget of Europol and exercise other functions in respect of Europol's budget;

   (b) adopt the financial rules applicable to Europol;

   (c) adopt and regularly update the communication and dissemination plans, based on an analysis of needs;

   (d) adopt its rules of procedure, including provisions concerning the tasks and the functioning of its secretariat;

   (e) exercise, in accordance with paragraph 5 and with respect to Europol staff, the powers conferred by the Staff Regulations on the appointing authority and by the Conditions of Employment of Other Servants on the authority empowered to conclude a contract of employment of other servants ('the appointing authority powers');

   (f) adopt implementing rules giving effect to the Staff Regulations and the Conditions of Employment of Other Servants in accordance with Article 110(2) of the Staff Regulations;

   (g) appoint by a majority of two-third the Executive Director and, where appropriate, the Deputy Executive Directors, and where relevant extend their term of office or remove them from office;

(h) establish the organisational structure of Europol and adopt Europol's staff policy having regard to sound budgetary management;

(i) establish, where appropriate, advisory bodies, determine their mandate, composition, and implementing rules;

(j) decide, on a proposal from the Executive Director and subject to the prior approval of the Commission, on the establishment of operational, technical or administrative functions, capacities or facilities in Member States other than the host Member State, where necessary for the performance of Europol's tasks;

(k) authorise the conclusion of working arrangements;

(l) taking into account the opinion of the Commission, adopt Europol's single programming document by a majority of two-thirds of members entitled to vote with voting rights.

(m) define the evaluation criteria for assessing Europol's performance and adopt, by a majority of two-thirds of its members with voting rights, a consolidated annual activity report on Europol's activities and, by 1 July of the following year, send it to the European Parliament, the Council, the Commission, the Court of Auditors and the national parliaments. The consolidated annual activity report shall be made public. The Commission shall adopt implementing acts establishing reporting indicators to ensure a uniform approach to the collection and presentation of information by Europol in respect of crimes affecting the financial interests of the Union;

(n) adopt rules for the prevention and management of conflicts of interest in respect of its members, including in relation to their declaration of interests;

(o) adopt appropriate measures to support the recognition of skills and professional experience acquired in the course of employment with, or activities carried out for, Europol, including through the development of a common competency framework in cooperation with CEPOL;

(p) monitor Europol's strategic priorities and objectives, as reflected in the evaluation criteria referred to in point (m), and ensure appropriate follow-up to operational, technological and organisational challenges affecting the fulfilment of Europol's tasks;

(q) oversee the performance of the Executive Director, including the implementation of Management Board decisions and the effective exercise of the powers conferred on the Executive Director under this Regulation;

(r) appoint a Data Protection Officer, who shall be functionally independent in the performance of his or her duties;

(s) appoint an accounting officer, who shall be functionally independent in the performance of his or her duties;

(t) establish and oversee an independent internal audit capability, and ensure adequate follow-up to recommendations stemming from the internal or external audit reports evaluations and investigations of the EPPO, the European Anti-Fraud Office (OLAF) and the EDPS;

(u) adopt guidelines for the processing of information by Europol in accordance with Article 32, after consulting the EDPS;

(v) adopt implementing rules governing the Centres in accordance with Articles 13 to 19, and regularly assess their functioning and adapt them where necessary in light of operational needs and evolving security threats;

(w) designate the Fundamental Rights Officer, who shall be functionally independent in the performance of his or her duties;

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

3. Where the Management Board considers it necessary for the performance of Europol's tasks, it may suggest to the Council that it draw the attention of the Commission to the need for an adequacy decision as referred to in Article 94a Regulation (EU) 2018/1725, or for a recommendation for a decision authorising the opening of negotiations to conclude an international agreement as referred to in Article 94b(2) of Regulation (EU) 2018/1725.

4. Where at least one third of the members of the Management Board identify a need for action by Europol in a specific area falling within its competence, the Management Board shall invite the Executive Director to propose appropriate measures.

5. The Management Board shall adopt, in accordance with Article 110(2) of the Staff Regulations, a decision based on Article 2(1) of the Staff Regulations and on Article 6 of the Conditions of Employment of Other Servants, delegating the relevant appointing authority powers to the Executive Director and establishing the conditions under which such delegation of powers may be suspended. The Executive Director shall be authorised to subdelegate those powers.

6. Where exceptional circumstances so require, the Management Board may, by way of a decision, temporarily suspend the delegation of the appointing authority powers to the Executive Director and any sub-delegation of such powers and exercise them itself or delegate those powers to one of its members or to a staff member other than the Executive Director.

7. The Management Board may delegate certain tasks, except those requiring a two-thirds majority of the Management Board, to the Executive Board referred to in Article 75, and shall adopt internal rules governing its tasks, composition and functioning.

Article 73

Multiannual programming and annual work programmes

1. The Management Board shall, by the end of each year, adopt a single programming document containing Europol's multiannual programming and annual work programme, based on a draft put forward by the Executive Director, in accordance with the opinion of the Commission and, as regards the multiannual programming, after having consulted the Joint Parliamentary Scrutiny Group (JPSG), established jointly by the European Parliament and national parliaments.

   Where the Commission delivers a negative opinion on grounds relating to compliance with Union law, consistency with Union policy objectives or sound financial management, the Management Board shall review the draft single programming document prior to its adoption to ensure compliance with Union law, consistency with Union policy objectives and sound financial management.

Where the Management Board decides not to take into account any of the matters raised by the JPSG in accordance with Article 71(6), point (c), it shall provide a thorough justification.

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

2. The multiannual programming shall set out the overall strategic programming, including the objectives, expected results and performance indicators. It shall also set out the resource planning, including the multiannual budget and establishment plan taking into account the need to ensure an appropriate mix of skills and expertise required for the performance of Europol's tasks. It shall include the strategy for relations with third countries and international organisations and Europol's planned research and innovation activities.

The multiannual programming shall be implemented by means of annual work programmes and shall, where appropriate, be updated following the outcome of external and internal evaluations. The conclusion of those evaluations shall also be reflected, where appropriate, in the annual work programme for the following year.

3. The annual work programme shall comprise detailed objectives, expected results and performance indicators. It shall also contain a description of the actions to be financed and an indication of the financial and human resources allocated to each action, in accordance with the principles of activity-based budgeting and management. The annual work programme shall be consistent with the multiannual programming. It shall clearly indicate tasks that have been added, changed or deleted compared to the previous financial year.

4. Where, after adoption of an annual work programme, a new task is assigned to Europol, the Management Board shall amend the annual work programme.

5. Any substantial amendment to the annual work programme, especially a modification resulting in a reallocation of the budgetary resources above 2 % of the annual budget, shall be adopted by the same procedure as that applicable to the adoption of the initial annual work programme. The Management Board may delegate to the Executive Director the power to make non-substantial amendments to the annual work programme.

Article 74

Voting rules of the Management Board

1. Without affecting Article 70(2), Article 72(2), points (a),(g), (l) and (m), Article 76(7) and Article 126(2), the Management Board shall take decisions by an majority of its members with voting rights.

2. In the event that the Commission raises serious concerns on a decision proposal presented to the Management Board on matters related to Delegated Regulation (EU) 2019/715, the Staff Regulations and the Conditions of Employment of Other Servants, the Management Board shall postpone the adoption of the decision concerned. Within 15 days of the Commission's raising of serious concerns on a decision proposal presented to the Management Board, the Management Board shall re-examine and adopt that decision, possibly amended, at second reading either by a two-thirds majority of its members with voting rights, including the Commission

representatives, or by a four-fifths majority of the representatives of the Member States.

3. Each member with voting rights shall have one vote. In the absence of a member with voting rights, his or her alternate shall be entitled to exercise his or her right to vote.

4. The Chairperson shall take part in the voting.

5. The Executive Director shall not take part in the voting.

6. The Management Board's rules of procedure shall establish more detailed voting arrangements, in particular the circumstances in which a member may act on behalf of another member.

SECTION 3
EXECUTIVE BOARD

Article 75

Executive Board

1. The Management Board shall be assisted by an Executive Board.

2. The Executive Board shall:

   (a) prepare the decisions to be adopted by the Management Board and monitor the implementation of the decisions adopted by it, without affecting the responsibilities of the Executive Director;

   (b) review the draft annual budget, the draft consolidated annual activity report and the oversee the preparation and implementation of the annual and multiannual programming;

   (c) monitor the implementation of Europol's budget and prepare the financial and budgetary decisions to be adopted by the Management Board;

   (d) adopt an internal anti-fraud strategy, proportionate to risk of fraud;

   (e) ensure, together with the Management Board, adequate follow-up to the findings and recommendations resulting from internal or external audit reports and evaluations, to the findings of investigations conducted by the European Anti-Fraud Office (OLAF), and to the outcomes, including judicial decisions, of investigations, conducted by the EPPO, in accordance with applicable Union law;

   (f) without affecting the responsibilities of the Executive Director, assist and advise him or her in the implementation of the decisions of the Management Board, with a view to reinforcing supervision of administrative and budgetary management;

3. Where necessary on grounds of urgency, the Executive Board may adopt provisional decisions on behalf of the Management Board, in particular in matters relating to administrative and budgetary management, management, including the suspension of the delegation of appointing authority powers. Such decisions shall be submitted to the Management Board for confirmation at its next meeting.

4. The Executive Board shall be composed of the Chairperson of the Management Board, one representative of the Commission to the Management Board and three

other members appointed by the Management Board from among its members with the right to vote. The Chairperson of the Management Board shall also be the Chairperson of the Executive Board. The Executive Director shall take part in the meetings of the Executive Board but shall not have the right to vote.

5. The term of office of members of the Executive Board shall be four years. The term of office of members of the Executive Board shall end when their membership of the Management Board ends.

6. The Executive Board shall hold at least one ordinary meeting every three months. In addition, it shall meet on the initiative of its Chairperson or at the request of its members.

7. The Executive Board may also invite as observers without the right to vote other participants for specific agenda items.

SECTION 4
EXECUTIVE DIRECTOR

Article 76

Appointment, dismissal, and extension of the term of office

1. The Executive Director shall be engaged as a temporary agent of Europol under Article 2, point (a), of the Conditions of Employment of Other Servants.

2. The Executive Director shall be appointed by the Management Board from a list of candidates proposed by the Commission. For the purpose of concluding the contract of the Executive Director, Europol shall be represented by the Chairperson of the Management Board.

3. The term of office of the Executive Director shall be five years. In due time before the end of that period, the Commission shall carry out an assessment that takes into account an evaluation of the performance of the Executive Director and Europol's future tasks and challenges.

4. The Management Board, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 3, may extend the term of office of the Executive Director once, for no more than five years.

5. An Executive Director whose term of office has been extended shall not participate in another selection procedure for the same post at the end of the overall period.

6. The Executive Director may be removed from office only upon a decision of the Management Board acting on a proposal from the Commission.

7. The Management Board shall reach decisions on appointment, extension of the term of office or removal from office of the Executive Director and/or Deputy Executive Director(s) on the basis of a two-thirds majority of its members with voting rights.

8. In case of vacancy, unless the Management Board decides which Deputy Executive Director will ensure tasks and responsibilities of the Executive Director until the appointment of a new Executive Director, a Deputy Executive Director in the highest grade shall ensure that role.

Article 77

Tasks and responsibilities of the Executive Director

1. The Executive Director shall be responsible for the management of Europol. The Executive Director shall be accountable to the Management Board.

2. The Executive Director shall report to the European Parliament, the JPSG and the Council on Europol's performance and tasks when invited to do so.

3. The Executive Director shall be the legal representative of Europol.

4. The Executive Director shall be responsible for the implementation of the tasks assigned to Europol by this Regulation. In particular, the Executive Director shall be responsible for:

   (a) ensuring the day-to-day administration of Europol;

   (b) proposing to the Management Board the establishment of operational, technical or administrative functions or capacities hosted in Member States other than the host Member State, where necessary for the performance of Europol's tasks;

   (c) identifying operational priorities, capability gaps and emerging security threats relevant to Europol's competence and propose appropriate operational, technological or organisational measures to the Management Board;

   (d) ensuring compliance with the financial rules of Europol;

   (e) preparing the draft single programming document and submitting it to the Management Board after consulting the Commission;

   (f) preparing Europol's consolidated annual activity report and presenting it to the Management Board for assessment and adoption;

   (g) protecting the financial interests of the Union by applying preventive measures against fraud, corruption and any other illegal activities, without prejudicing the investigative competence of OLAF and EPPO by effective checks and, if irregularities are detected, by recovering amounts wrongly paid and, where appropriate, by imposing effective, proportionate and dissuasive administrative and financial penalties;

   (h) reporting any criminal conduct to the EPPO in accordance with Article 24 of Regulation (EU) 2017/1939 in respect of which the EPPO could exercise its competence and reporting to OLAF in accordance with Article 8(1) of Regulation (EU, Euratom) 883/ 2013;

   (i) preparing a follow-up action plan related to the conclusions of internal or external audit reports and evaluations, and investigation reports and recommendations from investigations by the EPPO, OLAF and the EDPS, and report on progress regularly to the Management Board and inform the Commission, where appropriate and without undue delay, of significant findings and the measures taken in response;

   (j) preparing draft financial rules applicable to the Agency;

   (k) preparing the Agency's draft statement of estimates of revenue and expenditure and implementing its budget in accordance with the principles of sound financial management and performance-based budgeting;

   (l) preparing appropriate draft implementing rules to give effect to the Staff Regulations and the Conditions of Employment of Other Servants in accordance with Article 110 of the Staff Regulations;

(m) preparing draft internal rules for the prevention and management of conflicts of interest in respect of the members of the Management Board and present those draft rules to the Management Board for adoption;

(n) promoting diversity and gender balance as regards the recruitment of the Agency's staff;

(o) regularly informing the Management Board of cooperation with Union institutions, bodies, missions and agencies, including on the preparation and conclusion of working arrangements and the operational considerations relating thereto, and, where appropriate submit proposals for follow-up measures to the Management Board;

(p) regularly informing the Management Board of cooperation with third countries and international organisations, including on the preparation and conclusion of working arrangements with authorities of third countries and international organisations;

(q) regularly informing the Management Board of the application of Regulation (EU) 2018/1725 for the transfer of personal data and the operational considerations relating thereto;

(r) regularly informing the Management Board of working arrangements concluded with private parties, including their strategic relevance, operational impact and any associated risks;

(s) performing other tasks pursuant to this Regulation.

Article 78

Deputy Executive Directors

1. One or more Deputy Executive Directors may assist the Executive Director. The Executive Director shall define their tasks.

2. Article 77 shall apply to the Deputy Executive Directors. The Executive Director shall be consulted prior to their appointment, any extension of their term of office or their removal from office.

Chapter VI
Relations with Union entities

Article 79

Common provisions

1. Europol may establish and maintain cooperative relations with Union bodies, offices and agencies in accordance with the tasks attributed to Europol and to those bodies, offices and agencies and shall seek to ensure synergies in the performance of their respective tasks. Europol shall establish and maintain a close relationship with the Union bodies, offices and agencies under Articles 81 to 90, which shall not be limited to the areas referred to therein.

   Europol may also establish and maintain cooperative relations with Union institutions and missions set up on the basis of the Treaties in accordance with the tasks attributed to Europol and to those institutions and missions.

2. Europol's cooperation with Union bodies, offices and agencies under this Chapter shall notably aim at strengthening the overall effectiveness of the Union's response to forms of crime listed in Annex I, in particular by seeking to ensure complementarity and, where possible, enhance coordination and avoid duplication of actions, including by means of:

(a) the exchange of information, in accordance with the conditions laid down in this Regulation;

(b) operational activities;

(c) strategic and analytical activities;

(d) the exchange of specialist knowledge and expertise;

(e) training activities;

(f) the development of capabilities, including through research and innovation, and joint procurement;

(g) coordination of activities, where relevant, in relation to third countries and international organisations;

(h) coordination of activities for the implementation of relevant Union strategies and policy priorities.

3. The cooperation referred to in paragraphs 1 and 2 shall take place within the framework of working arrangements concluded with the entities referred to in paragraph 1. Such working arrangements shall not allow for the exchange of personal data and shall not bind the Union or its Member States.

The working arrangements concluded with Union bodies, offices and agencies established within the framework of the TFEU shall be subject to the Commission's prior approval, with the exception of the working arrangement referred to in Article 81. These working arrangements shall be subject to regular review depending on the evolution of operational needs, at the own initiative of Europol and the Union institution, body, mission, office or agency concerned or, with the exception of the working arrangement referred to in Article 81, at the request of the Commission.

Any working arrangement concluded by Europol with a Union institution, body, mission, office or agency before the entry into force of this Regulation shall be subject to review after the start date of application of this Regulation.

4. The Executive Director shall inform the Management Board about any regular cooperative relations which Europol intends to establish and maintain in accordance with paragraphs 1, 2 and 3, and about the development of such relations once established.

5. Subject to any restriction pursuant to Article 33(2) and to the rules applicable pursuant to Article 129, Europol may directly exchange any information, with the exception of personal data, with a Union institution, body, mission, office or agency, in so far as such an exchange is relevant for the performance of Europol's tasks or those of that Union institution, body, mission, office or agency.

6. Subject to any restrictions indicated pursuant to Article 33(2) or (3) and to the rules applicable pursuant to Article 129, Europol may transmit personal data to the entities referred to in paragraph 1, insofar as such transmission is necessary and proportionate for the legitimate performance of the tasks of that entity. Personal data

transmitted to the entities referred to in paragraph 1 by Europol may be processed for another purpose only where authorised by Europol and where compatible with the initial purpose for which the data were collected and transmitted by Europol. Where the data to be transmitted have been provided by a Member State or a Union institution, body, office or agency and the conditions in Article 81 paragraphs (3) and (4) are fulfilled, Europol shall share personal data and other relevant information with the EPPO regardless of any restriction indicated pursuant to Article 33(2) or (3).

7. Europol may receive and process personal data from Union institutions, bodies, missions, offices and agencies insofar as necessary and proportionate for the legitimate performance of its tasks. Any information which has clearly been obtained in obvious violation of human rights shall not be processed.

8. Where a Union institution, body, mission, office or agency has received personal data from Europol, onward transmissions or transfers of such data shall be prohibited unless Europol has given its prior explicit authorisation.

9. Europol shall ensure that detailed records of all transmissions or transfers of personal data and of the grounds for such transmissions or transfers are recorded in accordance with this Regulation.

Article 80

Common provisions on indirect information exchange on the basis of a hit/no-hit system

1. Europol shall take all appropriate measures to ensure indirect access by other Union bodies, offices and agencies, where such access is provided for in Union law, to information held by Europol, on the conditions of reciprocity, by means of an automated hit/no-hit system operated through the searching of indexes which shall be kept up to date.

2. Indirect access to information under the first paragraph shall not affect any restrictions indicated by the Member States, Union institutions, bodies, missions, offices and agencies, third countries or international organisations providing the information, in accordance with Article 33(2).

3. In the case of a hit, Europol shall initiate the procedure by which the information that generated the hit is to be transmitted to the searching Union body, office or agency as referred to in paragraph 1, in accordance with the restrictions set by the provider of the information pursuant to this Regulation. In case of a hit with information that is subject to restrictions indicated pursuant to Article 33(2), the automated hit/no-hit system referred to in paragraph 1 shall not notify the searching Union body, office or agency of that hit. In that case, Europol shall contact expeditiously the provider of the information to inquire if the information that generated the hit can be shared with the searching Union body, office or agency. Where the provider of the information lifts those restrictions, Europol shall transmit the information that generated the hit to the searching Union body, office or agency. Where the provider of the information maintains those restrictions, Europol shall comply with those restrictions and not transmit the information that generated the hit to the searching Union body, office or agency.

4. Searches of information in accordance with paragraphs 1 and 2 shall be carried out only for the purpose of identifying whether information available at another Union body, office or agency matches information processed at Europol for the purposes of points (a), (b) and (c) of Article 32(2).

5. While preserving the automated nature of the hit/no-hit system, Europol shall allow searches in accordance with paragraphs 1 and 2 only by persons designated by other Union bodies, offices or agencies as authorised to perform such searches.

6. Under the conditions of reciprocity referred to in the first paragraph, Europol shall, within the limits of its competence, have indirect access, on the basis of an automated hit/no-hit system, to information provided to Union bodies, offices and agencies, subject to the conditions set out in Union law.

7. Such access shall not affect any restrictions indicated by the Member State, Union institution, body, office or agency, third country or international organisation that provided that information.

8. Europol and other Union bodies, offices and agencies shall inform each other if, as a result of a hit in accordance with paragraphs 1 and 3, there are indications that data may be incorrect or may conflict with other data.

9. Where necessary for the implementation of the hit/no-hit system referred to in paragraphs 1 to 8, the technical procedure, including the data sets that should be included in the indexes as well as performance and availability requirements, shall be laid down by means of implementing acts adopted in accordance with Article 138.

Article 81

Relations with the EPPO

1. Europol shall establish and maintain a close relationship with the EPPO based on a working arrangement setting out the modalities of their cooperation. The working arrangement shall be subject to regular review.

2. Upon request by the EPPO in accordance with Article 102 of Regulation (EU) 2017/1939, Europol shall support the investigations of the EPPO, namely by providing any information held by Europol and related to crimes falling within the competence of the EPPO and by providing the requested operational support for the performance of the EPPO's tasks.

3. For the purpose of providing the EPPO with the information and support referred to in the first subparagraph, Europol shall ensure that the necessary organisational arrangements are in place, including the allocation of dedicated human resources.

4. To ensure that Europol provides the EPPO with the necessary information under paragraph 2 of this Article, Europol shall enable the EPPO to have indirect access on the basis of a hit/no hit automated system to data related to offences that fall within the competence of the EPPO, held for the purposes referred to in Article 32(2), points (a), (b) and (c). That hit/no hit system shall notify Europol and the provider of the information referred to in Article 33(1) in the case of a hit.

5. Pursuant to Article 43(2) of Regulation (EU) 2017/1939, in the case of a hit, Europol shall share with the EPPO the information that generated the hit to the extent that relates to offences within the competence of the EPPO and shall notify the provider of the information.

6. In accordance with Article 24(1) of Regulation (EU) 2017/1939, Europol shall, without undue delay, report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence in accordance with Regulation (EU) 2017/1939.

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

8. Europol may carry out joint operational analysis with the EPPO.

9. When Europol receives information from the EPPO on forms of crime falling outside the scope of the competence of the EPPO and within the scope of Europol's competence, Europol shall process and analyse such information and, where relevant, disseminate it to the competent authorities of the Member States in accordance with this Regulation.

Article 82

Relations with Eurojust

1. Where, during Europol's activities, including at any stage of an operational task force, Europol or a Member State identifies the need for effective judicial follow-up within the mandate of Eurojust, Europol shall, without undue delay, notify Eurojust and any Member State concerned to that effect. Europol shall initiate the procedure for sharing the relevant information, in accordance with the decision of the Member State providing the information. In such a case, Eurojust shall consult with Europol.

2. Europol and Eurojust may agree on establishing joint operational platforms and other forms of structured cooperation to support the competent authorities of the Member States in specific crime areas which fall within their respective competence. This may include joint operational analysis.

3. Europol shall cooperate with Eurojust, within their respective mandates, in supporting the competent authorities of the Member States in the context of digital investigations and access to data, and in particular act as a knowledge hub for advising, assisting and providing capacity-building on the cross-border access to e-evidence.

4. Europol shall support Eurojust, within their respective mandates, in relation to core international crimes.

Article 83

Relations with OLAF

Where, during Europol's information-processing activities in respect of an individual investigation or in the process of asset recoveries, Europol or a Member State identifies the need for coordination, cooperation or support in accordance with the mandate of OLAF, Europol shall notify OLAF to that effect and shall initiate the procedure for sharing the relevant information, in accordance with the decision of the Member State providing the information. In such a case, OLAF shall consult with Europol.

Article 84

Relations with the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA)

1. Europol's relationship with the AMLA shall aim notably at supporting Financial Intelligence Units (FIUs) in the context of a joint analysis carried out pursuant to

Article 32 of Directive (EU) 2024/1640 of the European Parliament and of the Council[74] and Article 40 of Regulation (EU) 2024/1620.

2. For the purposes of Article 41(4) of Regulation (EU) 2024/1620, Europol shall receive, process and analyse the results of the joint analyses and any additional information in accordance with this Regulation.

Article 85

Relations with the European Border and Coast Guard Agency (Frontex)

Europol shall cooperate with Frontex, notably in:

(a) identifying high-risk cross-border movements and related criminal activities, including by analysing travel information contained in Union large-scale IT systems, and for that purpose, Europol shall compare such data with information it holds in accordance with this Regulation and provide Frontex with relevant risk indicators.

(b) implementing the activities carried out under Regulation (EU) 2024/1356 and in the framework of Regulation (EU) 2019/1896, and for that purpose, Europol may, at the request of the concerned Member State, deploy staff to support checks against relevant Union large-scale IT systems, in accordance with Article 22 of this Regulation, including in the context of activities carried out under Regulation (EU) 2019/1896, and major international events.

Article 86

Relations with eu-LISA

1. Europol shall cooperate with eu-LISA in areas of common interest related to the development, deployment and operation of information systems and related communication infrastructure.

2. The cooperation between Europol and eu-LISA referred to in paragraph 1 shall include, where appropriate and in accordance with their respective mandates, but shall not be limited to:

(a) the participation in, or use of, procurement procedures, including joint procurement actions, framework contracts or other procurement instruments for the acquisition of works, supplies or services;

(b) the sharing, re-use or adaptation of technical components, tools, services or building blocks developed or operated by either agency;

(c) the provision of technical support, expertise or services, including in the field of system development, testing, maintenance and security;

(d) the establishment of joint project teams and the exchange of staff, expertise and other resources necessary for the implementation of common projects and technical activities.

---

[74] Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (OJ L, 2024/1640, 19.6.2024, ELI: http://data.europa.eu/eli/dir/2024/1640/oj).

3. For the development and maintenance of services, tools and applications created, hosted or managed by Europol, Europol shall request eu-LISA to provide public key infrastructure certificates from eu-LISA's Certification Authority to Europol and, where appropriate, to the competent authorities of the Member States.

4. Cooperation under paragraphs 1, 2 and 3 shall take place within the framework of working arrangements setting out the practical modalities, including financial aspects, governance arrangements, arrangements for staff exchanges and temporary assignments, and the establishment and operation of joint project teams.

5. Paragraphs 1 to 4 shall not affect the responsibilities of Europol as regards the development and operation of its own information systems.

Article 87

Relations with the European Union Drugs Agency

Europol's cooperation with the European Union Drugs Agency, established by Regulation (EU) 2023/1322 of the European Parliament and of the Council[75], shall concern notably the collection of data, and the monitoring of trends, on drug supply, including illicit production and trafficking and other related crimes, on the use of new technologies and on new psychoactive substances.

Article 88

Relations with the European Union Agency for Fundamental Rights (FRA)

Europol's cooperation with the FRA shall support Europol in ensuring full respect of the fundamental rights and freedoms enshrined in the Charter in the performance of its different tasks. This shall notably include areas of Europol's activity that can have particular impact on the rights of individuals, including vulnerable persons, such as children.

Article 89

Relations with the European Union Customs Authority

Europol's cooperation with the European Union Customs Authority, established by Regulation […], shall aim at enabling reciprocal exchange of relevant data and information for the prevention and combating of serious crime and terrorism, notably by enabling Europol to obtain, upon request, data, including personal data and commercially sensitive data, available in the EU Customs Data Hub, in accordance with Regulation […].

Article 90

Relations with ENISA

Europol's cooperation with ENISA shall aim notably at:

(a) enhancing shared situational awareness of the cyber threat and incident landscape, in particular with respect to cyber threat intelligence; and

(b) improving cybersecurity preparedness, response to and recovery from ransomware incidents.

[75] Regulation (EU) 2023/1322 of the European Parliament and of the Council of 27 June 2023 on the European Union Drugs Agency (EUDA) and repealing Regulation (EC) No 1920/2006 (OJ L 166, 30.6.2023, p. 6, ELI: http://data.europa.eu/eli/reg/2023/1322/oj).

Chapter VII
Relations with partners

SECTION 1
COMMON PROVISIONS

Article 91

Common provisions

1. Where necessary for the performance of its tasks, Europol may establish and maintain cooperative relations with the authorities of third countries, international organisations and private parties.
2. Subject to any restriction laid down in Article 33(2) and without affecting Article 129, Europol may directly exchange all information, with the exception of personal data, with entities referred to in paragraph 1 of this Article, in so far as such an exchange is relevant for the performance of Europol's tasks.
3. The Executive Director shall inform the Management Board about any regular cooperative relations which Europol intends to establish and maintain in accordance with paragraphs 1 and 2, and about the development of such relations once established.
4. For the purposes set out in paragraphs 1 and 2, Europol may conclude working arrangements with entities referred to in paragraph 1, which shall be subject to prior approval of the Commission. Such working arrangements shall not allow the exchange of personal data, shall not create legal obligations under international or Union law, and shall not express positions binding upon the Union or its Member States.
5. Europol may receive and process personal data from entities referred to in paragraph 1 insofar as necessary and proportionate for the legitimate performance of its tasks and in accordance with Regulation 2018/1725 and this Regulation.
6. Where third countries, international organisations or private parties have received personal data from Europol, onward transmissions or transfers of such data shall be prohibited unless Europol has given its prior explicit authorisation.
7. Europol shall ensure that detailed records of all transmissions or transfers of personal data and of the grounds for such transmissions or transfers are recorded in accordance with this Regulation.
8. Any information which has clearly been obtained in obvious violation of human rights shall not be processed by Europol.

SECTION 2
COOPERATION WITH THIRD COUNTRIES AND INTERNATIONAL ORGANISATIONS

Article 92

Priorities for external engagement

Europol shall ensure that its cooperation with third countries and international organisations is coherent with the Union's external policies and priorities and is conducted, where appropriate,

in coordination with Union delegations. To that end, Europol, within the limits of its mandate, shall adopt an external strategy as part of the multiannual programming and annual work programme referred to in Article 73, subject to prior approval by the Commission.

Article 93

Cooperation with Schengen associated countries

1. Europol shall maintain a close cooperation with countries associated with the implementation, application and development of the Schengen *acquis* ("Schengen associated countries").

2. The scope, modalities, rights and obligations relating to the cooperation referred to in paragraph 1 may be determined by a dedicated international agreement to be concluded between the Union and the Schengen associated country concerned.

3. The international agreement referred to in paragraph 2 may provide for:

   (a) access to, and the ability to query, the Europol Cross-Matching Service and the Europol Analytical Environment in accordance with Articles 39 and 41;

   (b) observer status in the Management Board and in the ICT/Information Management Steering Group, which shall not confer voting rights in accordance with Article 69;

   (c) the posting of liaison officers, subject to the same conditions as those applicable to liaison officers from Member States pursuant to Article 27.

4. Any international agreement providing for the form of cooperation referred to in paragraph 3 may also provide for:

   (a) the provision of information by the Schengen associated country concerned to Europol under conditions corresponding to those laid down in Article 29(1), (2) and (5) and the obligation for Europol to take into account the information provided by the Schengen associated country concerned as set out in Article 29(6);

   (b) an appropriate financial contribution to be paid by the Schengen associated country concerned to Europol.

Article 94

Transfer of personal data to third countries and international organisations

1. Europol may transfer personal data to third countries and international organisations without affecting Article 129.

5. The Executive Director shall be competent to authorise the transfer of personal data in accordance with Articles 94b, 94c and 94d of Regulation (EU) 2018/1725.

   The Management Board may, following an authorisation by the EDPS, authorise for a period not exceeding one year, which shall be renewable, a set of transfers where the conditions of Article 94c of Regulation (EU) 2018/25 are fulfilled.

6. For the purposes of paragraph 2, the Executive Director shall take a decision, without undue delay, on the basis of all relevant information, including, where appropriate, input from the Data Protection Officer and the relevant operational centres. As a general rule, such transfers shall be authorised when the applicable conditions are

met and shall be carried out via SIENA. Where the third country or international organisation concerned does not have access to SIENA, transfers shall take place via INTERPOL channels.

7. The Executive Director shall as soon as possible inform the Management Board of the cases in which Articles 94b, 94c and 94d of Regulation (EU) 2018/1725 have been applied.

Article 95

Relations with the Member States or third countries in the context of their participation in the Maritime Analysis and Operations Centre (Narcotics)

1. In so far as necessary for the performance of its tasks, Europol shall establish and maintain cooperation with the Member States and third countries participating in the Maritime Analysis and Operations Centre (Narcotics) (MAOC (N)) by means of a working arrangement.

2. Europol may exchange information with third countries participating in MAOC (N) subject to compliance with the general principles and rules for transfers of operational personal data to third countries of Regulation (EU) 2018/1725.

3. The Member States participating in MAOC (N) shall connect their liaison officers posted at MAOC-N to SIENA to submit relevant information to Europol.

4. Europol shall provide analytical support to MAOC (N) for the purpose of criminal investigations against high-risk criminal networks trafficking drugs at sea.

SECTION 3
COOPERATION WITH PRIVATE PARTIES AND NATURAL PERSONS

Article 96

Exchanges of personal data with private parties

1. Insofar as is necessary for Europol to perform its tasks, Europol may process personal data obtained from private parties.

2. Europol may receive directly from a private party personal data which that private party declares it is legally allowed to transmit in accordance with the applicable law.

3. For the purpose of informing the competent authorities of the Member States of any criminal offence that concerns them and that relates to personal data received from a private party, and of enabling them to take the necessary measures, Europol shall forward the personal data and any relevant results from the processing of those data to the Europol national units concerned.

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

5. Europol shall only transmit or transfer personal data to private parties, when it is strictly necessary and proportionate, to be determined on a case-by-case basis, and in particular where it is in the interests of the data subject or necessary to prevent the imminent commission of a crime, including terrorism.

Such transmission or transfer shall only take place when the rights and freedoms of the data subject do not outweigh the public interest requiring the transmission or transfer.

The transmission or transfer referred to in the first subparagraph of this paragraph is subject to any restrictions pursuant to Article 33(2) or (3) and shall not affect Article 129.

6. Where the private party is not established within the Union or in a third country as referred to in Article 94a of Regulation (EU) 2018/1875, the transfer shall be authorised by the Executive Director only in the following cases:

   (a) the transfer is necessary to protect the vital interests of the data subject concerned or of another person;

   (b) the transfer is necessary to safeguard legitimate interests of the data subject concerned;

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

   (d) the transfer is necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of a specific crime falling within the scope of Europol's competence;

   (e) the transfer is 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 falling within the scope of Europol's competence.

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

7. Transmissions or transfers of personal data under paragraphs 5 and 6 shall not be systematic, massive or structural.

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

9. Europol's mechanism referred to in Article 47 may be used for exchanges of information between the competent authorities of the Member States and private parties in accordance with the respective Union and national law. Those exchanges may also cover crimes not falling within the scope of Europol's competence.

   Where Member States use Europol's mechanism for the exchange of information on crimes falling within the scope of Europol's competence, they shall provide Europol with a copy of such information.

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

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

10. Europol shall ensure that detailed records of all transmissions or transfers of personal data and the grounds for such transmissions or transfers are recorded in accordance with this Regulation and communicated upon request to the EDPS in accordance with Regulation (EU) 2018/1725.

11. Where the personal data received or to be transmitted or transferred affect the interests of a Member State, Europol shall immediately inform the Europol national unit of the Member State concerned.

12. By 31 March, the Management Board shall adopt an annual report on the personal data exchanged with private parties pursuant to this Article, on the basis of quantitative and qualitative evaluation criteria established by the Management Board.

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

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

Article 97

Information from natural persons

1. Insofar as is necessary for Europol to perform its tasks, Europol may receive and process information originating from natural persons.

2. Personal data originating from natural persons shall only be processed by Europol provided that they are received through one of the following ways:

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

   (b) the contact point of a third country or an international organisation to which personal data may be transferred pursuant to Article 94b(2), point (c), of Regulation (EU) 2018/1725;

   (c) an authority of a third country or an international organisation to which personal data may be transferred pursuant to Article 94a, Article 94b(1) or Article 94b(2), point (a), of Regulation (EU) 2018/1725.

3. Where Europol receives information, including personal data, from a natural person residing in a third country in respect of which the conditions for a transfer pursuant to Articles 94a or 94b of Regulation (EU) 2018/1725 are not fulfilled, Europol shall forward that information only to a Member State or to such third country.

4. Where the personal data received affect the interests of a Member State, Europol shall immediately inform the Europol national unit of the Member State concerned.

5. Europol shall not contact natural persons to retrieve information.

6. Without prejudice to Articles 104 and 105, Europol may not provide personal data to natural persons.

Chapter VIII
Data protection

Article 98

Processing of personal data by Europol

1. Unless otherwise provided for in this Regulation, Regulation (EU) 2018/1725 shall apply to the processing of personal data by Europol.

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

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

Article 99

Assessment of reliability of the source and accuracy of information

1. The reliability of the source of information originating from a Member State shall be assessed as far as possible by the providing Member State using the following source evaluation codes:

   (a) (A): where there is no doubt as to the authenticity, trustworthiness and competence of the source, or where the information is provided by a source which has proved to be reliable in all instances;

   (b) (B): where the information is provided by a source which has in most instances proved to be reliable;

   (c) (C): where the information is provided by a source which has in most instances proved to be unreliable;

   (d) (X): where the reliability of the source cannot be assessed.

2. The accuracy of information originating from a Member State shall be assessed as far as possible by the providing Member State using the following information evaluation codes:

   (a) (1): information the accuracy of which is not in doubt;

   (b) (2): information known personally to the source but not known personally to the official passing it on;

   (c) (3): information not known personally to the source but corroborated by other information already recorded;

   (d) (4): information not known personally to the source and which cannot be corroborated.

3. Where Europol, on the basis of information already in its possession, comes to the conclusion that the assessment provided for in paragraphs 1 or 2 needs to be corrected, it shall inform the Member State concerned and seek to agree on an amendment to the assessment. Europol shall not change the assessment without such agreement.

4. Where Europol receives information from a Member State without an assessment conducted in accordance with paragraphs 1 or 2, it shall attempt to assess the reliability of the source or the accuracy of information on the basis of information already in its possession. The assessment of specific data and information shall take place in agreement with the providing Member State. A Member State may also agree with Europol in general terms on the assessment of specified types of data and specified sources. Where no agreement is reached in a specific case, or no agreement in general terms exists, Europol shall assess the information or data and shall attribute to such information or data the evaluation codes (X) and (4) referred to in paragraphs 1 and 2 respectively.

5. Paragraphs 1 to 4 shall apply *mutatis mutandis* where Europol receives data or information from a Union institution, body, mission, office or agency, a third country, an international organisation or a private party.

6. Information from publicly available sources shall be assessed by Europol using the evaluation codes set out in paragraphs 1 and 2.

7. Where information is the result of an analysis made by Europol in the performance of its tasks, Europol shall assess such information in accordance with this Article, and in agreement with the Member States participating in the analysis.

Article 100

Processing of personal data of different categories of data subjects and of special categories of personal data

1. Processing of personal data in respect of victims of a criminal offence, witnesses or other persons who can provide information concerning criminal offences shall be allowed where it is strictly necessary and proportionate for preventing or combating crime falling within the scope of Europol's competence.

2. Processing of personal data, by automated or other means, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health or concerning natural persons' sex life or sexual orientation shall be allowed only where strictly necessary and proportionate for research and innovation projects pursuant to Article 102 and for operational purposes, within the scope of Europol's competence, and only for preventing or combating crime falling within the scope of Europol's competence. Such processing shall also be subject to appropriate safeguards laid down in this Regulation with regard to the rights and freedoms of the data subject, and, with the exception of biometric data processed for the purpose of uniquely identifying a natural person, shall be allowed only where those data supplement other personal data processed by Europol. The selection of a particular group of persons solely on the basis of such personal data shall be prohibited.

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

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

5. Notwithstanding the first subparagraph, where it is necessary to grant staff of the competent authorities of the Member States or Union bodies and agencies, direct access to personal data for the performance of their tasks and in accordance with this Regulation, or for research and innovation projects in accordance with Article 102(2), point (c), the Executive Director shall duly authorise a limited number of such staff to have such access.

6. Personal data as referred to in paragraphs 1 and 2 shall not be transmitted to Member States or Union institutions, bodies, missions, offices and agencies or transferred to third countries, international organisations or private parties, unless such transmission or transfer is required under this Regulation or Union law or is strictly necessary and proportionate in individual cases concerning crimes falling within the scope of Europol's competence and in accordance with Chapters VI and VII.

7. Every year Europol shall provide the EDPS with a statistical overview of all personal data as referred to in paragraph 2 which it has processed.

Article 101

Time-limits for the storage and erasure of personal data

1. Personal data processed by Europol shall be stored by Europol only for as long as is necessary and proportionate for the purposes for which the data are processed.

2. Europol shall in any event review the need for continued storage no later than three years after the start of initial processing of personal data. Europol may decide on the continued storage of personal data until the following review, which shall take place after another period of three years, where continued storage is still necessary for the performance of Europol's tasks. The reasons for the continued storage shall be justified and recorded. Where no decision is taken on the continued storage of personal data, that data shall be erased automatically after three years.

3. Where personal data as referred to in Article 100(1) and (2) are stored for a period exceeding five years, the EDPS shall be informed thereof.

4. Where a Member State, a Union institution, body, mission, office or agency, a third country or an international organisation has indicated any restriction as regards the earlier erasure or destruction of the personal data at the moment of transmission or transfer in accordance with Article 33(2), Europol shall erase the personal data in accordance with those restrictions. Where continued storage of the data is deemed necessary, on the basis of information that is more extensive than that possessed by the data provider, in order for Europol to perform its tasks, Europol shall request the authorisation from the data provider to continue storing the data and shall present a justification for such request.

5. A Member State, a Union institution, body, mission, office or agency, a third country or an international organisation that erases from its own data files personal data provided to Europol shall inform Europol accordingly. Europol shall erase the data unless the continued storage of the data is deemed necessary, on the basis of information that is more extensive than that possessed by the data provider, in order for Europol to perform its tasks. Europol shall inform the data provider of the continued storage of such data and present a justification of such continued storage.

6. Personal data shall not be erased in the following cases:

(a) such erasure would damage the interests of a data subject who requires protection, in which case the data shall be used only with the express and written consent of the data subject;

(b) the accuracy of the personal data is contested by the data subject, for a period enabling Member States or Europol, where appropriate, to verify the accuracy of the data;

(c) the data have to be maintained for purposes of proof or for the establishment, exercise or defence of legal claims;

(d) the data subject opposes their erasure and requests the restriction of their use instead.

Article 102

Processing of personal data for research and innovation

1. Europol may process personal data for the purpose of the relevant research and innovation projects, provided that the processing of those personal data is required and duly justified to achieve the objectives of the project concerned.

   As regards special categories of personal data, such processing shall only be carried out when it is strictly necessary and subject to appropriate safeguards, which may include pseudonymisation.

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

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

   (a) any research and innovation project shall require the prior authorisation by the Executive Director, based on:

   i. a description of the objectives of the project and an explanation of how the project assists Europol or competent authorities of the Member States in their tasks;

   ii. a description of the envisaged processing activity, setting out the objectives, scope and duration of the processing and the necessity and proportionality to process the personal data;

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

   iv. an assessment of compliance with Article 71 of Regulation (EU) 2018/1725 regarding the time limits for the storage and conditions for access to the personal data.

   (b) the Management Board shall be informed of the launch of the project, in accordance with the guidelines referred to in Article 32(11);

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

   i. be temporarily copied to a separate, isolated and protected data processing environment, which may, where appropriate, support iterative development,

testing and validation processes, within Europol for the sole purpose of carrying out that project;

ii. be accessed in accordance with Article 100(4) by specifically authorised Europol staff and, subject to technical security measures, by specifically authorised staff of the competent authorities of the Member States and Union agencies;

iii. not be transmitted or transferred;

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

v. be erased once the project is concluded or the time limit for the storage of personal data has expired in accordance with Article 91;

vi. subject to appropriate safeguards and where duly justified, be reused within Europol for subsequent research and innovation projects pursuing compatible objectives, in particular for the improvement, testing or validation of algorithms and AI models and AI systems;

(d) the logs of the processing of personal data in the context of the project shall be kept for two years after the conclusion of the project, solely for the purpose of and only as long as necessary for verifying the accuracy of the outcome of the data processing.

3. Where Europol considers that a new type of research and innovation project poses a significant risk to the rights and freedoms of data subjects, it shall, in addition to the requirements set out under paragraph 2, point (a), of this Article also carry out a data protection impact assessment in accordance with Article 89 of Regulation (EU) 2018/1725. In such cases, the EDPS shall be informed prior to the launch of the project.

4. Paragraphs 2 and 3 shall not apply to the adjustment, modification or deployment of existing capabilities, including in a defined operational context, provided that such activities do not substantially alter the nature, scope or purpose of the processing in a manner that would increase the risk to the rights and freedoms of data subjects.

5. The Management Board shall establish in a binding document the general scope for the research and innovation projects. Such document shall be updated where appropriate and made available to the EDPS for the purpose of its supervision.

6. Europol shall keep a document containing a detailed description of the process and of the rationale behind the training, testing and validation of algorithms to ensure transparency of the process and the algorithms, including their compliance with the safeguards provided for in this Article, and to allow for verification of the accuracy of the results based on the use of such algorithms. Upon request, Europol shall make that document available to interested parties, including Member States and the JPSG.

7. Where the data to be processed for a research and innovation project have been provided by a Member State, a Union body, a third country or an international organisation, Europol shall request consent from that provider of data in accordance with Article 33(2), unless the provider of data has granted its prior authorisation to such processing for the purpose of research and innovation projects, either in general terms or subject to specific conditions.

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

Article 103

Notification of a personal data breach to the authorities concerned

1. Without affecting Article 92 of Regulation (EU) 2018/1725, in the event of a personal data breach, Europol shall notify the competent authorities of the Member States concerned of that breach, without undue delay, and 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.

2. The notification referred to in paragraph 1 shall, as a minimum:

   (a) describe the nature of the personal data breach including, where possible and appropriate, the categories and number of data subjects concerned and the categories and number of data records concerned;

   (b) describe the likely consequences of the personal data breach;

   (c) describe the measures proposed or taken by Europol to address the personal data breach;

   (d) where appropriate, recommend measures to mitigate the possible adverse effects of the personal data breach.

Article 104

Communication of a personal data breach to the data subject

Without affecting Article 93 of Regulation (EU) 2018/1725, where Europol does not have the contact details of the data subject concerned, it shall request the provider of the data to communicate the personal data breach to the data subject concerned and to inform Europol about the decision taken. Member States providing the data shall communicate the personal data breach to the data subject concerned in accordance with national law.

Article 105

Right of access for the data subject

1. Any data subject wishing to exercise the right of access referred to in Article 80 of Regulation (EU) 2018/1725 to personal data that relate to the data subject may make a request to that effect to the authority appointed for that purpose in the Member State of their choice, or to Europol. That authority shall refer the request to Europol without undue delay and within one month of receipt.

2. Europol shall confirm receipt of the request referred to in paragraph 1. Europol shall answer it without undue delay, and in any case within four months of receipt by Europol of the request., without prejudice to Article 81 of Regulation (EU) 2018/1725.

3. Europol shall consult the competent authorities of the Member States and the provider of the data concerned on a decision to be taken. A decision on access to personal data shall be conditional on close cooperation between Europol and the Member States and the provider of the data directly concerned by the access of the data subject to such data. Member States and the provider of the data concerned shall

cooperate closely with Europol and shall reply to the consultation carried out by Europol without undue delay. Where a Member State or the provider of the data objects to Europol's proposed response, it shall notify Europol of the reasons for its objection. Europol shall take the utmost account of any such objection. Europol shall subsequently notify its decision to the competent authorities of the Member States concerned and to the provider of the data.

Article 106

Right to rectification, erasure and restriction

1. Any data subject wishing to exercise the right to rectification or erasure of personal data or of restriction of processing of personal data that relate to them referred to in Article 82 of Regulation (EU) 2018/1725 may make a request to that effect, through the authority appointed for that purpose in the Member State of their choice, or to Europol. Where the request is made to that authority, it shall refer the request to Europol within one month of receipt.

2. Without prejudice to Article 82(3) of Regulation (EU) 2018/1725, Europol shall restrict the processing of personal data rather than erase personal data where there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject.

3. Restricted data shall be processed only to protect the rights of the data subject, where that is necessary to protect the vital interests of the data subject or of another person, or for the purposes laid down in Article 82(3) of Regulation (EU) 2018/1725.

4. Where personal data as referred to in paragraphs 1 and 2 held by Europol have been provided to it by third countries, international organisations or Union institutions, bodies, missions, offices or agencies, have been directly provided by private parties, have been retrieved by Europol from publicly available sources or result from Europol’s own analyses, Europol shall rectify or erase such data or restrict their processing and, where appropriate, inform the providers of the data.

5. Where personal data referred to in paragraphs 1 and 2 held by Europol have been provided to it by Member States, the Member States concerned shall rectify or erase such data or restrict their processing in cooperation with Europol, within their respective competences.

6. Europol shall rectify or erase data in collaboration with the provider of the data concerned in all of the following cases:

   (a) incorrect personal data have been transmitted or transferred by another appropriate means;

   (b) the errors in the data provided by Member States are due to faulty transmission or transfer or transmission or transfer in breach of this Regulation;

   (c) the errors in the data result from data being input, taken over or stored in an incorrect manner or in breach of this Regulation by Europol.

7. In the cases referred to in paragraphs 3, 4 and 5, all addressees of the data concerned shall be notified forthwith. In accordance with the rules applicable to them, the addressees shall then rectify, erase or restrict those data in their systems.

Article 107

Responsibility in data protection matters

1. Europol shall process personal data in a manner that ensures that their source, in accordance with Article 28, can be established.

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

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

   (b) Europol in respect of personal data provided by third countries or international organisations or directly provided by private parties, of personal data retrieved by Europol from publicly available sources or resulting from Europol's own analyses and of personal data stored by Europol in accordance with Article 101(5).

3. Where Europol becomes aware that personal data provided pursuant to Article 28(1), points (a) and (b), are factually incorrect or have been unlawfully stored, it shall inform the provider of those data accordingly.

4. The responsibility for the legality of a data transmission or transfer shall lie with:

   (a) the Member State which provided the personal data to Europol;

   (b) Europol in the case of personal data provided by it to Member States, third countries or international organisations.

5. In the case of a transmission between Europol and a Union institution, body, mission, office or agency, the responsibility for the legality of the transmission shall lie with Europol.

   Without affecting the first subparagraph, where the data are transmitted by Europol following a request from the recipient, both Europol and the recipient shall be responsible for the legality of such a transmission.

6. Europol shall be responsible for all data processing operations carried out by it, with the exception of the bilateral exchange of data using Europol's infrastructure between Member States, Union institutions, bodies, missions, offices and agencies, third countries, international organisations and private parties to which Europol has no access. Such bilateral exchanges shall take place under the responsibility of the entities concerned and in accordance with their law. The security of such exchanges shall be ensured in accordance with Article 91 of Regulation (EU) 2018/1725.

Article 108

Prior consultation

1. Europol may initiate processing operations which are subject to prior consultation of the EDPS pursuant to Article 90(1) of Regulation (EU) 2018/1725 unless the EDPS has provided written advice pursuant to Article 90(4) of that Regulation within a period of eight weeks, which starts on the date of submission of the initial request for consultation and is not to be suspended or extended.

2. Where the processing operations referred to in paragraph 1 of this Article have substantial significance for the performance of Europol's tasks and are particularly urgent and necessary to prevent and combat an immediate threat of a crime falling

within the scope of Europol's competence or to protect vital interests of the data subject or another person, Europol may exceptionally initiate processing.

In that case, Europol shall inform the EDPS prior to the start of processing operations and shall provide it with a reasoned description of the intended purpose of the processing, the categories of data concerned and an initial assessment of the risks to data subjects. Europol shall submit to the EDPS the additional information required for the purpose of the prior consultation of the EDPS within four weeks following the start of processing operations.

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

The Data Protection Officer shall be involved in assessing the urgency of such processing operations and shall oversee the processing in question.

Article 109

Data Protection Officer

1. The Management Board shall appoint a member of Europol staff as Data Protection Officer, who shall be designated for that sole position.
2. To support the Data Protection Officer in carrying out his or her tasks, a member of Europol staff may be designated as assistant Data Protection Officer
3. The Data Protection Officer shall report directly to the Management Board.
4. The Management Board shall adopt implementing rules concerning the Data Protection Officer. Those implementing rules shall in particular concern the procedure for the selection of the Data Protection Officer and his or her dismissal, tasks, duties and powers, as well as safeguards for his or her independence.
5. The Data Protection Officer shall be appointed for a term of four years and shall be eligible for reappointment.
6. The provisions applicable to the Data Protection Officer shall apply *mutatis mutandis* to the assistant Data Protection Officer.
7. Where the Data Protection Officer considers that the provisions of this Regulation or of Regulation (EU) 2018/1725 concerning the processing of personal data have not been complied with, he or she shall inform the Executive Director and shall require him or her to resolve the non-compliance within a specified period. Where the Executive Director does not resolve the non-compliance of the processing within the specified period, the Data Protection Officer shall inform the Management Board. The Management Board shall reply within a specified time limit agreed with the Data Protection Officer. Where the Management Board does not resolve the non-compliance within the specified period, the Data Protection Officer shall refer the matter to the EDPS.

Article 110

Fundamental Rights Officer

1. The Management Board shall, upon a proposal of the Executive Director, designate a Fundamental Rights Officer. The Fundamental Rights Officer may be a member of Europol staff who received special training in fundamental rights law and practice.

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

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

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

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

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

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

   (f) any other tasks where provided for by this Regulation.

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

Article 111

Fundamental Rights Training

Europol staff shall receive mandatory training on the protection of fundamental rights and freedoms. All Europol staff involved in operational tasks involving personal data processing should receive dedicated training concerning the processing of personal data. This training shall be developed in cooperation with the European Union Agency for Fundamental Rights and CEPOL.

Article 112

Supervision by the national supervisory authority

1. For the purpose of exercising their supervisory function, the national supervisory authorities referred to in Article 41 of Directive (EU) 2016/680 shall have access, at the Europol national unit or at the liaison officers' premises, to data submitted by their Member State to Europol in accordance with the relevant national procedures and to logs as referred to in Article [...] of Regulation (EU) 2018/1725.

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

3. National supervisory authorities shall, in accordance with the relevant national procedures, supervise the activities of Europol national units and the activities of liaison officers, insofar as such activities are relevant to the protection of personal data. They shall also keep the EDPS informed of any actions they take with respect to Europol.

4. Any person shall have the right to request the national supervisory authority to verify the legality of any transmission or transfer or communication to Europol of data concerning him or her in any form and of access to those data by the Member State

concerned. That right shall be exercised in accordance with the national law of the Member State in which the request is made.

Article 113

Cooperation between the EDPS and national supervisory authorities

1. The EDPS shall act in close cooperation with the national supervisory authorities on issues requiring national involvement, in particular where the EDPS or a national supervisory authority finds major discrepancies between the practices of Member States or potentially unlawful transmissions or transfers in the use of Europol's channels for exchanges of information, or in the context of questions raised by one or more national supervisory authorities on the implementation and interpretation of this Regulation.

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 Regulation (EU) 2018/1725.

   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 Regulation (EU) 2018/1725 and be bound by an obligation equivalent to that laid down in Article 129 of this Regulation

3. The EDPS shall keep national supervisory authorities fully informed of all issues directly affecting or otherwise relevant to them. Upon the request of one or more national supervisory authorities, the EDPS shall inform them of specific issues.

4. In cases relating to data originating from one or more Member States, including the cases referred to in Article 114, the EDPS shall consult the national supervisory authorities concerned. The EDPS shall not decide on further action to be taken before those national supervisory authorities have informed the EDPS of their opinion, within a deadline specified by him or her which shall not be shorter than one month and not longer than three months from when the EDPS consults the national supervisory authorities concerned. The EDPS shall take the utmost account of the respective positions of the national supervisory authorities concerned. Where the EDPS intends not to follow the position of a national supervisory authority, he or she shall inform that authority, provide a justification and submit the matter to the European Data Protection Board.

Chapter IX
Remedies and liability

Article 114

Procedure for the handling of complaints by the EDPS

1. Where a complaint relates to a decision referred to in Articles 105 or 106 of this Regulation or Articles 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. In adopting his or her decision,

which may extend to a refusal to communicate any information, the EDPS shall take into account the opinion of the national supervisory authority.

2. Where a complaint relates to the processing of data provided by a Member State to Europol, the EDPS and the national supervisory authority of the Member State that provided the data shall, each acting within the scope of their respective competences, ensure that the necessary checks on the lawfulness of the processing of the data have been carried out correctly.

3. Where a complaint relates to the processing of data provided to Europol by Union institutions, bodies, offices or agencies, third countries or international organisations, or of data retrieved by Europol from publicly available sources or resulting from Europol's own analyses, the EDPS shall ensure that Europol has correctly carried out the necessary checks on the lawfulness of the processing of the data.

Article 115

General provisions on liability and the right to compensation

1. Europol's contractual liability shall be governed by the law applicable to the contract in question.

2. The Court of Justice of the European Union shall have jurisdiction to give judgment pursuant to any arbitration clause in a contract concluded by Europol.

3. In the case of non-contractual liability, Europol shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its departments or by its staff in the performance of their duties.

4. The Court of Justice of the European Union shall have jurisdiction in disputes relating to compensation for damage as referred to in paragraph 3.

5. The personal liability of Europol staff vis-à-vis Europol shall be governed by the provisions laid down in the Staff Regulations or in the Conditions of Employment of Other Servants applicable to them.

Chapter X
Joint parliamentary scrutiny

Article 116

Joint parliamentary scrutiny

1. Pursuant to Article 88 TFEU, the scrutiny of Europol's activities shall be carried out by the European Parliament together with national parliaments. That shall constitute a specialised JPSG established jointly by the national parliaments and the competent committee of the European Parliament. The organisation and the rules of procedure of the JPSG shall be determined together by the European Parliament and the national parliaments in accordance with Article 9 of Protocol No 1 on the role of National Parliaments in the European Union.

2. The JPSG shall politically monitor Europol's activities in fulfilling its mission, including as regards the impact of those activities on the fundamental rights and freedoms of natural persons.

3. The Chairperson of the Management Board, the Executive Director or their Deputies shall appear before the JPSG at its request to discuss matters relating to the activities

referred to in the first subparagraph, including the budgetary aspects of such activities, the structural organisation of Europol and the potential establishment of new units and specialised centres, taking into account the obligations of discretion and confidentiality. The JPSG may decide to invite to its meetings other relevant persons, where appropriate.

4. The EDPS shall appear before the JPSG at its request, and at least once a year, to discuss general matters relating to the protection of fundamental rights and freedoms of natural persons, and in particular the protection of personal data, with regard to Europol's activities, taking into account the obligations of discretion and confidentiality.

5. Europol shall consult the JPSG in relation to the multiannual programming of Europol in accordance with Article 73(1).

6. Europol shall transmit the following documents, for information purposes, to the JPSG, taking into account the obligations of discretion and confidentiality:

   (a) strategic analyses, threat assessments, trend reports and situational briefings relating to Europol's competence and the results of studies and evaluations commissioned by Europol;

   (b) the administrative arrangements concluded pursuant to Article 79(3);

   (c) the document containing the multiannual programming and the annual work programme of Europol, referred to in Article 73(1);

   (d) the consolidated annual activity report on Europol’s activities, referred to in Article 73(2), including relevant information on Europol’s activities and results obtained in processing large data sets, without disclosing any operational details and without prejudice to any ongoing investigations;

   (e) the evaluation report drawn up by the Commission, referred to in Article 130;

   (f) annual information pursuant to Article 96(12) on the personal data exchanged with private parties pursuant to Articles 96, including an assessment of the effectiveness of cooperation, specific examples of cases demonstrating why those requests were necessary and proportionate for the purpose of enabling Europol to carry out its tasks, and, as regards personal data exchanges pursuant to Article 96, the number of children identified as a result of those exchanges to the extent that this information is available to Europol;

   (g) annual information about the number of cases where it was necessary for Europol to process personal data that do not relate to the categories of data subjects listed in Annex II, alongside information on the duration and outcomes of the processing, including examples of such cases demonstrating why that data processing was necessary and proportionate;

   (h) annual information about transfers of personal data to third countries and international organisations pursuant to Article 94, including the number of cases authorised transfers pursuant to Article 94(2);

   (i) annual information about the number of cases in which Europol proposed the possible entry of information alerts in accordance with Article 30, including specific examples of cases demonstrating why the entry of those alerts was proposed;

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

(k) annual information on the number and types of cases where special categories of personal data were processed, pursuant to Article 100.

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

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

7. The JPSG may request other relevant documents necessary for the fulfilment of its tasks relating to the political monitoring of Europol's activities, subject to Regulation (EC) No 1049/2001 of the European Parliament and of the Council[76] and without affecting Articles 117 and 129 of this Regulation.

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

Article 117

Access by the European Parliament to information processed by or through Europol

1. For the purpose of enabling it to exercise parliamentary scrutiny of Europol's activities in accordance with Article 116, access by the European Parliament and the JPSG to sensitive non-classified information processed by or through Europol, upon the European Parliament's request, shall comply with the rules referred to in Article 129(1).

2. Access by the European Parliament to EU classified information processed by or through Europol shall be consistent with the applicable Interinstitutional Agreement between the European Parliament and the Council concerning the forwarding to and the handling by the European Parliament of classified information held by the Council on matters other than those in the area of the common foreign and security policy, and shall comply with the rules referred to in Article 129(2) of this Regulation.

3. The necessary details regarding access by the European Parliament to the information referred to in paragraphs 1 and 2 shall be governed by working arrangements concluded between Europol and the European Parliament.

[76] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43, ELI: http://data.europa.eu/eli/reg/2001/1049/oj)

Chapter XI
Staff

Article 118

General provisions

1. The Staff Regulations, the Conditions of Employment of Other Servants and the rules adopted by agreement between the institutions of the Union for giving effect to the Staff Regulations and to the Conditions of Employment of Other Servants shall apply to Europol staff.

2. Europol staff shall consist of temporary staff and contract staff. The Management Board shall be informed on a yearly basis of contracts of an indefinite duration granted by the Executive Director. The Management Board shall decide which posts to be occupied by temporary agents provided for in the establishment plan can be filled only by staff from the competent authorities of the Member States. The Management Board shall regularly review those posts in light of operational requirements and the need to preserve specialised expertise. Staff recruited to occupy such posts may be awarded only fixed-term contracts, renewable once. The overall maximum period of such temporary agent contracts shall not exceed ten years.

Article 119

Seconded national experts

1. Europol may make use of seconded national experts.

2. The Management Board shall adopt a decision laying down rules on the secondment of national experts to Europol.

Chapter XII
Financial provisions

Article 120

Budget

1. Estimates of all revenue and expenditure for Europol shall be prepared each financial year, which shall correspond to the calendar year, and shall be shown in Europol's budget.

2. Europol's budget shall be balanced in terms of revenue and of expenditure.

3. Without prejudice to other resources, Europol's revenue shall comprise of:

   (a) a contribution from the Union entered in the general budget of the Union;

   (b) contributions from countries associated with the implementation, application and development of the Schengen acquis, where such contributions are provided for in the relevant international agreements;

   (c) any voluntary financial contributions from Member States, in accordance with the rules adopted by the Management Board.

4. Europol may benefit from Union funding in the form of contribution agreements or ad hoc grants in accordance with its financial rules referred to in Article 124 and with the provisions of the relevant instruments supporting the policies of the Union.

5. Europol's expenditure shall include staff remuneration, administrative and infrastructure expenses, and operating costs.

6. Budgetary commitments for actions extending over more than one financial year may be broken down into several annual instalments.

Article 121

Establishment of the budget

1. Each year the Executive Director shall draw up a draft statement of estimates of Europol's revenue and expenditure for the following financial year, including an establishment plan, and shall send it to the Management Board. The draft statement of estimates shall be established in a manner that ensures a clear differentiation of appropriations by sub-activity, in accordance with the structure of the Single Programming Document.

2. The Management Board shall, on the basis of the draft statement of estimates, adopt a provisional draft estimate of Europol's revenue and expenditure for the following financial year, including the provisional establishment plan. The Management Board shall send it to the European Parliament, to the Council and to the Commission by 31 January each year, as part of the draft single programming document.

3. The Management Board shall send the final draft estimate of Europol's revenue and expenditure, which shall include a draft establishment plan, to the Commission by 31 March each year.

4. The Commission shall send the statement of estimates to the European Parliament and the Council, together with the draft general budget of the Union.

5. On the basis of the statement of estimates, the Commission shall enter in the draft general budget of the Union the estimates that it considers necessary for the establishment plan and the amount of the contribution to be charged to the general budget, which it shall place before the European Parliament and the Council in accordance with Articles 313 and 314 TFEU.

6. The European Parliament and the Council shall authorise the appropriations for the contribution from the Union to Europol.

7. The European Parliament and the Council shall adopt Europol's establishment plan.

8. Europol's budget shall be adopted by the Management Board. It shall become final following the final adoption of the general budget of the Union. Where necessary, it shall be adjusted accordingly.

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

Article 122

Implementation of the budget

1. The Executive Director shall implement Europol's budget.

2. Each year the Executive Director shall send to the European Parliament and the Council all information relevant to the findings of any evaluation procedures.

Article 123

Presentation of accounts and discharge

1. Europol's accounting officer shall send the provisional accounts for the financial year (year N) to the Commission's accounting officer and to the Court of Auditors by 1 March of the following financial year (year N + 1).

2. Europol shall send a report on the budgetary and financial management for year N to the European Parliament, the Council and the Court of Auditors by 31 March of year N + 1.

3. The Commission's accounting officer shall send Europol's provisional accounts for year N, consolidated with the Commission's accounts, to the Court of Auditors by 31 March of year N + 1.

4. On receipt of the Court of Auditors' observations on Europol's provisional accounts pursuant to Article 252 of Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council, Europol's accounting officer shall draw up Europol's final accounts for that year. The Executive Director shall submit those final accounts to the Management Board for an opinion.

5. The Management Board shall deliver an opinion on Europol's final accounts for year N.

6. Europol's Executive Director shall, by 1 July of year N + 1, send the final accounts for year N to the European Parliament, the Council, the Commission, the Court of Auditors and national parliaments, together with the Management Board's opinion referred to in paragraph 5.

7. The final accounts for year N shall be published in the Official Journal of the European Union by 15 November of year N + 1.

8. The Executive Director shall send to the Court of Auditors, by 30 September of year N + 1, a reply to the observations made in its annual report. He or she shall also send the reply to the Management Board.

9. Upon the request of the European Parliament, the Executive Director shall submit to it any information required for the smooth application of the discharge procedure for year N, in accordance with Article 261(3) of Regulation (EU, Euratom) 2024/2509.

10. On a recommendation from the Council acting by a qualified majority, the European Parliament shall, before 15 May of year N + 2, grant a discharge to the Executive Director in respect of the implementation of the budget for year N.

Article 124

Financial rules

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

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

3. Europol may award grants without a call for proposals to Member States, third countries and international organisations for the performance of activities falling within the scope of Europol's competence.

4. Where duly justified for operational purposes, following authorisation by the Management Board, financial support may cover the full investment costs of equipment and infrastructure.

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

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

Chapter XIII
Miscellaneous provisions

Article 125

Privileges and immunities

1. Protocol No 7 on the privileges and immunities of the European Union, annexed to the TEU and to the TFEU, shall apply to Europol and its staff.

2. Privileges and immunities of liaison officers and members of their families shall be subject to an agreement between the Kingdom of Netherlands and the other Member States. That agreement shall provide for such privileges and immunities as are necessary for the proper performance of the tasks of liaison officers.

Article 126

Language arrangements

1. The provisions laid down in Regulation No 1 shall apply to Europol.

2. The Management Board shall decide by a majority of two-thirds of its members on the internal language arrangements of Europol.

3. Translation and all other linguistic services required by Europol, other than interpretation, shall be provided by the Translation Centre for the bodies of the Union established by Council Regulation (EC) No 2965/94[77].

Article 127

Transparency

1. Regulation (EC) No 1049/2001 shall apply to documents held by Europol. When Europol supports the investigations of the EPPO, the application of Regulation (EC) No 1049/2001 by Europol shall not affect Article 109 of Regulation (EU) 2017/1939.

2. Decisions taken by Europol under Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the European Ombudsman or of an action before the

[77] Council Regulation (EC) No 2965/94 of 28 November 1994 setting up a Translation Centre for bodies of the European Union (OJ L 314, 7.12.1994, p. 1, ELI: http://data.europa.eu/eli/reg/1994/2965/oj).

Court of Justice of the European Union, in accordance with Articles 228 and 263 TFEU respectively.

3. Europol shall publish on its website a list of the Management Board members and summaries of the outcome of the meetings of the Management Board. The publication of those summaries shall be temporarily or permanently omitted or restricted where such publication would jeopardise the performance of Europol's tasks, taking into account its obligations of discretion and confidentiality and the operational character of Europol.

Article 128

Prevention and combating fraud and irregularities

1. The Court of Auditors shall have a power of audit, on the basis of documents and on-the-spot checks, over all grant beneficiaries, contractors and subcontractors who have received Union funds from Europol.

2. OLAF may carry out investigations, including on-the-spot checks and inspections, to establish whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant or a contract awarded by Europol, or serious matters relating to the discharge of professional duties constituting a dereliction of the obligations of members or staff members liable to result in disciplinary or, as the case may be, criminal proceedings. Such investigations shall be carried out in accordance with the provisions and procedures laid down in Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council[78] and in Council Regulation (Euratom, EC) No 2185/96[79].

3. In accordance with Regulation (EU) 2017/1939, the EPPO investigates and prosecutes fraud and other illegal activities affecting the financial interests of the Union as provided for in Directive (EU) 2017/1371 of the European Parliament and of the Council[80].

Article 129

Rules on the protection of sensitive non-classified and classified information

1. Europol shall adopt its 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 (SNC) information including, inter alia, provisions for the exchange of such information with third

---

78 Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/883/oj).

79 Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities (OJ L 292, 15.11.1996, p. 2, ELI: http://data.europa.eu/eli/reg/1996/2185/oj).

80 Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law (OJ L 198, 28.7.2017, p. 29, ELI: http://data.europa.eu/eli/dir/2017/1371/oj).

countries, and processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/443[81] and (EU, Euratom) 2015/444[82].

2. The management board shall adopt 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[83].

Article 130

Evaluation and review

1. Not later than … [five years after the entry into force of this Regulation], and every five years thereafter, the Commission shall carry out an evaluation of Europol's performance in relation to its competence, mandate, tasks and governance in accordance with Commission's guidelines. The Management Board shall be heard in the evaluation process. When assessing the impact of Europol's activities on fundamental rights, the Commission shall seek input from the European Union Agency for Fundamental Rights.

2. The evaluation shall, in particular, address the possible need to modify the mandate of Europol, and the financial implications of any such modification.

3. On the occasion of every second evaluation, there shall be an assessment of the results achieved by Europol having regard to its competence, mandate, governance and tasks, including an assessment of whether the continuation of the Agency is still justified with regard to such competence, mandate, governance and tasks.

4. The Commission shall report to the European Parliament, the Council and the Management Board on the evaluation findings. The findings of the evaluation shall be made public.

Article 131

Administrative inquiries

The activities of Europol shall be subject to inquiries by the European Ombudsman in accordance with Article 228 TFEU.

Article 132

Headquarters

The necessary arrangements concerning the accommodation to be provided for Europol in the Kingdom of the Netherlands and the facilities to be made available by the Kingdom of the Netherlands, together with the specific rules applicable there to the Executive Director, members of the Management Board, Europol staff and members of their families, shall be laid down in a headquarters agreement between Europol and the Kingdom of the Netherlands, in accordance with Protocol No 6.

---

81 Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41, ELI: http://data.europa.eu/eli/dec/2015/443/oj).

82 Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53, ELI: http://data.europa.eu/eli/dec/2015/444/oj).

83 Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

This shall be without prejudice to the possibility for Europol to host operational, technical or administrative functions and capacities in other Member States.

Chapter XIV
Transitional provisions

Article 133

Legal succession

1. Europol as established by this Regulation shall be the legal successor of Europol as established by Regulation (EU) 2016/794 for all its rights and obligations under the applicable national, Union and international law.

2. This Regulation shall not affect the validity of the cooperation agreements and working arrangements concluded by Europol under the Europol Convention, Decision 2009/371/JHA or Regulation (EU) 2016/794. Such cooperation agreements and working arrangements shall remain in force and shall be applied until they expire or are replaced.

Article 134

Transitional arrangements

1. Europol may continue the activities initiated pursuant to Regulation (EU) 2016/794 that are not concluded before the date of application of this Regulation. Such activities shall be continued in accordance with this Regulation.

2. Personal data processed by Europol before the date of application of this Regulation in compliance with Regulation (EU) 2016/794 may continue to be processed by Europol where such processing complies with this Regulation.

3. Any set of transfers to third countries and international organisations authorised by the Management Board under the terms and conditions set out in Article 25(6) of Regulation (EU) 2016/794 shall remain valid under this Regulation until the date of expiry of the period for which the transfer was authorised.

4. Decisions, implementing measures, rules and arrangements adopted pursuant to Regulation (EU) 2016/794 shall remain in force until repealed or replaced under this Regulation.

5. The Management Board shall repeal decisions and measures adopted pursuant to Regulation (EU) 2016/794, which do not comply with this Regulation.

6. Staff employed by Europol on the date of application of this Regulation shall retain the rights and obligations arising from their contracts of employment and appointments.

7. The Executive Director and the Deputy Executive Directors appointed on the basis of Regulation (EU) 2016/794 shall, for the remaining period of his or her term of office, have the respective responsibilities of Executive Director and Deputy Executive Directors, as provided for in this Regulation.

   Where, on the date of application of this Regulation, the Executive Director or a Deputy Executive Director is serving his or her first term of office, that term of office shall be of 5 years. Any extension of that term of office shall follow the procedure set out in Article 76(3)-(7) of this Regulation.

Where, on the date of application of this Regulation, the Executive Director or a Deputy Executive Director is serving his or her second term of office, that term of office shall be of 5 years. It shall not be subject to any further extension.

8. The members of the Management Board and their alternates appointed under Regulation (EU) 2016/794 shall continue to exercise their functions until the end of their respective terms of office as determined under Regulation (EU) 2016/794.

Chapter XV
Amendments to other existing instruments

Article 135

Amendments to Regulation (EU) 2018/1726

In Regulation (EU) 2018/1726, the following Article 41a is inserted:

'Article 41a

Cooperation with Europol

1. eu-LISA may cooperate with Europol in areas of common interest related to the development, deployment and operation of information systems and related communication infrastructure.

2. The cooperation between eu-LISA and Europol referred to in paragraph 1 shall in particular include, where appropriate and in accordance with their respective mandates:

   (a) the participation in, or use of, procurement procedures, including joint procurement actions, framework contracts or other procurement instruments for the acquisition of works, supplies or services;

   (b) the sharing, re-use or adaptation of technical components, tools, services or building blocks developed or operated by either agency;

   (c) the provision of technical support, expertise or services, including in the field of system development, testing, maintenance and security;

   (d) the establishment of joint project teams and the exchange of staff, expertise and other resources necessary for the implementation of common projects and technical activities.

3. Upon request by Europol in accordance with Article 86 of Regulation (EU) …/…. of the European Parliament and of the Council*, eu-LISA shall provide public key infrastructure certificates from eu-LISA's Certification Authority to Europol and, where appropriate, to the competent authorities of the Member States for the purposes of Europol's services, tools and applications.

4. Cooperation under paragraphs 1 to 3 shall take place within the framework of working arrangements setting out the practical modalities, including financial aspects, governance arrangements, arrangements for staff exchanges and temporary assignments, and the establishment and operation of joint project teams.'.

* Regulation (EU) …/… of the European Parliament and of the Council [*on the European Union Agency for Law Enforcement Cooperation (Europol), amending Regulations (EU) 2018/1726 and (EU) 2024/982, and repealing Regulation (EU) 2016/794*]'.

Article 136

Amendments to Regulation (EU) 2024/982

Article 49 of Regulation (EU) 2024/982 is amended as follows:

(1) in paragraph 5, the following second subparagraph is added:'

'Europol may conduct such searches using:

(a) data provided by third countries;

(b) data originating from Member States.';

(2) the following paragraphs are inserted:

'5a. For searches performed with DNA profiles, dactyloscopic data and facial images, Europol may only use data originating from Member States where authorised by the data-owning Member State. This authorisation may be granted in the following cases:

(a) on a case-by-case basis;

(b) pursuant to a standing authorisation, subject to conditions defined by the Member State.

5b. When conducting searches with biometric data originating from Member States, Europol shall act as a technical and forensic service provider on behalf of the authorising Member State and respecting any restrictions on access, transfer, transmission, deletion, destruction or further use of information indicated by that Member State.

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

'Where the procedures referred to in Articles 6, 11 or 20 show a match between the data used for the search and data held in the national database of the requested Member State or Member States, Europol shall inform only the Member State or Member States involved and, where applicable, the Member State or Member States that authorised the use of data pursuant to paragraph 6.';

(4) in paragraph 6, second subparagraph, point (c) is replaced by the following:

'(c) the name of the third country or Member State which provided the data has been transmitted.';

(5) paragraph 7 is replaced by the following:

'7. Europol's use of information obtained from a query made in accordance with this Article, and from the exchange of a set of core data in accordance with paragraph 6, shall be subject to the consent of the Member State in whose database the match occurred and, where applicable, of the Member State that authorised the use of data pursuant to paragraph 6. Where the Member State allows such information to be used, its handling by Europol shall be governed by Regulation (EU) …/… of the European Parliament and of the Council* [*this Regulation*].

* Regulation (EU) …/… of the European Parliament and of the Council [*on the European Union Agency for Law Enforcement Cooperation (Europol), amending Regulations (EU) 2018/1726 and (EU) 2024/982, and repealing Regulation (EU) 2016/794*]'.

Chapter XVI
Final provisions

Article 137

Start of operations

1. The Commission shall determine the date from which the Member States can start using the data loader solutions referred to in Article 38(3) to upload information to the Europol cross-checking service by means of an implementing act as referred to in paragraph 8 of that Article.

   The Commission shall determine, by means of the implementing act referred to in the first subparagraph, the date from which the Member States are to start using the data loader solutions.

   The Commission shall determine the date from which Europol is to start using the Europol cloud infrastructure referred to in Article 50, by means of an implementing act as referred to in paragraph 9 of that Article.

2. The Commission shall determine the date from which Europol and the Member States can start using the Police Shared Data Platform referred to in Article 42, by means of an implementing act as referred to in paragraph 5 of that Article.

   The Commission shall determine, by means of the implementing act referred to in the first subparagraph, the date from which Europol and the Member States are to start using the Police Shared Data Platform.

3. The Commission shall determine the date from which the Member States can start using the EU DNA matching application referred to in Article 54 by means of an implementing act as referred to in Article 49.

4. The Commission shall determine the date from which Europol, the Member States and the Commission are to start using the statistics and reporting tools referred to in Article 52, by means of an implementing act as referred to in paragraph 6 of that Article.

5. The Commission shall determine the date from which other Union bodies, offices and agencies are to start using the Hit/No-hit system referred to in Article 80, by means of an implementing act as referred to in paragraph 9 of that Article.

Article 138

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this Article, Article 5 of Regulation (EU) No 182/2011 shall apply. Where the committee delivers no opinion, the Commission shall not adopt the draft implementing act and Article 5(4), third subparagraph, of Regulation (EU) No 182/2011 shall apply.

Article 139

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 19 shall be conferred on the Commission for an indeterminate period of time from … [the date of entry into force of this Regulation].

3. The delegation of power referred to in Article 19 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Article 19 shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 140

Repeal

1. Regulation (EU) 2016/794 is repealed with effect from [date of application of this Regulation].

2. References to Regulation (EU) 2016/794 shall be construed as references to this Regulation.

Article 141

Entry into force and application

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

2. It shall apply from [date].

3. 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 AND DIGITAL STATEMENT- AGENCIES

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/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) 2018/1726 and Regulation (EU) 2024/982, and repealing Regulation (EU) 2016/794

1.2. Policy area(s) concerned

Policy area: Home Affairs

Activity: 12 Security

12 02 01: Internal Security Fund (ISF)

12 10 01: Europol

1.3. Objective(s)

1.3.1. General objective(s)

The general objective of this initiative is to strengthen Europol's capacity to support Member States in preventing and combating serious and organised crime and terrorism in an increasingly complex and cross-border security environment, and hence to contribute to the overall security and safety of the EU. In particular, it is to ensure that Europol can effectively provide operational and analytical support, facilitate information exchange, and contribute to coordinated EU responses to emerging and evolving criminal threats,

1.3.2. Specific objective(s)

Specific objective No 1

Reinforce Europol's role as an information hub for law enforcement

This objective aims to strengthen Europol's capacity to collect, process, analyse and share high-quality criminal information across borders. It seeks to improve the timeliness, interoperability and usability of information exchanges with Member States and EU bodies and agencies. The objective addresses fragmentation and under-utilisation of existing tools, while ensuring robust data protection and fundamental rights safeguards.

Specific objective No 2:

Europol as an operational hub

The objective is to strengthen Europol's capacity to provide timely, actionable and comprehensive operational support in investigations into serious and organised crime and terrorism. This includes enabling Europol to engage more effectively in cross-border cases, by strengthening its ability to identify operational links between national investigations, coordinate operational follow-up between Member States, and provide continuous criminal intelligence, analytical, technical, forensic and financial investigation support.

The aim is also to strengthen Europol's cooperation with Union bodies and agencies, in particular the European Public Prosecutor's Office (EPPO). It seeks to ensure a

continuum of Union-level support throughout the operational lifecycle by improving information flow, operational coordination, and the complementary use of Union-level capabilities

Specific objective No 3:

Europol as a technology and innovation hub

The proposal aims to strengthen Europol's capacity to support the competent authorities of the Member States along the full research, innovation and capability development cycle. This includes enabling Europol to identify common capability needs, drive research and innovation activities, support the testing, validation and scaling of innovative solutions, and develop or provide shared capabilities addressing common operational requirements. The aim is also to position Europol as a central platform for cooperation on technology and innovation, facilitating the pooling of expertise, resources and investments and supporting the strategic technological autonomy and resilience of the Union in the field of internal security.

1.3.3. General objective(s)

Overall impact:

The initiative is expected to improve the effectiveness, speed and coordination of cross-border investigations, enabling earlier identification of criminal actors and networks and more effective disruption of serious and organised crime and terrorism affecting the security of the Union. The initiative is also expected to strengthen the Union's capacity to detect and combat fraud, corruption, money laundering and other criminal activities that affect the financial interests of the EU.

As a result, **EU citizens** are expected to benefit from safer communities, better protection of victims, reduced infiltration of criminal networks into the economy and public institutions, lower financial and societal harm caused by criminal activities, and a more secure environment for businesses for legitimate economic activity and investment across the Union. The proposal does not contain regulatory obligations for citizens/consumers and does not create additional costs in that regard.

The proposal is expected to generate significant economies of scale for **public authorities** by pooling specialised operational, analytical, technical and digital forensic capabilities at EU level, thereby reducing duplication of resources and investments across Member States. National authorities will benefit from more efficient access to advanced expertise, operational support and technological capacities that would be costly and resource-intensive to develop individually at national level.

More specifically:

Benefits to **Member States law enforcement authorities and EU bodies and agencies:**

– Increased availability at Union level of relevant operational and analytical information supporting national and cross-border investigations.

– Earlier and more effective operational coordination in cross-border investigations, including faster initiation of operational cooperation, more timely judicial follow-up where needed, and joint analytical activities across Member States.

- Faster, more accessible and more operationally relevant support from Europol for national and joint investigations, including more timely, reliable and enriched operational analytical products, financial investigation support and operational follow-up.
- Improved identification of criminal networks, cross-border operational links and illicit financial flows across jurisdiction.
- More effective handling of complex investigations involving digital evidence and large unstructured datasets through increased access to specialised analytical, technical, forensic and digital forensic capabilities at Union level.
- Increased analytical and operational support to relevant Union bodies and agencies, in particular the European Public Prosecutor's Office, facilitating complementarity, coordinated investigative follow-up and more coherent Union-level action across the investigative and judicial lifecycle.
- Increased efficiency:
  - Increased share of national investigations benefiting from Union-level information, operational support and specialised capabilities.
  - Faster operational follow-up and reduced delays in cross-border investigations.
  - Reduced costs associated with access to specialised analytical, technical and digital forensic capabilities through economies of scale at Union level.
  - Reduced duplication of efforts and parallel investigations through improved information sharing, operational coordination and deconfliction mechanisms.
  - More efficient use of existing Union information systems through increased interoperability and shared operational use.
  - Reduced need for the development of separate analytical capacities by relevant Union bodies and agencies, in particular the EPPO, unless such latter capacities are made necessary by the specific mandate of the relevant Union bodies and agencies, through increased access to Europol's Union-level analytical capabilities.

Benefits to the **Union's internal security**:

- Strengthened capacity to anticipate, detect and respond to evolving serious and organised crime and terrorism.
- Earlier identification of criminal structures operating across multiple jurisdictions.
- Stronger evidential support for judicial proceedings through enhanced analytical, technical and forensic capabilities.
- Strengthened public trust in the Union's capacity to protect citizens, businesses and public finances against serious and organised crime.

1.3.4. Indicators of performance

Specify the indicators for monitoring progress and achievements.

Specific Objective 1:

- Europol maintains up to **5 standards** and reference guidance document on information exchange (number of standards and guidance on data format and exchange actively supported by Europol; baseline 0; target 5.)
- Half of the criminal investigators in EU have been issued an **EU digital Police ID** and given **an effective access to the EU Police Shared Data Space** (share of police officers in the EU with criminal investigative powers registered as users of the EU Police Shared Data Space; baseline 0%; target 50%)
- Half of the criminal investigations warranting the use of high-end analytical tools **rely on tools made available by Europol** (share of criminal cases opened within the year across the EU for which investigations relied on analytical tools either jointly procured or made available online by Europol through the EU Police Shared Data Space; baseline 0%; target 10%[84])
- All individuals found **suspect or convicted** of a criminal offense[85] over the year have been **checked against Europol data**, in every Member State (number of Member States for which the ratio "number of yearly searches into Europol databases" against Eurostat figures on persons suspect or offender within the year is over 1.00; baseline 1; target = 26)
- Law enforcement authorities have **systematically followed-up with other Member States** for cross-border cases (number of Member States for which the ratio "new cross border cases initiated such as with SIENA, or JOAC…" against "new cases over the year having triggered a hit in Europol databases" is over 0.90; target = 26)
- Law enforcement authorities have **provided information to Europol** on cross-border case half of the times (number of Member States for which the ration "provision of information to Europol via SIENA or other means" vs "number of new cases over the year having triggered a hit in Europol database" is over 50%; baseline = 5; target = 26)
- The information on all individuals convicted of a criminal offense over the year has been **shared with Member States and Europol** into Europol information system (ratio "records uploaded or updated into EIS within the year" against Eurostat number of persons convicted; target = 100%)

Specific Objective 2:

- Increased share of cross-border investigations benefiting from Europol's operational, analytical or technical support.
  (target: +30%)
- Reduction in the average time between receipt of operational information by Europol and dissemination of analytical outputs to Member States *(target: < 24 hours*)
- Increased number of investigations involving digital evidence supported through Europol analytical and digital forensic capabilities

84 Commission assessment that 10% to 15% of criminal investigation warrants the use of AI tools.

85 Offences, suspects and offenders, as defined https://ec.europa.eu/eurostat/cache/metadata/en/crim_sims.htm.

(target: +50%)

- Increased number or value of financial investigations, asset tracing or asset recovery cases supported by Europol. *(target: +40%)*
- Number of cases in which Europol issues proposals for urgent freezing or asset-preservation measures to Member States' Asset Recovery Offices.
- Increased number of operational links identified by Europol between investigations conducted in different Member States. *(target: +40%)*
- Increased number of national investigations supported directly through Europol Support Offices.
- Increased share of cases handled by the EPPO requiring analytical support that benefit from Europol. (target: 90%)

Specific Objective 3:

- Number of capability gaps and technology development priorities identified through the Foresight and Capability Development Framework leading to concrete follow-up actions at Union or Member State level. *(target: 10 actions/year)*
- Number of advanced capabilities or technological solutions made available by Europol for operational use by Member States. *(target: 5/year)*
- Number of specialised training activities supported by Europol on advanced technologies, digital investigations and forensic capabilities. *(target: 6/year)*

1.4. The proposal/initiative relates to:

☐ a new action

☐ a new action following a pilot project / preparatory action[86]

☒ the extension of an existing action

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

1.5. Grounds for the proposal/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 initiative

The implementation of the legislative initiative will require the progressive deployment of legal, organisational, operational and technological measures at Union and national level. The roll-out should start upon the entry into force and application of the Regulation and will require a gradual scaling-up of resources, in particular human and ICT resources, in line with the increasing demand for Europol services and capabilities.

[86] As referred to in Article 58(2), point (a) or (b) of the Financial Regulation.

Implementation will notably require: (i) the adoption of tertiary legislation and technical standards; (ii) the establishment of new governance, operational support and capability-development structures within Europol; (iii) major investments in secure, interoperable and cloud-based information management and analytical infrastructures; (iv) the progressive development and deployment of advanced analytical, artificial intelligence-enabled and digital forensic capabilities; and (v) the integration of Europol services, systems and operational support into national investigative workflows and cross-border law enforcement cooperation mechanisms.

The implementation will also require reinforced cooperation and updated working arrangements between Europol, and relevant Union bodies and agencies, notably the European Public Prosecutor's Office.

Indicative milestones are counted from the year of entry into application of the new Regulation, and referred to Y.

Commission:

– **Y+1** and subsequent years: adoption of tertiary legislation, notably on the information hub (SO1).

Europol organisational, operational and governance measures:

– **Y:** establishment of the ICT and Information Management Steering and Advisory Groups, the Capabilities and Innovation Advisory Group and the Executive Board.

– **Y:** establishment of a dedicated operational capability supporting EPPO-related cases.

– **Y+3:** fully staffed and structured EPPO operational support capability.

– **Y:** simplified rules on data subject categorisation become applicable.

– **Y:** establishment of Union Centres of specialised expertise, Operational and Analysis Service (SO2) and Capabilities and Innovation Service (SO3), including adoption by the Management Board of relevant implementing rules.

– **Y+3:** full staffed Union Centres of specialised expertise, Operational and Analysis Service (SO2) and Capabilities and Innovation Service (SO3).

– **Y:** establishment of Europol Support Offices in Member States.

– **Y+1 to Y+3**: staff seconded to national Europol Support Office.

– **Y+1 to Y+3:** update of relevant working arrangements between Europol and Union bodies.

– **Y+3 to Y+4:** progressive development, together with relevant Union bodies, of automated hit/no-hit cross-checking mechanisms against Europol data.

– **Y+1:** development of specialised EU-level support for national authorities seeking to obtain electronic evidence from online service providers.

Europol capability development, ICT, innovation:

– **Y+1:** establishment of the Foresight and Capability Development Framework and central joint procurement capability for technical components (SO3).

- **Y+2**: first update of the UMF standard under Europol leadership and availability of the DNA capability (SO1).
- **Y+2:** establishment of a scalable and secure hybrid cloud infrastructure at Basic Protection Level (BPL) equivalent to sensitive non-classified information.
- **Y+5:** extension of the cloud infrastructure to classified information environments.
- **Y+2**: first integration test with a national police identity credential.
- **Y+3 to Y+5:** progressive integration of national police digital identity credentials.
- **Y+2:** migration of a first major information management platform and analytical tools to the cloud infrastructure.
- **Y+3 to Y+5:** progressive migration of remaining Europol systems and analytical tools to the cloud infrastructure at BPL level.
- **Y+6:** migration of relevant systems to classified cloud environments.
- **Y+1 to Y+6:** gradual upgrade of core information management and analytical platforms, including SIENA, cross-matching services and the Europol analytical environment, through enhanced automation, artificial intelligence-enabled functionalities, improved usability, increased performance, data standardisation and expanded biometric functionalities.
- **Y:** first enhanced interconnection with national databases under Prüm II using a first biometric modality.
- **Y+2:** extension to additional biometric modalities.
- **Y to Y+6:** progressive expansion of innovative and AI-based analytical tools available to Europol and Member States.
- **Y onwards:** progressive consolidation of open-source intelligence (OSINT) capabilities.

Member States:

- **Y to Y+7** (continuous)**:** Progressively adjust their national organisation and introduce or reinforce automation for information exchange with Europol.
- **Y to Y+7** (continuous)**:** Upgrade of national systems and criminal investigation workflows to progressively integrate Europol services, analytical tools and interoperability standards.
- **Y+1:** first Member States upgrade national law enforcement digital credentials in line with harmonised Union standards.
- **Y+2 to Y+4:** progressive issuance of the EU Digital Police ID to national criminal investigators.
- **Y+6:** all national systems connected to Europol require prior authentication through the EU Digital Police ID.
- **Y+1:** harmonisation of investigators' digital endpoints to facilitate access to EU Police Cloud infrastructure, platforms and tools.

– **Y:** establishment and hosting of Europol Support Offices by Member States.

Union bodies:

– **Y+1 to Y+3:** update of relevant working arrangements with Europol.

– **Y:** the EPPO to progressively implement the technical and organisational measures necessary to support enhanced operational cooperation and access to Europol analytical support.

– **Y+3 to Y+4:** progressive development, together with Europol, of automated hit/no-hit cross-checking mechanisms.

1.5.2. Added value of EU involvement

Ex ante EU added value:

Serious and organised crime and terrorism increasingly operate across borders, rely on digital technologies and infrastructures, and exploit differences between national legal, operational and technical frameworks. The scale, speed and complexity of these threats require coordinated action, interoperable systems and shared capabilities at Union level. Action by Member States alone would not be sufficient to ensure effective cross-border operational coordination, large-scale criminal intelligence analysis, or the development and deployment of advanced technological and analytical capabilities across the Union.

EU added value of the existing legal framework:

The evaluation of the current legal framework confirmed, based on a large stakeholder consultation, that Europol delivers a clear EU added value by serving as a centralised platform for criminal intelligence sharing and cross-border operational coordination. Its infrastructure enables real-time information exchange among Member States, helping identify links between investigations that would otherwise remain undetected. Without Europol, cooperation would depend on slower, less effective bilateral channels, making it harder to combat sophisticated transnational criminal networks. Stakeholders agree that Europol's analytical and coordination support significantly improves the efficiency of cross-border investigations compared to national or bilateral efforts alone.

According to the evaluation, Europol also provides specialised EU-level capabilities, such as digital forensics, financial intelligence, and cybercrime expertise, which many Member States, particularly smaller or less-resourced ones, could not develop independently. This pooling of resources avoids duplication and ensures all Member States benefit from advanced tools. Case studies show that Europol's involvement often proves critical in dismantling complex criminal networks operating across multiple jurisdictions. Additionally, it acts as a single gateway for EU-international law enforcement cooperation, reducing the need for multiple bilateral agreements.

EU added value of the proposed action

The proposed action provides clear added value at Union level by establishing common operational, technical and interoperability frameworks that cannot be effectively developed through isolated national measures or bilateral cooperation arrangements. In particular, the development of harmonised standards for law enforcement digital credentials, digital endpoints, data formats and investigative data

workflows requires Union-level coordination to ensure interoperability, secure information exchange and coherent cross-border investigations across Member States and relevant Union bodies.

The proposal also provides added value by enabling Union-level operational support, coordination and cross-checking mechanisms based on Europol data and information systems. Enhanced access to, and operational use of, Europol capabilities by Member States and relevant Union bodies, notably the EPPO can by their nature only be organised effectively at Union level.

In addition, the proposal generates economies of scale by pooling advanced technological, analytical and digital forensic capabilities at Union level, including artificial intelligence-based tools, secure cloud infrastructures, advanced forensic technologies and joint procurement mechanisms. This reduces duplication of investments and operational fragmentation across Member States and allows capabilities to be developed and deployed more efficiently and at lower cost than through parallel national solutions.

.

1.5.3. Lessons learned from similar experiences in the past

The evaluation of the current legal framework, and notably the stakeholder consultation, confirmed that:

- **EU-level coordination is indispensable.** As transnational crime demands structured, centralised cooperation (and national efforts alone are insufficient) Europol's criminal intelligence-sharing systems and operational and analytical capabilities are critical for effective cross-border investigations.
- **Advanced technological and analytical capabilities are essential.** With the rising relevance of digital evidence, encryption, and cybercrime requiring specialised expertise beyond individual Member States' capacities, Europol must continuously innovate (e.g., digital forensics, AI-driven analysis) to be able to meet Member States' operational needs.
- **Systematic, automated information sharing must be strengthened.** Inconsistent data-sharing practices among Member States reduce operational effectiveness, which could be addressed by a greater use of automated exchange systems and standardised procedures.
- **Coherence within the EU security framework is crucial:** Clear mandates, aligned data-protection rules, and efficient information exchange are needed for seamless cooperation between Europol and other Union bodies.
- **REFIT principles should guide procedural efficiency.** Simplifying processes, enhancing interoperability, and reducing administrative burdens would boost operational speed. Digital tool upgrades (e.g., AI, secure data platforms) should therefore be prioritised to support real-time collaboration.

Therefore, Europol's **current legal framework remains effective** but needs to **evolve to address emerging threats and operational needs**. Future adaptations should focus on technology, interoperability, and streamlined cooperation to ensure the resilience of the EU security framework.

In view of ensuring an effective implementation of the proposed measures, past experience has also shown the importance of ensuring clear governance structures,

robust prioritisation mechanisms and effective coordination between Europol, Member States, the Commission and other relevant Union bodies to avoid duplication of efforts and ensure coherent operational and technological development at Union level.

In addition, experience from previous capability development and ICT modernisation projects demonstrated the need for clear allocation and traceability of Union resources across operational and technological support activities, combined with strong monitoring, reporting and accountability arrangements. The proposal therefore reinforces governance, planning and reporting mechanisms. Moreover, there are clear synergies that can be achieved in ICT projects through the cooperation between Europol and eu-LISA, the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. Building on its expertise, experience and cooperation with external service providers, eu-LISA can effectively and efficiently provide Europol with services related to Information Management and ICT. To that end, the proposal establishes a structured cooperation between Europol and eu-LISA when it comes to the development, deployment and operation of information systems and related communication infrastructure.

1.5.4. Compatibility with the multiannual financial framework and possible synergies with other appropriate instruments

In the Political Guidelines for the 2024-2029 European Commission, the President of the European Commission announced the objective "to make Europol a truly operational police agency and more than double its staff over time. This should come with a strengthened oversight and mandate", to enhance support to national law enforcement authorities.

On 16 July 2025, the Commission presented its proposal for the Multiannual Financial Framework[87] ("MFF") for 2028-2034 amounting to almost EUR 2 trillion. In light of the increasing security threats facing the Union and the demonstrated added value of coordinated EU and Member State action in the area of internal security, the proposed MFF aims to support the implementation of ProtectEU – a European Internal Security Strategy and to strengthen the EU prevention, preparedness and response capacity.

Within that framework, the Commission proposed a significant reinforcement of the resources allocated to Justice and Home Affairs decentralised agencies including Europol.

The figures presented in this LFDS exclusively concern the additional financial and human resources required to implement the new measures introduced by the proposal compared to the current Europol Regulation[88]. The proposal is estimated to require additional resources for Europol and for eu-LISA, linked to the implementation of the tasks delegated to the agency in this Regulation, amounting to approximately **EUR 1.053 billion** and **910 additional staff**[89] posts over the 2028-2034 MFF,

[87] COM(2025) 570 final; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0570

[88] 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) http://data.europa.eu/eli/reg/2016/794/2026-01-11

[89] In principle, the governance functions of Europol are expected to remain broadly stable in staffing terms. The proposal is expected to generate efficiency gains, notably through the simplification and

compared to the 2027 baseline budget amounting to 1 226 staff and EUR 256.557 million in appropriations.

Those figures should therefore be read together with the resources necessary to implement the existing measures under the current legal framework, estimated at EUR 1.946 billion and 1 226 staff over the 2028-2034 MFF, based on the 2027 annual budget projected over seven years with a 2% annual inflation rate. When summed, those amount to a global envelope of **EUR 2.999 billion** over the next MFF and 2 336 staff at the end of the 2034, which align with Commission legislative proposal for the 2028-2034 MFF

The activities to be carried out by Member States over the same period in support of enhanced interoperability, integration of Europol systems into national investigative workflows, deployment of digital police credentials and reinforced information exchange capacities are estimated at approximately EUR 590 million over the first seven years implementation period, notably for the adaptation of national systems, workflows and technical interfaces necessary to support more integrated and automated cooperation with Europol systems and tools.

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the 2028-2034 MFF and thereafter shall be determined through the annual budgetary procedure. All appropriations and staffing allocations as of 2028 are indicative.

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

The 2022 revision of Europol's mandate represented a significant step towards modernising the Agency's mandate, notably by reinforcing its capacities in data processing, innovation and support in response to the increasingly digital, cross-border and complex nature of serious and organised crime and terrorism. That revision was accompanied by an increase of approximately EUR 178 million compared to the EUR 1 285 million budget initially adopted for Europol in the 2021-2027 MFF proposal, corresponding to an increase of 14%.

Since then, the operational environment has evolved significantly. Criminal networks have rapidly expanded their use of digital technologies, artificial intelligence, encrypted communications and online infrastructure, while increasingly combining cyber-enabled crime, financial crime, trafficking and other illicit activities into highly adaptive and transnational criminal models. At the same time, the volume and strategic importance of operational data in criminal investigations have increased substantially. This has led to a continuous increase in Member States' and Union bodies' expectations regarding Europol's operational, analytical, technological, forensic and coordination support, resulting in repeated requests for annual reinforcements of Europol's budget and staffing beyond the levels initially programmed under the current MFF.

This proposal introduces substantial new operational, technological and capability-

streamlining of procedures relating to data protection, thereby limiting additional staffing needs for horizontal governance and administrative functions.

development tasks, while also integrating and consolidating existing activities within a more coherent operational and governance framework. Achieving the intended operational impact and strengthening the Union's law enforcement capabilities accordingly requires substantial additional investments in specialised staff, advanced technological infrastructure, secure cloud and analytical environments, artificial intelligence-enabled tools and operational support mechanisms. Such investments cannot be accommodated within the current financial envelope and therefore require additional financial support from the Union budget.

All estimations of additional resource needs under the proposal are based on Europol's 2027 baseline budget, including operational appropriations and staff. The Commission has carried out an extensive assessment of redeployment possibilities within the Agency to identify whether the new tasks introduced by the proposal could be accommodated within the existing resource framework. That assessment concluded that Europol is already operating at or close to maximum operational capacity. In particular, the Management Board already adopted reprioritisation measures in 2024 in response to resource constraints. In this context, no significant redeployment possibilities were identified that would allow Europol to absorb the additional tasks envisaged by the proposal without negatively affecting the implementation of existing operational activities and support to Member States.

Consequently, the proposal foresees additional financial and human resources for Europol over the next MFF period to ensure the sustainable implementation of the revised mandate and avoid structural underfunding of the Agency's expanded responsibilities.

The implementation of the proposal will entail additional activities for eu-LISA to provide Europol with services related to Information Management and ICT. Consequently, the proposal provides for targeted changes of the mandate of eu-LISA and foresees that a limited number of additional human resources for eu-LISA over the next MFF period to ensure the sustainable implementation of the structured cooperation between Europol and eu-LISA as set out in the revised mandates of the Agencies. At this point, it is not possible to quantify the operational expenditure for these activities to be allocated to eu-LISA, as it is not yet clear which services exactly Europol would implement through the services provided by eu-LISA. Therefore, operational expenditure for these activities to be allocated to eu-LISA from the total operation expenditure foreseen in this LFDS will be assessed at a later date.

The implementation of the proposal will also entail additional activities for the Commission services, notably the Directorate-General for Migration and Home Affairs (DG HOME), in relation to governance, oversight, policy coordination and the preparation and adoption of implementing acts. Additional support will also be required from the Directorate-General for Digital Services (DG DIGIT), notably regarding the establishment and management of ICT supply chain and cloud-computing contractual frameworks supporting Europol's technological infrastructure.

1.6. Duration of the proposal/initiative and of its financial impact

☐ **limited duration**

– ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

☒ **unlimited duration**

– Implementation with a start-up period from YYYY to YYYY,

– followed by full-scale operation.

1.7. Method(s) of budget implementation planned

☒ **Direct management** by the Commission

– ☒ by its departments, including by its staff in the Union delegations;

– ☐ by the executive agencies

☐ **Shared management** with the Member States

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

– ☐ third countries or the bodies they have designated

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

– ☐ the European Investment Bank and the European Investment Fund

– ☒ bodies referred to in Articles 70 and 71 of the Financial Regulation

– ☐ public law bodies

– ☐ bodies governed by private law with a public service mission to the extent that they are provided with 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 are provided with adequate financial guarantees

– ☐ bodies or persons entrusted with the implementation of specific actions in the common foreign and security policy pursuant to Title V of the Treaty on European Union, and identified in the relevant basic act

– ☐·bodies established in a Member State, governed by the private law of a Member State or Union law and eligible to be entrusted, in accordance with sector-specific rules, with the implementation of Union funds or budgetary guarantees, to the extent that such bodies are controlled by public law bodies or by bodies governed by private law with a public service mission, and are provided with adequate financial guarantees in the form of joint and several liability by the controlling bodies or equivalent financial guarantees and which may be, for each action, limited to the maximum amount of the Union support.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

The monitoring and reporting of activities implemented by Europol under indirect management will follow the provisions laid down in the new Europol's Regulation,

the Financial Regulation[90] and in line with the Common Approach on decentralised agencies[91].

Europol will annually submit a Single Programming Document (SPD) to the Commission, the European Parliament, and the Council, setting out its multiannual and annual work programmes, objectives, expected results, and performance indicators. This document is prepared taking into account the opinion of the Commission and the Joint Parliamentary Scrutiny Group (JPSG). Additionally, Europol will adopt a Consolidated Annual Activity Report (CAAR), which assesses progress against the SPD's objectives. The Management Board approves this report before it is transmitted to the Commission, the European Parliament, the Council, the Court of Auditors, and national parliaments by 1 July each year.

Under the proposed Article 130 of the revised Europol Regulation, the Commission will conduct an evaluation of Europol every five years, assessing its added value, impact, effectiveness, efficiency, and working methods. The evaluation may propose structural or operational modifications, including financial implications. The Commission submits its report to the Management Board, which provides observations within three months. The final report, along with the Commission's conclusions and the Board's observations, is then sent to the European Parliament, Council, national parliaments, and Management Board, with key findings made public where appropriate.

The proposal further reinforces the role of the Management Board in defining and monitoring the performance indicators, objectives and implementation priorities set out in the SPD, the corresponding annual work programmes and the Consolidated Annual Activity Report. To support those functions, the proposal establishes an Executive Board and specialised ICT and Information Management Steering structures responsible for supporting strategic oversight, budgetary monitoring and follow-up of operational and technological implementation. The proposal also strengthens the link between performance reporting and strategic programming by aligning the evaluation criteria of the CAAR more closely with the objectives and performance indicators established under the SPD and with the establishment of the annual budget.

Finally, the proposal further enhances Europol's governance, monitoring and accountability framework. It reinforces the oversight role of the Management Board by extending its supervision beyond performance indicators to the effective exercise of the powers conferred on the Executive Director, and to the monitoring of strategic and operational priorities. The Management Board will also be able to take action where concerns are raised by at least one third of its members regarding a specific operational or governance issue.

To support transparency, accountability and effective cooperation between Member States and Europol, Europol will report annually to the Commission, the European Parliament, the Council and national parliaments on the information contributed by Member States, including in relation to Union priority crime areas. Those reports will be based on quantitative and qualitative criteria established by the Management Board. The Joint Parliamentary Scrutiny Group (JPSG) will continue to exercise political scrutiny over Europol's activities, notably with regard to operational

[90] Financial regulation applicable to the general budget of the Union

[91] Joint Statement on decentralised agencies.

effectiveness, accountability and compliance with fundamental rights obligations.

2.2. Management and control system(s)

2.2.1. Justification of the budget implementation method(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. 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 the European Anti-Fraud Office (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.

Based on the evaluation of the current legal framework, the Impact Assessment accompanying the proposal for a new Europol Regulation, and the significant increase in financial and human resources expected to support the implementation of the proposal, additional governance, management and control mechanisms are introduced to strengthen financial oversight, accountability and compliance with principles of sound financial management:

- Under the proposed framework, where the European Commission considers that a draft decision of the Management Board, including the Single Programming Document (SPD), raises concerns regarding compliance with Union law, Europol's mandate or principles of sound financial management, it may request the Management Board to reconsider the draft decision before its adoption.
- The Management Board is empowered with disciplinary authority over the Executive Director, thereby strengthening accountability regarding operational and financial management.
- the proposal establishes an Executive Board responsible, inter alia, for monitoring follow-up to findings and recommendations resulting from internal

and external audits, including investigations conducted by OLAF and EPPO, and for preparing and, where necessary, adopting provisional budgetary decisions subject to subsequent validation by the Management Board.

These measures are intended to strengthen internal control, financial governance and oversight of Europol's budgetary implementation.

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

The following risks are identified:

- Imbalances between short-term operational needs and long-term strategic investments, notably concerning the migration towards secure cloud infrastructures and automation of operational workflow.
- Misalignment between legal obligations, strategic priorities, multiannual planning and annual implementation, notably in the domain of Information Management and ICT capabilities.
- Pressure on operational resources resulting from increasing data volumes, operational requests and evolving security threats.
- Capacity for Europol to reinforce staff and competences on IM and ICT and address broadening of the agency's mission and tasks.
- Delays in recruitment and retention of specialised ICT and analytical staff necessary to support major technological developments.
- Increasing costs of ICT maintenance.
- Lack of long-term ICT asset management and procurement strategy.
- Additional compliance and conformity costs linked to the deployment of advanced analytical and artificial intelligence-enabled tools under the Union regulatory framework, including the AI Act.
- Increased workload related to the handling of data subject access requests.
- Dependencies on the timely implementation of technical and organisational arrangements by other Union bodies and agencies, notably EPPO.

Regarding mitigation measures:

- 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, including as regards risk assessment. The CAAR 2024 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.

- 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.
- The Executive Board, introduced by the legal proposal, plays a critical auditing role by monitoring and ensuring accountability in Europol's financial operations. It is responsible for overseeing the implementation of Europol's budget, ensuring compliance with financial rules and sound financial management principles, while preparing financial and budgetary decisions for adoption by the Management Board. A key function is its obligation to ensure adequate follow-up to findings and recommendations from internal and external audits, and investigations conducted by OLAF and EPPO, thereby reinforcing financial integrity and transparency. While the Board itself does not conduct audits, it reviews audit reports, assesses their implications, and proposes corrective measures to address identified weaknesses or irregularities, thereby acting as a gatekeeper for financial probity within Europol.
- Finally, the ICT and Information Management steering group and advisory group and the Innovation and Capability advisory group will support the Management Board in delineating activities and sub activities related to budget planning and execution of the Agency's mandate and strategic priorities, notably by identifying concrete and representative indicators for the Agency's activity in the domain, and the monitoring of the Agency's implementation of the ICT related objectives and tangible deliverables.

2.2.3. Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and the 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 payments" is reported on by the Commission. The 2024 AAR of DG HOME reports 0.10% 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 2024, 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

The proposal includes measures to ensure sound financial management and prevent

fraud, irregularities and conflicts of interest in the implementation of Union funding and operational activities, notably Article 128 and the financial provisions under Chapter XII.

Within this legal framework, the Management Board of Europol is required to adopt and regularly update an internal anti-fraud strategy. Europol adopted an updated anti-fraud strategy on 25-26 June 2025. In accordance with that framework, Europol will continue to participate in fraud prevention activities carried out by OLAF and report suspected fraud and financial irregularities to the Commission without delay.

The proposal also strengthens internal governance and financial oversight through the establishment of an Executive Board responsible for monitoring audit findings and ensuring follow-up to audit and control recommendations. In addition, the Commission retains powers to object to Management Board decisions that may give rise to risks of financial mismanagement or non-compliance with Union law.

Europol's activities will remain subject to the applicable Union financial, audit, data protection and accountability frameworks, including oversight and investigations by OLAF, EPPO, the Court of Auditors and the Europol Cooperation Board.

DG HOME will continue to apply its Anti-Fraud Strategy in line with the Commission's Anti-Fraud Strategy (CAFS), which also covers decentralised agencies within its remit, including Europol.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and thereafter shall be determined through the annual budgetary procedure. All appropriations and staffing allocations as of 2028 are indicative.

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			
	1: Economic, social and territorial cohesion, agriculture, rural and maritime prosperity and security	Diff./Non-diff.[92]	from EFTA countries [93]	from candidate countries and potential candidates [94]	From other third countries	other assigned revenue
	Decentralised agencies Europol	Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO

[92] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.
[93] EFTA: European Free Trade Association.
[94] Candidate countries and, where applicable, potential candidates from the Western Balkans.

3.2 Estimated financial impact of the proposal on appropriations

3.2.1. Summary of estimated impact on operational appropriations

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

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

3.2.1.1. Appropriations from voted budget

EUR million (to three decimal places)

Heading of multiannual financial framework	1	Economic, social and territorial cohesion, agriculture, rural and maritime prosperity and security / National and Regional Partnership Plans

EUR million (to three decimal places)

[Agency]: Europol	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**
Budget line: 12 10 01 Europol / EU Budget contribution to the agency[95]	**57.512**	**92.346**	**120.831**	**150.385**	**178.830**	**207.164**	**234.384**	**1041.452**
Budget line: 11 10 02 eu-LISA / EU Budget contribution to the agency[96]	**0.756**	**1.687**	**1.863**	**1.863**	**1.863**	**1.863**	**1.863**	**11.758**
Total Europol and eu-LISA	**58,268**	**94,033**	**122,694**	**152,248**	**180,693**	**209,027**	**236,247**	**1053,21**

	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**

[95] Commitments and Payments are identical.

[96] Commitments and Payments are identical.

TOTAL operational appropriations (including contribution to decentralised agency)	Commitments	(4)	58,268	94,033	122,694	152,248	180,693	209,027	236,247	**1053,21**
	Payments	(5)	58,268	94,033	122,694	152,248	180,693	209,027	236,247	**1053,21**
TOTAL appropriations of an administrative nature financed from the envelope for specific programmes		(6)	0	0	0	0	0	0	0	**0**
TOTAL appropriations under HEADING 1 of the multiannual financial framework	Commitments	=4+6	58 268	94 033	122 694	152 248	180,693	209,027	236,247	**1053,21**
	Payments	=5+6	58 268	94 033	122 694	152,248	180,693	209,027	236,247	**1053,21**

EUR million (to three decimal places)

Heading of multiannual financial framework	4	'Administrative expenditure'

EUR million (to three decimal places)

DG: HOME		Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**
Human resources		0.496	0.496	0.690	0.690	0.884	0.884	1.078	**5.218**
Other administrative expenditure		0.268	0.518	0.268	0.518	0.268	0.518	0.268	**2.626**
TOTAL DG HOME		**0.764**	**1.014**	**0.958**	**1.208**	**1.152**	**1.402**	**1.346**	**7.844**

TOTAL appropriations under HEADING 4 of the multiannual financial framework (Total commitments = Total payments)	**0.764**	**1.014**	**0.958**	**1.208**	**1.152**	**1.402**	**1.346**	**7.844**

EUR million (to three decimal places)

		Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL MFF 2028-2034**
TOTAL appropriations under HEADINGS 1 to 4	Commitments	**59 032**	**95 047**	**123 652**	**153 456**	**181 845**	**210 429**	**237 593**	**1 061 054**
of the multiannual financial framework	Payments	**59 032**	**95 047**	**123 652**	**153 456**	**181 845**	**210 429**	**237 593**	**1 061 054**

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and thereafter shall be determined through the annual budgetary procedure. All appropriations and staffing allocations as of 2028 are indicative.

3.2.2. Estimated output funded from operational appropriations

The additional operational appropriations and resources required exclusively for Europol to reach the three different Specific Objectives and implement the corresponding actions, and for eu-LISA linked to the implementation of the tasks delegated to the agency in this Regulation, amount to EUR 1,053 billion and 910 additional staff under the budget of both agencies. Those additional appropriations and resources add up to the cost of existing measures of Europol's budget (EUR 1,946 billion and 1226 staff) to an overall sum of EUR 2.999 billion and 2 126 staff

under the Europol budget, and 10 additional staff for the eu-LISA budget linked to the implementation of the tasks delegated to the agency in this Regulation. Those additional operational appropriations and resources will be fully dedicated to support:

– **SO1**: Europol's Information Management and ICT.

– **SO2**: the Union Centres of specialised expertise, Europol Support Offices, EPPO-dedicated support.

– **SO3**: Europol's research, innovation and capability-building capacity.

At the same time, governance functions of Europol are expected to remain broadly stable in staffing terms, due to efficiency gains generated by the proposal, notably through the simplification and streamlining of procedures relating to data protection, thereby limiting additional staffing needs for horizontal governance and administrative functions.

Specific Objective	**Cost**	**EUR million**	**Staff**
N/A	Baseline 2027	**1 796,200**	**1 226**
	Inflation	**149,590**	**0**
	Existing measures	**1 945,790**	**1 226**
SO1	Upgrade to existing systems and tools	**130,070**	**115**
	Access to national databases	**37,857**	**53**
	Integration with national systems	**25,400**	**34**
	EU Digital Police Cloud	**415,415**	**194**
SO2	Europol support offices	**112,163**	**157**
	Union Centres of specialised expertise	**118,703**	**171**
	Inter-agency cooperation	**18,801**	**26**
	EPPO-dedicated support	**40,895**	**70**
SO3	Advanced capabilities	**117,615**	**50**
	Technical support & procurement	**36,292**	**40**
	New measures	**1 053,210**	**910**
	TOTAL	**2 990,000**	**2 136**

3.2.3 *Summary of estimated impact on administrative appropriations*

– ☐ 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

3.2.3.1. Appropriations from voted budget

VOTED APPROPRIATIONS	Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034	TOTAL 2028 - 2034
HEADING 4								
Human resources	0.496	0.496	0.690	0.690	0.884	0.884	1.078	**5.218**
Other administrative expenditure	0.268	0.518	0.268	0.518	0.268	0.518	0.268	**2.626**
Subtotal HEADING 4	**0,764**	**1,014**	**0,958**	**1,208**	**1,152**	**1,402**	**1,346**	**7,844**
Outside HEADING 4								
Human resources	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Other expenditure of an administrative nature	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Subtotal outside HEADING 4	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**	**0.000**
TOTAL	**0,764**	**1,014**	**0,958**	**1,208**	**1,152**	**1,402**	**1,346**	**7,844**

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that 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.

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and thereafter shall be determined through the annual budgetary procedure. All appropriations and staffing allocations as of 2028 are indicative.

3.2.4. *Estimated requirements of human resources*

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

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

3.2.4.1. Financed from voted budget

Estimate to be expressed in full-time equivalent units (FTEs)

VOTED APPROPRIATIONS	Year 2028	Year 2029	Year 2030	Year 2031	Year 2032	Year 2033	Year 2034
• Establishment plan posts (officials and temporary staff)							
20 01 02 01 (Headquarters and Commission's Representation Offices)	2	2	3	3	4	4	5
20 01 02 03 (EU Delegations)	0	0	0	0	0	0	0

(Indirect research)		0	0	0	0	0	0	0
(Direct research)		0	0	0	0	0	0	0
Other budget lines (specify)		0	0	0	0	0	0	0
• External staff (in FTEs)								
20 02 01 (AC, END from the 'global envelope')		1	1	1	1	1	1	1
20 02 03 (AC, AL, END and JPD in the EU Delegations)		0	0	0	0	0	0	0
Admin. Support line [XX.01.YY.YY]	• at Headquarters	0	0	0	0	0	0	0
	• in EU Delegations	0	0	0	0	0	0	0
(AC, END - Indirect research)		0	0	0	0	0	0	0
(AC, END - Direct research)		0	0	0	0	0	0	0
Other budget lines (specify) - Heading 4		0	0	0	0	0	0	0
Other budget lines (specify) - Outside Heading 4		0	0	0	0	0	0	0
TOTAL		**3**	**3**	**4**	**4**	**5**	**5**	**6**

Considering the overall strained situation in Heading 4, in terms of both staffing and the level of appropriations, the human resources required will be met by staff from the DG who are already assigned to the management of the action and/or have been redeployed within the DG or other Commission services.

The staff required to implement the proposal (in FTEs):

	To be covered by current staff available in the Commission services	**Exceptional additional staff***		
		To be financed under Heading 4 or Research	**To be financed from BA line**	**To be financed from fees**
Establishment plan posts	5		N/A	
External staff (CA, SNEs, INT)	1			

Description of tasks to be carried out by:

Officials and temporary staff	2 AD in setup phase dedicated for the 2028-2029 period in charge of the adoption of the secondary legislation, maintained in the "running" phase, to cater for the growing implementing acts related to Information Management platforms and systems, which need to be adapted on a regular basis in line with

	constant evolution of law enforcement tools notably related to forensics and analytics, and the corresponding data protection aspects 1 AD specialist in cost accounting and IM and R&I strategy, in relation to both Executive IM and ICT Steering group 1 AD with budgetary skills to support doubling of the representation to the MB, to the creation of the Executive Board and additional monitoring obligations 1 AST: support and preparation of the additional meetings and briefings of the additional bodies (14+ per year)
External staff	1 SNE: expertise support in information management, data protection, research and innovation: participate to IM and ICT advisory group

The estimated impact on expenditure and staffing for 2028 and beyond is added for illustrative purposes only and does not pre-judge the next Multiannual Financial Framework. The source of financing and scope of Union financial commitment in the post-2027 period remain subject to the outcome of interinstitutional negotiations on the MFF 2028-2034 and thereafter shall be determined through the annual budgetary procedure. All appropriations and staffing allocations as of 2028 are indicative.

3.2.5. Overview of estimated impact on digital technology-related investments

3.2.6. Compatibility with the current multiannual financial framework (not to be completed for decentralised agencies)

3.2.7. Third-party contributions

The proposal/initiative:

– ☒ does not provide for co-financing by third parties

– ☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	Total
Specify the co-financing body								
TOTAL appropriations co-financed								

3.2.8. Estimated human resources and the use of appropriations required in a decentralised agency

The amount of appropriations to be allocated to the agencies in the next MFF is indicative and subject to the agreement on the MFF. It should be integrated into the Agencies' subsidy due to the permanent nature of the tasks allocated by this proposal and will be compensated, if

relevant, by an equivalent reduction of a relevant programme envelope under the same MFF heading. If a compensatory reduction is needed, the resources allocated to the Agencies may also need to be revised through the annual budgetary procedure.

Staff requirements (full-time equivalent units):

Agency: Europol	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**
Temporary agents (AD Grades)	109	216	322	429	535	637	749
Temporary agents (AST grades)	0	0	0	0	0	0	0
Temporary agents (AD+AST) subtotal	***109***	***216***	***322***	***429***	***535***	***637***	***749***
Contract agents	0	10	19	36	51	64	77
Seconded national experts	12	22	34	45	53	64	74
Contract agents and seconded national experts subtotal	***12***	***32***	***53***	***81***	***104***	***128***	***151***
TOTAL staff	**121**	**248**	**375**	**510**	**639**	**765**	**900**

Appropriations covered by the EU budget contribution in EUR million (to three decimal places)[97]:

Agency: Europol	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL 2028 - 2034**
Title 1: Staff expenditure	12 491	37 722	63 154	89 056	115 069	140 307	166 197	**623 996**
Title 2: Infrastructure and operating expenditure								
Title 3: Operational expenditure	45 021	54 624	57 677	61 329	63 761	66 857	68 187	417 456
TOTAL of appropriations covered by the EU budget	**57 512**	**92 346**	**120 831**	**150 385**	**178 830**	**207 164**	**234 384**	**1 041 452**

97 Please refer to footnote **Error! Bookmark not defined.**.

Overview/summary of human resources and appropriations (in EUR million) required by the proposal/initiative in a decentralised agency[98]:

Agency: Europol	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL 2028 - 2034**
Temporary agents (AD+AST)	109	216	322	429	535	637	749	749
Contract agents	0	10	19	36	51	64	77	77
Seconded national experts	12	22	34	45	53	64	74	74
Total staff	**121**	**248**	**375**	**510**	**639**	**765**	**900**	**900**
Appropriations covered by the EU budget	57 512	92 346	120 831	150 385	178 830	207 164	234 384	1 041 452
Appropriations covered by fees (if applicable)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Appropriations co-financed (if applicable)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
TOTAL appropriations	**57 512**	**92 346**	**120 831**	**150 385**	**178 830**	**207 164**	**234 384**	**1 041 452**

Staff requirements (full-time equivalent units):

Agency: eu-LISA	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**
Temporary agents (AD Grades)	7	7	7	7	7	7	7
Temporary agents (AST grades)	0	0	0	0	0	0	0
Temporary agents (AD+AST) subtotal	**7**	**7**	**7**	**7**	**7**	**7**	**7**
Contract agents	0	3	3	3	3	3	3
Seconded national experts	0	0	0	0	0	0	0
Contract agents and seconded national experts subtotal	0	3	3	3	3	3	3
TOTAL staff	**7**	**10**	**10**	**10**	**10**	**10**	**10**

Appropriations covered by the EU budget contribution in EUR million (to three decimal places)[99]:

[98] Please refer to footnote **Error! Bookmark not defined.**.

Agency: eu-LISA	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL 2028 - 2034**
Title 1: Staff expenditure	0.756	1.687	1.863	1.863	1.863	1.863	1.863	**11.758**
Title 2: Infrastructure and operating expenditure								
Title 3: Operational expenditure	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.
TOTAL of appropriations covered by the EU budget	**0.756**	**1.687**	**1.863**	**1.863**	**1.863**	**1.863**	**1.863**	**11.758**

Any additional budget needs for eu-LISA linked to the implementation of the tasks delegated to the agency in this Regulation will be offset against the appropriations allocated to Europol within this LFDS.

[99] Please refer to footnote **Error! Bookmark not defined.**.

Overview/summary of human resources and appropriations (in EUR million) required by the proposal/initiative in a decentralised agency[100]:

Agency: eu-LISA	Year **2028**	Year **2029**	Year **2030**	Year **2031**	Year **2032**	Year **2033**	Year **2034**	**TOTAL 2028 - 2034**
Temporary agents (AD+AST)	7	7	7	7	7	7	7	**7**
Contract agents	0	3	3	3	3	3	3	**3**
Seconded national experts	0	0	0	0	0	0	0	**0**
Total staff	**7**	**10**	**10**	**10**	**10**	**10**	**10**	**10**
Appropriations covered by the EU budget	0.756	1.687	1.863	1.863	1.863	1.863	1.863	**11.758**
Appropriations covered by fees (if applicable)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
Appropriations co-financed (if applicable)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**0.000**
TOTAL appropriations	**0.756**	**1.687**	**1.863**	**1.863**	**1.863**	**1.863**	**1.863**	**11.758**

Any additional budget needs for eu-LISA linked to the implementation of the tasks delegated to the agency in this Regulation will be offset against the appropriations allocated to Europol within this LFDS.

[100] Please refer to footnote **Error! Bookmark not defined.**.

DIGITAL DIMENSIONS

4.1. Requirements of digital relevance

Reference to the requirement	Requirement description	Actors affected or concerned by the requirement	High-level Processes	Categories
Article 8(7)	Member States respond to Europol request for information and criminal intelligence to contribute to coordination measures.	Europol MS CA	Information exchange Access to MS information	Process digitalisation and automation Data Digital public service
Article 9(2)	Member States ensure Europol access to information accessible by Asset Recovery Offices (ARO) and maintains level of direct accessibility.	Europol MS AROs	Information exchange Access to MS information	Digital public services Data
Article 9(3)	Member States to inform Europol on decision not to freeze upon Europol request MS LEA to take immediate action in case of risk of disappearance of property.	Europol MS LEA	Information exchange Request for freezing	Digital public services Data
Articles 9(4) and 9(5)	Member State Financial Investigation Units (FIU) to reply to Europol requests (mirrors Directive 2019/1153 Article 12).	Europol MS FIU MS ENU	Eropol-FIU information exchange Analysis	Digital public services Data
Articles 7(1) and 7(2)	Europol analytical products of operational and strategical nature on the	Europol, Commission, MS	Analysis	Process digitalisation and automation

	basis of information provided by Member States, relevant Union bodies and from OSINT.	LEA, Council	Report	Data
Article 7(2)	Europol support to common methodologies and standards on analytical products.	Europol And beneficiaries: MS LEA, Council, Commission, Eurojust/EUBOAs	Standardisation Analysis	Data
Articles 7(3) and 7(4)	MS, EUBOA provide information to Europol for strategic and operational analytical products.	Europol MS (in general) EUBOAs	Analysis Information exchange share to Europol	Digital public services Data
Article 11	Data flows in the context of requests by Europol for the initiation of a criminal investigation.	Europol Member States (national units) Eurojust EPPO	Operational cooperation	Data
Articles 12 and 13	Europol coordination for handling incoming and outgoing provision and request for information.	Europol MS CA, TC, IO, EUBOAs	Information Exchange Analysis	Process digitalisation and automation Digital public service
Article 18(a)	Europol cooperation with competent authorities in the context of removal order of terrorist online content.	Europol MS CA Private parties	Information Exchange with CA and PP TCO removal orders	Digital public services Data

Article 18(a)	Europol referrals to online service providers.	Europol MS CA Private parties	Information exchange with PP TCO referrals	Digital public services Data
Article 18(c)	Europol support to crisis response.	Europol MS CA Private parties	Information exchange Crisis response	Digital public service Data
Article 16(a)	Europol supports ARO in the tracing and identification of instrumentalities, proceeds, and properties, which are, or might become, the object of a freezing or confiscation order, in accordance with Article 6.	Europol MS AROs	Information exchange Freezing procedure	Digital public service Data
Article 16(c)	Europol operational and analytical support to the EPPO.	Europol EPPO	Information exchange Analysis	Digital public service Data
Article 21(4)	Europol may process information while part of JIT	Europol MS CA	collect analysis of information	Data
Article 22(5)(a)	ENU receive messages exchanged between Europol their competent authorities.	MS ENU MS CA Europol	Europol-MS information exchange	Process digitalisation and automation Data Digital public service
Article 22(5)(b)	ENU have access to national law enforcement data and relevant data necessary for cooperation with Europol.	MS ENU Europol	access to MS data	Data Process digitalisation and automation

				Digital public service
Articles 22(8), 25(6) and 26	Technical and operational uptake of Europol systems and tools nationally by ENU and by Europol Support offices (ESO). Europol staffs ESO, covers cost of ENU connection, and provides ENU technical and financial support.	Europol MS ENU MS LEA	Uptake	Process digitalisation and automation
Article 28	Information sources available to Europol.	Europol, the EPPO, MS law enforcement authorities (LEA) Private parties Third countries and international organisations	Collect information	Data
Article 29	Member States' mandatory provision of information to Europol via the SIENA channel, including immigration liaison officers.	MS CA Europol Immigration liaison officers	share to Europol	Data Digital public service
Article 29(3)	Use of SIENA channel by Member States.	MS CA Europol	share to Europol Europol access to MS data	Process digitalisation and automation
Article 29(6)	Europol report on information provided	Europol	Report	Data

	by Member States.	Council European Parliament		
Article 30	Europol to support Member States in application of SIS Regulations[57]. Member shall inform Europol of insertion and hits on information alerts.	Europol Member States LEA	SIS information exchange	Digital public Service Data
Articles 32 and 33	Limitation to Europol processing by nature (i.e. category of data subject as victim vs. suspect) by purpose (analysis, cross-checking, research & innovation).	Europol All beneficiaries of analytical products	Cross-check Analysis Innovation	Process digitalisation and automation
Articles 32 and 33	Limitations to Europol processing of information, by restrictions set by the data owner (data ownership principle) at the moment of sharing.	Europol, Europol MB MS LEA EDPS	Collection Analysis Cross-check Analysis information exchange innovation	Process digitalisation and automation
Article 34	Europol notification to Member States law enforcement authorities when relevant operational information is found, across all processes.	Europol MS LEA	Information exchange Europol notification to LEA	Digital public service Data
Article 35 to Article 39	Creation of a **cross-checking service**: nature, format, and quality of data (IA); automated cross-check upon insertion.	Commission Europol Member States	Development Information exchange	Data Process digitalisation and automation

	Available to Europol, Member States LEA and EU information systems.	LEA EU Information Systems	Cross-check ETIAS and VIS security checks	Digital solution Digital public service
Article 35 to 39	Member States to connect their case management systems to the cross-checking service (IA), to upload data (IA) to query the data (IA)	Commission Europol MS CA	Development Collection share to Europol Cross checking	Data Process digitalisation and automation
Article 35 to Article 40	Creation of **Europol analytical environment**, to support Europol's analytical activities for the storage, processing, cross-checking, visualisation and analysis of data, including in support of criminal investigations and operational coordination. specialised analytical, technical, digital, forensic or multidisciplinary capabilities, including through investigative, analytical, technical and strategic services	Europol Indirectly, MS CA, EUBOAs, International organisations, Third countries	Collection, Analysis, Cross-check, exchange, report.	Data Digital solution Process digitalisation & automation
Article 41	Conditions for searching Europol analytical environment.	Europol MS CA, EU Information systems	Cross-check	Data Digital public service Digital solution
Articles 42, 43, 44 and 45	Creation of a **Police Shared Data Space,** using the Europol cloud infrastructure, and hosting analytical and communication tools for Member	Commission Europol MS CA, TC	Development Information exchange **Joint** analysis	Data Process digitalisation & automation

	States investigators (IA); creation of joint operational analysis cases.			Digital solution Digital public service
Article 46	Creation of Europol Secure Information Exchange Network Application (**SIENA**) for facilitating the exchanges of information. Responsibilities, Architecture, Obligations to use by Member States and Europol, and functionalities (IA).	Commission Europol MS, TC, IO, PP	Development Information exchange	Data Digital solution Process digitalisation & automation Digital public Service
Article 47	Creation of a p**latform for cooperation with private parties**.	Private Parties Europol Member States	Development	Digital solution Digital public Service
Article 47(2)(a)	Private parties to report and to notify to Europol under TCO Regulation[55] and Digital Services Act[56] via the Platform.	Europol	TCO removal orders, referrals DSA	Process digitalisation & automation
Article 47(2)(b)	Europol to provide private parties with the information necessary to identify relevant online content, services, accounts, infrastructures or digital activities via the Platform.	Europol Private Parties	Online crisis situation	Process digitalisation & automation
Article 48	Europol support the operation of the European Police Record Index System in application of the Prüm II regulation[58].	Europol	System development and Operation	Digital solution Digital public service

Article 49	Additional services and tools can be developed (IA) under the Police Shared Data Space	Commission Europol Committee Europol MS CA, TC, EUBOA, II, PP	Development Collection, Information exchange, Analysis, Cross-checking, report, joint analysis	Data Digital solution Process digitalisation & automation Digital public Service
Article 50	**Europol Cloud infrastructure:** creation, use as the standard infrastructure for Europol systems, services and tools offered to Member States, including existing ones, secure access (IA).	Commission Europol	Development Procurement	Digital solution Digital public service
Article 51	**EU Police Digital Identity**: creation of a harmonized scheme for identifying and granting police staff direct or indirect (via national systems) access Europol cloud infrastructure (IA).	Commission MS, Third countries Europol	Standardization of Police ID data Development Identification and access management	Data Digital solution Digital public service
Article 52	**Statistics and reporting tools:** creation, use of tools for the purpose of evaluation, monitoring, analysis and reporting (IA).	Europol Member States LEA, Commission	Development Reports	Data Digital solution Digital public service
Article 53	Europol support to the development and uptake of **Universal Message format.**	Europol eu-LISA Member States LEA	Standardization Information exchange	Data Process digitalisation and automation

		Commission		Digital public service
Articles 55 and 56	Creation of, the ICT and **Information Management Steering Group and Advisory Group**, supporting the Management Board decisions on ICT architecture, data management, interoperability, alignment with MS business needs.	Europol Member States LEA Commission	Development Standardization Uptake	Data Process digitalisation and automation Digital public service
Article 54	Creation of an EU **DNA matching application**, for the benefit of Europol and Member States.	Europol Member States LEA Commission	Development Standardization Procurement Uptake Cross-checking Analysis	Data Digital Solution Digital public service
Articles 57 to 64	Europol, through the Innovation Advisory Group and supported by the Capabilities and Innovation Advisory Group, develops and regularly reviews and updates a **Foresight and Capability Development Framework** to ensure the coordination and complementarity between Europol, relevant Union bodies and Member States in relation to research, innovation, testing, development, piloting, and uptake of advanced capabilities for law enforcement,	Europol Member States EUBOAs Commission	Development Standardisation Procurement Uptake Innovation	Process digitalisation and automation

	including through pooling of existing capabilities, coordinated participation in standardisation processes and joint procurements.			
Article 61	Use of regulatory sandbox for developing AI based advanced capabilities.	Europol	Development Innovation	Data
Articles 80 and 81	Union bodies and national VIS designated authorities have an indirect access to Europol. (IA). EPPO receives automatically information relevant to it.	EUBOA VIS designated authorities Commission	Cross check by EUBOAs VIS security check	Process digitalisation and automation Digital public services Data
Article 94	Transfer of personal data to third countries and international organisations.	Europol Third countries International organisations Member States	Data transfer	Data
Article 96(1) to 96(3)	Europol processes data from **private parties**.	Europol Private parties	Exchange with private parties Collect	Digital public services Data
Article 96(3)	Result of processing private party-sourced information forwarded to the ENU.	Europol Private parties MS ENU	Exchange with private parties Process, Analyse, Report	Process digitalisation and automation

Articles 96(4) to 96(6).	Europol allowed to transfer data to private parties in specific cases.	Europol PP, Data Subject Data owner	Exchange with private parties	Process digitalisation and automation Data
Article 86(8)	Europol sends request for information to private parties via ENU.	Europol MS ENU Private parties	Exchange with private parties	Digital public services Process digitalisation and automation Data
Article 97	Europol to forward information from natural persons to relevant Member State or third country.	Europol	Exchange with private parties	Digital public services Process digitalisation and automation Data
Article 98	Europol has access to exchanges between Member States and private parties.	Europol Private parties	Exchange with private parties	Process digitalisation and automation Digital public service
Articles 99, 100, 101, 102 and 107	Limitations and responsibilities to the processing of personal data including for research and innovation, limitations for the storage and erasure of personal data; on the basis on verifications to be carried out on the reliability of the source, on the accuracy of information, on the category of data subjects, on special categories of personal data.	Europol	All processing of operational data	Data Process digitalisation and automation

Article 103	Notification of a personal data breach to the authorities concerned.	Europol MS LEA	Personal Data breach	Digital public services Data
Article 104	Communication of a personal data breach to the data subject.	Europol Data Subject	Personal Data breach	Digital public services Data
Articles 105 and 106	Right of access, to rectification, erasure and restriction for the data subject.	Europol Data Subject	Right of data subject	Digital public services Data
Article 102	Europol to keep logs of all processing information.	Europol	All processing of operational information	Data Process digitisation and automation
Article 116(3)	Europol to inform regularly Joint Parliamentary Scrutiny Group (JSPG).	Europol JSPG	Report	Digital public services Data
Article 117	European Parliament to access to Sensitive non confidential (SNC) operational data.	Europol European Parliament	Access to information	Digital public services Data
Article 130	Commission shall submit every five years an evaluation report to the European Parliament, the Council, the national parliaments and the Management board.	Commission	Report	Data

Article 136	Europol queries national database via the Prüm II router mechanism.	Europol MS LEA	Information exchange Access to MS information	Data Process digitalisation and automation
Article 137	Start of operations provisions.	Commission Europol Member States	Start of operations	Digital public service

4.2. Data

Constraints on data depend on the operational process

The type of data processed and exchanged highly depend on the process and on the actors involved (see table A). Whilst the different applicable data format indeed depend on the type of data processes (table C), the applicability and its enforcement depend on the process, as the data is not exchanged in the same operational situation, and under the same legal constraints, notably on data quality.

– **Police officer identification** will be the process where constraints on data will be the highest to ensure the highest level of security assurance when accessing to applications, services and data provided under Europol Cloud infrastructure, including notably the Police Shared data space.

– **Information exchange, analysis**, and similarly **innovation.** Europol operates in an information environment characterised by high volumes of heterogeneous data, which often originate from multiple sources, jurisdictions, and operational contexts. A substantial portion of this information is received in an unstructured or mixed form. This reflects the reality of modern law enforcement, in which datasets are complex, dynamic, and not fully standardised, and where the extraction of information relevant to ongoing investigations constitutes the core operational task. This is particularly true for electronic evidence such as seized informational material which comes unstructured and most often encrypted. This data is analysed and processed either by Europol within the *Europol analytical environment*, or jointly by Member States competent authorities, EU bodies, private parties under the *Police shared data space.* Information can be exchanged between parties via the *Police shared data space* or *SIENA.* The Application of standards depends mostly on the source of data and therefore MAY follow the standards and specifications underpinning the corresponding database. However, as information necessary for Europol to carry out its tasks are only defined by the purpose, the following list remains not exhaustive.

– **Cross-checking** A *cross-checking service* (Articles 35 to 39) is established for the rapid identification of links with previous individuals, objects, involved in a criminal activity and only relating to convicted, suspects of having committed or to about to commit a crime. Member

States can access *the Europol Analytical environment* (Article 41(4)) on a hit/no-hit basis. A *hit/no hit mechanism* (Article 80) allows to cross-check information against the Europol analytical environment for EUBOAs, and can relate to suspects, convicted but as well to victims or persons indirectly related.

– **Administrative Reports** while being published in digital form, do not follow strict *technical* standard requirements.

– **Personal data rights** related processes, are highly manual; while data processes and shared might be structured and can follow certain standards, it is not a requirement.

Constraints across processes

Process / Reference to the requirement	Police officer identification	Cross check	Information exchange between LEA	Exchange with private parties	Operational and Strategical Analysis	Innovation	Administrative report	Personal data rights
Article 8(7)			X					
Article 9(2)			X					
Article 9(3)			X					
Article 9(4)			X					
Article 9(5)			X					
Article 7(1)					X			

Process / Reference to the requirement	Police officer identification	Cross check	Information exchange between LEA	Exchange with private parties	Operational and Strategical Analysis	Innovation	Administrative report	Personal data rights
Article 7(2)					X			
Article 7(3)					X			
Article 7(4)			X		X			
Article 7(5)			X		X			
Article 11			X					
Article 18(a)			X	X				
Article 18(b)				X				
Article 18(c)			X	X				
Article 16(a)			X					
Article 16(c)			X		X			
Article 21(4)			X		X			
Article 25(5)(a)			X					

Process / Reference to the requirement	Police officer identification	Cross check	Information exchange between LEA	Exchange with private parties	Operational and Strategical Analysis	Innovation	Administrative report	Personal data rights
Article 25(5)(b)			X					
Article 28			X					
Article 29			X		X			
Article 29(6)							X	
Article 30			X					
Article 34			X					
Article 35		X			X			
Article 36		X			X			
Article 37		X			X			
Article 38		X			X			
Article 39		X			X			
Article 40					X			

Process / Reference to the requirement	Police officer identification	Cross check	Information exchange between LEA	Exchange with private parties	Operational and Strategical Analysis	Innovation	Administrative report	Personal data rights
Article 41		X			X			
Article 42			X		X			
Article 43			X		X			
Article 44			X		X			
Article 45			X		X			
Article 46			X					
Article 49		X	X	X	X		X	
Article 51	X							
Article 52							X	
Article 53		X	X		X			
Article 55	X	X	X	X	X		X	
Article 56	X	X	X	X	X		X	

Process / Reference to the requirement	Police officer identification	Cross check	Information exchange between LEA	Exchange with private parties	Operational and Strategical Analysis	Innovation	Administrative report	Personal data rights
Article 54		X	X		X			
Article 61						X		
Article 80		X						
Article 81		X						
Article 94			X					
Article 96(1)				X	X			
Article 96(2)				X	X			
Article 96(3)				X	X			
Article 96(4)				X				
Article 96(5)				X				
Article 96(6)				X				
Article 96(7)				X				

Process / Reference to the requirement	Police officer identification	Cross check	Information exchange between LEA	Exchange with private parties	Operational and Strategical Analysis	Innovation	Administrative report	Personal data rights
Article 97			X					
Article 98						X		
Article 99						X		
Article 100						X		
Article 101						X		
Article 102						X		
Article 102								X
Article 104								X
Article 105								X
Article 106								X
Article 107						X		
Article 102	X	X	X	X	X	X	X	X

Process / Reference to the requirement	Police officer identification	Cross check	Information exchange between LEA	Exchange with private parties	Operational and Strategical Analysis	Innovation	Administrative report	Personal data rights
Article 116(3)							X	
Article 117								X
Article 130							X	
Article 136		X	X					

Type of data per process

Process / General data type and standards applicability	Police officer Identification	Cross-check	Information exchange between LEA and/or Europol	Exchange with private parties	Operational and Strategical Analysis	Innovation	Administrative report	Personal data rights

Do data format standards apply? (Mandatory/Optional)	M	M	O	O	O	O	N/A	N/A
Type of data								
EU digital police identity	X							
Police and justice records		X	X		X	X		X
Information held by other administrations			X		X	X		X
Information held by private authorities			X	X	X	X		X
OSINT			X	X	X	X		X
Digital evidence			X	X	X	X		X
Operational report			X		X	X		X
Strategical report			X		X	X		X
Administrative Report						X	X	X

Type of data and applicable data standards

Data type	**Applicable data standard**
EU digital police identity	To be determined by
Police and justice records	
Prüm II, EPRIS, ECRIS, ECRIS-TCN, SIS record	When exchanged under EU framework, the corresponding standards

	apply as EPRIS, Prüm II, ECRIS, ECRIS-TCN or SIS. UMF applies to them. UMF sets out a taxonomy of data stored in police records and help national authorities map their data to other Member States and Europol law enforcement authorities.
National police and justice databases	When not exchanged under EU framework, national databases format usually prevails, as UMF implementation in national Case management systems was not made mandatory. In substance data type covered are found in UMF: Person (identity), physical description, DNA profile, Face recognition data, dactyloscopic data, palm print, offence, travel/identification/official document, photograph, weapon, firearm, organization, criminal case, flight/journey; means of payment, means of transportation; account, and associated, action to be taken in case found, conviction, sentence.
Information held by other administrations	
Civil register	Regulation (EU) 2016/1191 – Multilingual Standard Forms (MSF) European Civil Registry Network (ECRN) – secure cross-border data exchange RISER – uniform electronic service for registry access Alignment with UN CRVS standards – structured fields, metadata, unique identifiers
Travel document / Identity card	ICAO 9303 Travel information PNR Directive

	API Regulations
Immigration records held by administration	EU central databases: VIS, EURODAC, EES, ETIAS: standards are set by the corresponding legislation and should adhere to UMF. Data held are of related to the persons identity, travel document. National database information may be exchanged as well.
National real-estate registers or electronic data retrieval systems and land and cadastral registers	
National citizenship and population registers of natural persons	
National motor vehicle, aircraft and watercraft register	SIS II, Prüm II
Commercial registers, including business and company registers	
Fiscal data, including data held by tax and revenue authorities	
National social security data	
Information held by private authorities	
Bank account information	As under Directive (EU) 2024/1640,
Transaction records	
Information on mortgages and loans	

information contained in national currency databases and currency exchange databases	
Information on securities	
Customs data, including cross-border physical transfers of cash	
Information on annual financial statements by companies	
Information on wire-transfers and account balances	
Information on crypto-asset accounts and crypto-asset transfers	As defined in Article 3 of Regulation (EU) 2023/1113 of the European Parliament and of the Council (44).
OSINT	
	Applicable multi-media format dependent
Digital evidence	
Legal interception	ETSI TS 103 705, ETSI TS 104 007
Communication metadata	Applicable ETSI standards
Video footage	Applicable multi-media format dependent
Operational report	
Strategical report	
Administrative Report	

Alignment with the European Data Strategy

Explanation of how the requirement(s) are aligned with the European Data Strategy

The proposed revision of Europol's mandate fully aligns with Regulation (EU) 2018/1725 (EUDPR), integrating its core principles into Europol's operational framework while addressing the specific needs of law enforcement cooperation. The text explicitly subjects Europol's processing of personal data to the EUDPR's requirements in Article 98(1), embedding key obligations such as lawfulness, purpose limitation, and data minimisation into its legal framework. Article 32(2) restricts data processing to predefined purposes—such as cross-checking, operational analysis, and research—directly reflecting EUDPR requirement that personal data be collected for specified, explicit, and legitimate purposes. Similarly, the storage limitation principle is reinforced through Article 101, which requires Europol to review the necessity of data retention every three years and sets a five-year maximum storage period, aligning with Article 4 EUDPR. The proposal also incorporates the EUDPR's accountability mechanisms, such as the requirement for Data Protection Impact Assessments (DPIAs) for high-risk processing (Article 102(3)) and the obligation to consult the European Data Protection Supervisor (EDPS) prior to engaging in new types of processing (Article 108), mirroring Article 90 of the EUDPR. Additionally, the text ensures compliance with the EUDPR's provisions on data subject rights, including access, rectification, and erasure (Articles 105–106), fulfilling the EUDPR's documentation and transparency obligations (Article 98). By systematically integrating these substantive requirements, the proposal ensures that Europol's expanded operational capabilities remain fully compliant with the EUDPR's robust data protection standards.

Data Act[59] does not apply to this proposal, as no obligation is set out in the proposal requiring business to make data available to other business.

Europol will promote the development of **common data standards** across EU Member States, on strategical analytical products (Article 7) the criminal information exchange, notably on DNA, and forensics and data analysis techniques, whilst the policy does not concern public sector information *per se* which can be reused as put forward Open Data Directive[60], notably for public security reasons.

The **Police Shared Data Space** put forward in the proposal will be the common space for investigators to bring in common investigative information for operational analysis, and will constitute an important enabler for feeding Europol's research and innovation activities (Art 60) for the training, development, testing and validation of advanced analytical and forensic capabilities within regulatory sandboxes according to AI Act. Both Police Shared Data Space and R&I activities will benefit from the Europol Cloud infrastructure scalable storage and processing capacities. Those three components contribute to the emergence of a common law enforcement data space.

Provision of **data governance Act[61]** to transfer to third countries does not apply as concerning law enforcement activity.

Alignment with the once-only principle

Explanation of how the once-only principle has been considered and how the possibility to reuse existing data has been explored

Request for information by Europol to private parties are effectively carried out by Member States under Article 96(7). Member States law enforcement authorities Implementation of the once-only principle is therefore governed by national law and are therefore out of scope of this proposal. Information gathered by Europol and law enforcement authorities under such conditions are managed centrally under the *Platform for cooperation with private parties* (Article 47) to facilitate communication between Europol, the Member States and the private parties, and to ensure Europol does not request the same information twice. Requests for information **directly initiated by Member States** under Article 96(8) handled via the Platform and corresponding exchanges with private parties are made available to Europol in the same spirit of limiting the requests to businesses.

Request for information by Europol to Member States competent authorities, EUBOA, third countries, International Organisation will neither be asked twice, such requests are managed centrally within the Agency by Europol Operational and Analysis Service in application of Article 12. Conversely their request for information or for support, be it of analytical, technical, financial or operational nature will be followed up by the same Service insuring a proper and swift handling. Similarly, Member States ENU being as well informed of all exchange of information between Europol and its competent authorities, will ensure that no duplicate requests are made (Article 25(5))

Explanation of how newly created data is findable, accessible, interoperable and reusable, and meets high-quality standards

The proposed revision of Europol's regulatory framework ensures that newly created data **adheres to the FAIR principles within the closed community of Member States law enforcement authorities**, and, to a certain extent to third countries', EU bodies in the JHA domain, and International Organizations participating to the fight against serious organized crime and terrorism. In that regard, the proposed framework maintains high-quality standards through structured governance and advanced technical infrastructure.

Findability is achieved by establishing centralised platforms such as the *Europol Analytical Environment* (Article 40) and the *Police Shared Data Space* (Article 42), which provide secure, indexed repositories for criminal intelligence, operational analyses, and joint investigations. These systems incorporate metadata standards, unique identifiers, and search functionalities (including alphanumeric, biometric, and multimedia queries (Article 41))to enable precise retrieval of data. **Accessibility** is guaranteed through role-based access controls, *the EU Police Digital Identity* (Article 51), and interoperable tools like *SIENA* (Secure Information Exchange Network Application, Article 46), which facilitate seamless, secure data sharing among Member States, Union bodies, and authorised partners. The *Europol Cloud Infrastructure* (Article 50) further ensures scalable, on-demand access to data while complying with strict security and sovereignty requirements, including compartmentalisation and encryption. **Interoperability** is embedded in the proposal through mandatory technical standards, such as the *Universal Message Format* (UMF) (Article 53), which harmonises data exchange across Union information systems, and the integration of Europol's tools with existing EU platforms like the *Schengen Information System* (SIS) and *EPRIS* (European Police Record Index System, Article 48). *The cross-checking service* (Article 36) and *DNA matching application* (Article 54) automate comparisons across datasets, reducing silos and enabling real-time linkages between cases. **Reusability** is supported by the *Foresight and Capability Development Framework* (Article 57), which promotes standardised methodologies, common analytical tools, and modular system designs

(e.g., reusable software components in the cloud infrastructure). High-quality standards are enforced through data validation protocols (e.g., "data loaders" for automated uploads, Article 38), periodic reviews of data accuracy (Article 101), and statistics and reporting tools (Article 48) that monitor performance, consistency, and compliance with Union law. Additionally, the *ICT and Information Management Steering Group* (Article 50) oversees technical coherence, while training programmes (Article 64) ensure that personnel are equipped to maintain data integrity. Together, these measures create a robust ecosystem where data is not only operationally effective but also aligned with legal, and technical best practices.

Data flows

High-level description of the data flows

Type of data	Reference(s) to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)
Request for information to contribute for coordination measure	Art 8(7)	Europol	MS	Europol initiative	/
Information and criminal intelligence	Art 8(7)	MS LEA	Europol	Request from Europol	/
Request for information	Art 9(2)	Europol	MS ARO	Europol initiative	/
Information and criminal intelligence	Art 9(2)	MS ARO	Europol	Request from Europol	/
Request to act (freezing)	Art 9(3)	Europol	MS LEA	Europol initiative, risk of disappearing	/
Decision on freezing	Art 9(3)	MS LEA	Europol	Request from Europol	/
Request for information	Art 9(4)	Europol	MS FIU	Europol initiative	/
Information and criminal intelligence	Art 9(5)	MS FIU	Europol	Request from Europol	/
Analytical products	Article 7	Europol	MS	Europol initiative	/

			Council Commission		
Information and criminal intelligence	Art 7(4) & (5)	MS EUBOAs	Europol	Europol request for operational or strategic analytical product	/
Requests for the initiation of a criminal information	Article 11	Europol	MS	where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives	/
Removal order of online content	Art 18	MS LEA	Europol	MS decision to request removal	/
Removal order of online content	Art 18(a)	Europol	PP	Europol & MS LEA coordination	/
Referrals of online content	Art 18(b)	Europol	PP	Europol or MS LEA request	/
Information and criminal intelligence (online content, services, accounts, infrastructures or digital activities)	Art 18(e)	Europol	PP	Europol request	/
Information and criminal	Article 16(a)	Europol/ARO	ARO/Europol	Europol /ARO	/

intelligence				initiative	
Information and criminal intelligence	Article 16(c)	Europol/EPPO	EPPO/Europol	Europol / EPPO initiative	/
Information and criminal intelligence	Article 21(4)	Europol/JIT	JIT/Europol	Europol / JIT initiative	/
Information and criminal intelligence	Article 25(5)(a)	Europol	MS ENU	When exchanging with MS LEA	/
Request for information	Article 25(5)(a)	Europol	MS ENU	Europol initiative	/
Request for information	Article 25(5)(c)	MS ENU	MS authorities	Europol request	/
Information and criminal intelligence	Article 25(5)(b)	MS authorities holding information	MS ENU	Europol request	/
Information and criminal intelligence	Article 25(5)	MS ENU	Europol	Europol request	/
Publicly available Information	Article 28	Publicly available source	Europol	Europol initiative	/
Information and criminal intelligence	Article 29, 32, 33	MS CA Immigration LO	Europol	MS observation that information is necessary to fulfil Europol's objectives	/
Report	Article 29	Europol	Council	Regulation	Annually

			European Parliament	application	
Information and criminal intelligence	Article 34	Europol	MS LEA	When relevant operational information is found	/
Information and criminal intelligence	Article 38	MS LEA	Cross-checking service	without undue delay when data is found to fulfil conditions set under Article 35 to 38	Systematically
Information and criminal intelligence	Article 49	MS LEA	Cross-checking service	When conducting investigations / when a case has a cross-border dimension	systematically
Information and criminal intelligence	Article 49	Cross-checking service	MS LEA	Upon MS request above	/
Information and criminal intelligence	Article 41	Europol MS ENU	Europol Analytical environment	MS LEA/ENU initiative	/
Hit/no hit	Article 41	Europol Analytical environment	MS ENU	Upon request above	/

Any information	Article 46	Europol, MS, TC, EUBOA, II	Europol, MS, TC, EUBOA, II	/	/
Statistics and reports	Article 52	Tool	MS, Europol, other entities	Upon request	/
Information and criminal intelligence	Article 94	Europol	Third countries	Third party or Europol initiative	/
Information and criminal intelligence	Article 96(3)	PP	Europol	PP initiative	/
Information and criminal intelligence	Article 96(3)	Europol	MS CA	Europol initiative	/
Information and criminal intelligence	Article 96(4), Article 96(5)	Europol	PP	Europol initiative	/
Request for information	Article 96(7)	Europol	ENU	Europol initiative	/
Report	Article 96(11) Article 96(12)	Europol	MB, EP, Council	Regulation implementation	Yearly
Information and criminal intelligence	Article 97(1)	Natural person	Europol	PP initiative	/
Information and criminal intelligence	Article 97(3)	Europol	MS, TC	Upon reception of information above	/
Notification of a personal data breach	Article 103	Europol	MS LEA	In the event of a personal data	/

				breach	
Notification of a personal data breach	Article 104	Europol	Data subject	In the event of a personal data breach	/
Personal data	Article 105	Europol	Data subject	Upon Data subject request	/
Information to the JSPG	Article 116(3)	Europol	JSPG	Varies along the specific part of JSPG information	Varies.
Request for information	Article 117(1)	European Parliament	Europol	EP initiative	/
Information and criminal intelligence	Article 109(2)	Europol	European Parliament	Upon request above	/
Report	Article 130	Europol	MB, EP, Council, National Parliaments	Regulation implementation, Entry into application of the regulation	5 years
Request for information on person details	Article 136	Europol	MS databases via Prüm router	Europol initiative	/
Person's identity	Article 136	MS databases via Prüm router	Europol	Upon request above	/

Commission implementing acts determining the start of operations	Article 137	Commission	MS	Committee procedure	/
SIS supplementary information	Article 30	MS SIRENE	Europol	Upon hit on SIS alert	/
Information and criminal intelligence	Article 30	Europol	MS SIRENE	In response to above notification	/
Third country sourced information	Article 30	Europol	MS	Europol initiative	/
Notification of insertion	Article 30	MS	Europol	Upon insertion of SIS alert	/
Supplementary information	Article 30	Europol	MS	Upon request, when receiving hits on specific alerts	/

4.3. Digital solutions

Digital solution	Reference(s) to the requirement(s)	Main mandated functionalities	Responsible body	How is accessibility catered for?	How is reusability considered?	Use of AI technologies (if applicable)
Europol Cross checking service	Article 35 to Article 39	Storage, search and automated cross-checking of information via alphanumeric and biometric data. To be composed of: an	Europol	N/A machine interface	Synergies with eu-LISA Article 78(2) possibly with Prüm II components	Biometric matching modules

		infrastructure for the storage of information; a search interface; an interface for the upload, update, or deletion of information; a secure communication infrastructure between the cross-checking service and Member States/Union bodies/European Search Portal.			Article 36(4): cross-checking service shall make use of existing technological components, building blocks and infrastructure developed and managed by eu-LISA	
Europol Analytical Environment	Articles 40 and 41	Europol environment for storage, processing, cross-checking, visualisation and analysis of data, including in support of criminal investigations and operational coordination. It shall comprise analytical workspaces, case management functionalities, collaborative tools, data processing services, and other capabilities. It shall provide for logically separated analysis projects for storing and processing	Europol	Europol user interfaces' specifications	Cf Police Shared data space	Cf Police shared data space

		data for distinct analytical purposes. hit/no hit Search: shall enable the querying of the data stored to find connections with existing cases.				
Police Shared Data Space	Article 42 to Article 45	Member States environment to initiate joint operational analysis cases: upload, store, cross-check, process and analyse investigative data, jointly visualise, edit documents and reports, securely communicate and exchange information. To be based on the Cloud infrastructure.	Europol	For user interface, Implementing Act referred to Article 42(4), and Europol specifications	Requirement to share and re-use the hardware and software components of the Europol Analytical Environment and to make available its tools, functionalities and modules.	Tools, functionalities, and modules hosted (defined by implementing acts) are likely to integrate AI technology.
SIENA	Article 46	Secure information exchange between Member States, Europol, other Union bodies, third countries and international organisations. To be composed of: a	Europol	Set by Europol Specifications for user interface	Specific development.	Inline modules to aid the insertion, the interpretation of exchanged information

		central infrastructure for the storage and processing of data; web interface(s) and mobile application(s) enabling law enforcement staff to exchange information; dedicated programming interface(s) supporting interoperability with the IT systems of Member States and EU bodies; a secure communication infrastructure between SIENA and Member States/ Union bodies/ third countries/ international organisations.				
Platform for cooperation with private parties (included in the Europol Analytical Environment)	Article 47	Implement the TCO removal order DSA referral, and online crisis situation. Facilitate communication between Europol, Member States, and private parties offering service in the EU. Act as a crisis response platform in online crisis situations, facilitating communication and	Europol	Set by Europol Specifications for user interface	The platform already accommodates three different workflows	/

		enabling Europol to provide private parties with necessary information.				
European Police Record Index System (EPRIS)	Article 48	No new functionalities introduced. Article merely establishes that Europol shall perform the tasks conferred to it by Regulation (EU) 2024/982, as concerns EPRIS.	Europol	//	//	//
Other services and tools	Article 49	The Commission may adopt implementing acts laying down the procedures for defining the necessary functionalities of additional services and tools.	European Commission	//	//	//
Europol cloud infrastructure	Article 50	Provides scalable, secure and elastic storage and processing capacities enabling creation of the Police Shared Data Space. It therefore supports Europol and Member States' competent authorities to access Europol's tools,	Europol	N/A machine interface	Joint Procurement of cloud computing services	AI based analytics will rely on the expected scalability

		collaborative environments, and other operational data-processing capabilities. May also be used by other Union bodies and third countries for the same purpose. Shall support the storage, processing, analysis and exchange of data. Shall ensure strict access control, data compartmentalisation. Access rights detailed.				
EU Police Digital Identity	Article 51	Provides the necessary authentication and strong identification scheme for accessing the Police Shared Data Space	Member States Europol	Implementing act under Article 51	Implementing act should be developed with the view to reuse the technical components Framework set up by Regulation (EU) 910/2014 and its implementing	No

					acts. It should allow for the use on EU Digital Identity Wallets when possible	
Statistics and reporting tools	Article 52	Provide statistics and reports for the purposes of evaluation, monitoring, analysing and reporting. Shall collect, generate, and provide aggregated statistical information, indicators, technical logs, usage metrics, and analytical reports.	Europol	Implementing act under Article 52(6)	Article 86(2)(a) re-use similar components from EU large scale it systems such as CRRS	Limited to the formatting of the report
EU DNA matching application	Article 54	Enable the secure and reliable comparison of DNA profiles in support of Member States' investigations of criminal offences	Europol	N/A Machine interface	The matching application shall be used by Member States	No

Europol Cross-checking service & al.

Digital and/or sectorial policy (when these are applicable)	**Explanation on how it aligns**

AI Act	Cross-matching algorithms may make use of AI systems or models within the meaning of the AI Act, notably in the area of biometrics or law enforcement (e.g. fingerprint, facial image, profiling). Implementing act under Article 37(4) will cater for an ensuring alignment with the AI Act and the Commission guidelines notably on the classification of high-risk AI systems. Further guidance by Europol to Member States users on the integration and implementation within national procedures could be useful, according to different governing rules whether falling under high risk or not. Europol Analytical environment & Police shared data space; while the proposal does not envisage those environments to be based on AI technology, they will be the dedicated secured environment, respectively for Europol, and for Member States to carry out advanced criminal analyses on the basis of evidential material and other information, by the use of tools, mostly based on AI hosted in either environment. Many of the tools pursuing crime analytics fall outside the scope of the high risk classification (for example processing of large and complex data sets, such as transcribing audio files, for extracting entities, such as names and phone numbers from text messages without going through the content of the message; Image classification and object detection but without biometrics) Only a sheer part of the remaining cases (such as the use of lie detectors or profiling tools) would fall under Annexes I and III to the AI Act. The AI systems in and out of scope of high-risk AI systems are explained in the COM guidelines on high-risk AI systems classification. Under this proposal, capability is given to Europol to train and develop its own AI enabled tools by making use of regulatory sandboxes (Article 61(2)), and mission is given to support the adoption of the corresponding hosted tools and capabilities by Member States (Article 59(3)) and to provide the associated training (Article 64(1)(b)). With such large ambitions, Europol will be reinforced according to support its obligations as a provider, respectively, as a deployer of AI systems, including high-risk (cf. SO3/Advanced capabilities with EUR117million and 40 FTEs over the next MFF) Training and support for Member States to comply with AI rules when using Europol-provided tools will be supported by the creation of Europol support offices (EUR112million, 157 FTEs). SIENA and Platform cooperation for private parties

	Such digital solution may only embed non-high-risk in-line AI enabled module such as natural language processing (translation, transcription, etc) Obligations of transparency will be taken care of in the context of the effort to upgrade existing system and tools (EUR130 million, 115 FTEs). Europol Cloud Infrastructure EU Police digital Identity Statistics and reporting tools EU DNA matching application None of those solutions are set to rely on AI technology
EU Cybersecurity framework	The new proposed mandate is aligned with NIS2 (inter alia for the private parties) and with the Cybersecurity Act, as a) the new requirements made on the bodies concerned Europol, explicitly require application of EU cybersecurity framework (i) for the procurement of cloud services in Article 50(4) and (ii) and the production of statistics in Article 52(5). b) it reinforces Europol's role in cybercrime investigations. While Europol itself is not an NIS2-covered entity, the proposal strengthens organisational cybersecurity measures (e.g., secure data handling, incident response). It enhances Europol's ability to support Member States in investigating cyber incidents, without imposing direct obligations on private entities. The EU DNA matching application is also in line with the Cyber resilience act (CRA) as the product but does not impose requirements that would affect how manufacturer implement the essential requirements of the CRA.
eIDAS	While eIDAS does not apply to civil servants and to staff of Agencies, a EU digital police Identity will be required to access Europol Cloud infrastructure underpinning the Police Shared Data Space. Use of such identity may as well extend to other digital solution

	(SIENA, …). Implementing acts will cater for the roll out of a digital identification means to all criminal investigators with an assurance level high. To that end, an alignment and a reuse of existing schemes and infrastructure set out by the eIDAS regulation will be sought after.
Single Digital Gateway and IMI	Single Digital Gateway does not apply to services offered by Europol to Member states competent authorities, EUBOAs, Private parties or natural persons. The Internal Market Information System does not apply as the initiative does not fall within the scope of the internal market.
Others	

4.4. Interoperability assessment

High-level description of the digital public service(s) affected by the requirements

Digital public service or category of digital public services	**Description**	**Reference(s) to the requirement(s)**	**Interoperable Europe Solution(s)** **Not applicable**	**Other interoperability solution(s)**
Strategical support	Prepare analytical products of operational and strategical nature,	Article 7 Article 49, 50, 51, 52, 53		Europol supports the development and use of common analytical methodologies and standards
Facilitate Information	Sharing: obligations for MS including ARO and FIUs and	Articles 8(7), 9, 16(a), 16(c) Article 12 13, 25(5)(a), (b), 29, 30,		UMF, standards on financial and biometric

exchange	Europol to share information Cross-checking services: one central service, incl. DNA matching application for MS CA; hit no/hit mechanism for EUBOAs and EU information systems; further access by EPPO to Europol analytical environment Exchange Channels: Police Shared data space for joint cases, and SIENA for bilateral / multilateral exchanges.	34 Articles 35 to 39 Articles 46, 54 Articles 80, 81 Article 45, 46, 47, 49, 50-51, 136		information borne by sectorial / information exchange legislation (ARO, AML, Prüm II, VIS …) DNA application will materialize for the first time a EU led standard in the domain. EU Police Digital Identity support an easy addressing of counterparts in the exchanges.
Cooperation with private parties	Provision of information to private parties in crisis situation, for removing and referring terrorist content online, and illicit content, based on dedicated platform. Request information from private parties via ENU.	Articles 14, 47, 96 to 99 Articles 49, 50, 51, 53, 55, 56		UMF
Support Criminal intelligence analysis	<u>Provide criminal intelligence analysis</u> Europol analytical environment with advanced forensics. Set of advanced analytical	Articles 13 to Article 19 Article 48, 49, 50, 51, 53, 55, 56		UMF Set of governance measures and frameworks to steer, standardize, coordinate, develop, deploy, support the uptake

	tools and forensics Supports the joint criminal analysis Police Shared data space for Member State joint cooperation. Same advanced tools as above.	Article 41 to Article 45 Articles 48, 49, 50, 51, 53, 55, 56, 137		of advanced analytical capabilities by Member States including AI-based: Articles 13 to 19, 22(3)(a), 26, 53, 54, 55, 56, 57 to 64
Data protection Rights	Applications of rights of data subjects related to data protection, and oversight	Articles 103-106, 116(3), 117		N/A

Reliance of digital public services over digital solutions

X: depends on P: may depend on	Europol cross checking service	Europol Analytical environment	Police Shared Data Space	SIENA	Platform for cooperation with private parties	EPRIS	Other Services and tools	Europol cloud infrastructure	EU Police Digital Identity	Statistics and reporting tool	EU DNA matching application
Strategical support		X	X	X			P	P	P	X	
Facilitate information exchange	X	X	X	X	X	X	P	X	X		X

Cooperation with private parties		X	X		X		P	P	P		
Support criminal intelligence analysis	X	X	X	X	P	X	P	X	X		X

Impact of the requirement(s) as per digital public service on cross-border interoperability

Strategical support

Assessment	**Measure(s)**	**Potential remaining barriers (if applicable)**
Alignment with existing digital and sectorial policies	No digital or sectorial policy identified.	-
Organisational measures for a smooth cross-border digital public services delivery	- Management Board delegation to Executive Board delegation (Article 75(1)). - Executive Board to support MB decisions (Article 75(5)) - Regular Meeting of the HENU (Article 25(4)).	-
Measures taken to ensure a shared understanding of the data	- Europol to develop standards on strategic products (Article 7(3)).	-
Use of commonly agreed open technical specifications and standards	- Europol to develop standards on strategic products (Article 7(3)). - Common Statistical and reporting tool, with categories defined by implementing act (Article 52(6)).	-

Facilitate information exchange

Assessment	Measure(s)	Potential remaining barriers (if applicable)
Alignment with existing digital and sectorial policies	New policy reinforces the material reach of the two instruments . Prüm II: Regulation (EU) 2024/982 is amended to extend the capacity for Europol to consult national databases (Article 136); Europol develops an EU DNA matching application to support the DNA exchanges under Prüm II (Article 54) Europol responsibility over EPRIS is explicated under Article 48. . Information exchange Directive (EU) 2023/977: SIENA is used by national SPOC to provide information to Europol (Article 46(3)), as a default channel to exchange information with Europol (Article 46(5)); Creation of a JOAC can be the continuation of an exchange of information under the Directive (Art 46(4)); SIENA can be used for information exchange with third countries (Article 46(7)). . EPPO Council Regulation (UE) 2017/1939: under Article 73(3) information having triggered a hit shall be shared with EPPO. . Eurojust Regulation (EU) 2018/1727: reciprocal access to information for the purpose of cross-checking. . Asset Recovery Directive (EU) 2024/1260: under the proposed policy details and extends the responsibilities and abilities of the agency in the cooperation framework set out under Article 29 of the Directive. Under Article 9 Europol gains access to data either directly or indirectly	Regulation remains quiet on the interplay with the following regulations on specific provisions related to the exchange of information for the purposes of the prevention, detection, investigation of criminal activities . PNR: Directive 2016/681 . API: Regulation (EU) 2025/13 . VIS Regulation (EU) 767/2008, EES Regulation 2017/2226, ETIAS Regulation (EU) 2018/1240, Eurodac Regulation (EU) 2024/1358 . Information on crypto-assets Regulation (EU) 2023/1113 . Firearms Directive (EU) 2021/555 and Regulation (EU) 2025/41

	accessible by the asset recovery offices. . Interoperability Regulation (EU) 2019/818: Europol is entrusted to support UMF development (Article 53). <u>Clearer responsibilities with Codification of centers & systems</u> . Immigration liaison officer Regulation (EU) 2019/1240: obligations to connect to SIENA; obligations to contribute to the provision of information to Europol is clarified. . Financial information Directive (EU) 2019/1153: scope of cooperation with FIUs is clarified to be possibly broader than money laundering and financing of terrorism, and regrouped under a dedicated article 9(4) & 9(5) on the support to financial investigations and asset recovery. . Interoperability Regulation (EU) 2019/818: access by EU large scale IT systems and Screening regulation to Europol data for cross-checking (i.e. ETIAS and VIS central systems) relies on a secure communication channel established under Article 36(2)(e) with the European Search Portal (ESP). . Screening Regulation (EU) 2024/1356: access by screening authorities now relies on the established communication channel between the cross-checking mechanism and the ESP. <u>Alignment remains as is/ reformulation</u> . SIS: Regulation (EU) 2018/1860, 1861, 1862 the role of Europol with regards the analysis of supplementary	

	information, in the insertion of alert for information, on hits on alerts for information and terrorist activity relate alerts Regulations. . FIU Directive (EU) 2015/849: safeguard on the non-interference with exchanges with private parties under the Directive remains the same. . Cybersecurity Regulation (EU) 2019/881: Cooperation with ENISA remains identical.	
Organisational measures for a smooth cross-border digital public services delivery	Concerning the development of necessary capabilities to deliver digital public service - Creation of ICT and Information Management Steering group (Article 55). - Creation of ICT and Information Management Advisory group (Article 56). - Europol to provide technical support for integration (Article 22(2) para. 3). - Europol National Units tasks are clarified concerning the uptake of digital public service (Article 25(6)) including technical. - ENU is supported by the Europol Support Office (Article 26) staffed over the EU by 150+ Europol staff.	-
Measures taken to ensure a shared understanding of the data	- Cf Europol, ENU & Support Offices support.	-
Use of commonly agreed open technical specifications and standards	Generalisation of UMF: - Europol to support its development and adoption (Article 53).	- UMF is not mandated for building Europol digital Solutions. - UMF is not mandated for the

	- ICT/IM AG (Article 56(5)(c)) contributes to the identification and promotion of common technical standards. - Europol to support standardisation processes, including the development and promotion of common standard, interoperability requirements, operational and technical specifications relevant for law enforcement cooperation (Article 57(3)(b): notably (Article 65(2)(b) through its Capabilities and Innovation Service. - Europol to provide technical support for integration (Article 22(2) para. 3).	integration of national systems.

Exchange with private parties

Assessment	**Measure(s)**	**Potential remaining barriers (if applicable)**
Alignment with existing digital and sectorial policies	Clearer responsibilities with Codification of centres & systems . TCO Regulation (EU) 2021/784: The newly codified *European Counter Terrorism Centre* is untrusted all tasks from Europol regarding referrals and removals; and take place on a newly established digital *cooperation platform for cooperation with private parties* (Article 47(2)(a)). . DSA Regulation (EU) 2022/2065: similar as above under Article 47(2)(a). . Child sexual abuse material (CSAM) EU framework:	Regulation remains quiet on the interplay with the following regulations on specific provisions related to the exchange of information for the purposes of the prevention, detection, investigation of criminal activities.

	Europol tasks and capabilities regarding the exchange of CSAM is further streamlined with the generic regime of exchanges with private parties under Article 97. <u>Alignment remains as is/ reformulation</u> . FIU Directive (EU) 2015/849: safeguard on the non-interference with exchanges with private parties under the Directive remains the same.	
Organisational measures for a smooth cross-border digital public services delivery	Concerning the development of necessary capabilities to deliver digital public service to Member States and EUBOAs: cf supra "information exchange". For the deployment / uptake by private parties: - Europol may establish cooperative relation with private parties (Article 91). - Europol establishes a procedure for granting or withdrawing secure access of private parties to the platform (Article 43(3),	- Support to private parties similar to Member State at the discretion of Europol and to bilateral agreements.
Measures taken to ensure a shared understanding of the data	- Cf Europol, ENU & Support Offices support.	- Support to private parties similar to Member State at the discretion of Europol and to bilateral agreements
Use of commonly agreed open technical specifications and standards	- Europol Invites private parties to contribute to the work of the Innovation Advisory Group (Article 67).	- Invitation to private parties to contribute to the work of the Innovation Advisory Group not explicitly covering standard (Article 67)

<u>Support criminal intelligence analysis</u>

Assessment	Measure(s)	Potential remaining barriers (if applicable)
Alignment with existing digital and sectorial policies	New policy reinforces the material reach of the two instruments Anti money laundering Directive (EU) 2024/1640: Europol can support joint analysis carried out by the European Anti-fraud office (AMLA) pursuant to the Directive in Article 76 Frontex Regulation (EU) 2019/1896: Europol provides risk analyses to Frontex on the basis of travel information (Article 77(1)) Alignment remains as is/ reformulation	Regulation remains quiet on the interplay with the following regulations on specific provisions related to the exchange of information for the purposes of the prevention, detection, investigation of criminal activities . e-codex Regulation (EU) 2022/850 . JIT collaboration platform Regulation (EU) 2023/969
Organisational measures for a smooth cross-border digital public services delivery	Same as for "information exchange" - Specific interest for new Europol obligations supporting the uptake of new advanced analytical and forensic capabilities under Article 59	-
Measures taken to ensure a shared understanding of the data	Same as for "information exchange"	-
Use of commonly agreed open technical specifications and standards	Same as for "information exchange"	-

4.5. Measures to support digital implementation

High-level description of measures supporting digital implementation

Description of the measure	**Reference(s) to the requirement(s)**	**Commission role** (if applicable)	**Actors to be involved** (if applicable)	**Expected timeline** (if applicable)
Adoption of implementing / delegated acts or guidelines	Article 38(3) and 137(1) Article 50(9) and 137(2) Article 42(4) and 137(3) Article 81(8) and 137(4) Article 52(6) and 137(5)	Adopt the acts	Member States	Y0+1
Adoption of implementing rules	Article 13(5) Article 70(2)(j)	Vote in MB	Europol Member States Commission	Y0+1
Support to testing, deployment, integration, operation uptake incl. training	Article 25, 26 Article 65(2)(b) Article 66(1) Article 59, 62, 63, 64	Supervisory role in IM/ICT AG, Steering group	Europol Member States	Solution dependent; see § 1.5.1